SISTEMAS OPERATIVOS

ACTIVIDAD DE APRENDIZAJE 15
TAREA 8

Profesor:
VIOLETA DEL ROCIO BECERRA VELAZQUEZ

VERDUZCO ROSALES LUIS ENRIQUE
223992388
Ingenieria en Computación

30/11/25

CUCEI DIVTIC D04

ÍNDICE

---

1. Criptografía

La criptografía es la ciencia y el arte de asegurar mensajes mediante códigos, transformando la información legible (texto plano) en un formato ilegible (texto cifrado) a través de algoritmos y claves. Su objetivo principal es garantizar las propiedades del modelo CIA (Confidencialidad, Integridad y Disponibilidad).

- Confidencialidad: Se logra mediante el cifrado, asegurando que sólo el destinatario intencionado pueda leer el mensaje.
- Integridad: Se garantiza mediante funciones hash y firmas digitales, asegurando que el mensaje no ha sido alterado en tránsito.
- Autenticación y No Repudio: Se logra mediante el uso de claves públicas y firmas digitales, verificando la identidad del remitente y probando que la transacción se originó en él.

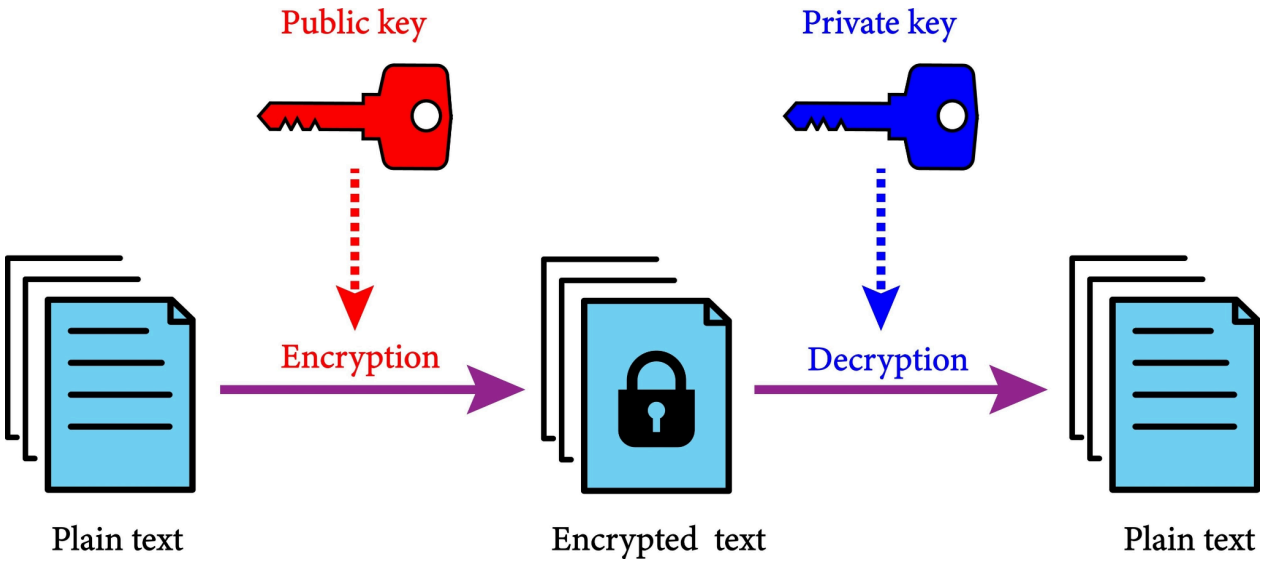
Clasificación de Algoritmos Criptográficos

Tipo de Algoritmo	Descripción	Uso Principal	Ejemplos
Cifrado Simétrico (Clave Secreta)	Utiliza la misma clave secreta para cifrar y descifrar el mensaje. Es extremadamente rápido y eficiente para grandes volúmenes de datos.	Confidencialidad y cifrado masivo de datos (datos en reposo o en tránsito).	AES (Advanced Encryption Standard), DES (Data Encryption Standard).
Cifrado Asimétrico (Clave Pública)	Utiliza un par de claves matemáticamente relacionadas: una pública (para cifrar/verificar firmas) y una privada (para descifrar/crear firmas). Es más lento.	Autenticación, intercambio seguro de claves, firmas digitales.	RSA, ECC (Elliptic Curve Cryptography), Diffie-Hellman.
Funciones Hash	Algoritmos unidireccionales que toman una entrada de cualquier tamaño y producen una salida de longitud fija llamada resumen criptográfico. Un cambio mínimo en la entrada produce un hash completamente diferente.	Integridad de datos y almacenamiento seguro de contraseñas.	SHA-256, SHA-3, MD5 (obsoleto).

Mecanismos Avanzados

- Perfect Forward Secrecy (PFS):
  Un principio criptográfico que asegura que el compromiso de una clave de largo plazo no comprometa las claves de sesión anteriores. Cada sesión de comunicación genera claves temporales únicas, usadas en protocolos como TLS 1.3.

- Curvas Elípticas (ECC):
  Permite obtener la misma fortaleza criptográfica que RSA con claves mucho más pequeñas. Por ejemplo, una clave ECC de 256 bits es tan fuerte como una clave RSA de 3072 bits, lo que es crucial para dispositivos de bajo consumo o entornos móviles.



2. Esteganografía

La Esteganografía (del griego escritura cubierta) es el arte de ocultar la existencia de un mensaje secreto dentro de un objeto portador (cover), como una imagen, un archivo de audio o un video.

Criptografía vs. Esteganografía:

- La criptografía oculta el contenido (haciéndolo incomprensible).
- La Esteganografía oculta la existencia misma del mensaje.

Técnicas de Ocultación:

1. LSB (Least Significant Bit):
   Es la técnica más común. Consiste en reemplazar el bit menos significativo de cada byte de datos del portador. En una imagen, cambiar el último bit de un píxel RGB (ej. de 11111110 a 11111111) resulta en un cambio de color imperceptible para el ojo humano, permitiendo almacenar una gran cantidad de datos secretos.

2. Dominio de Transformación:
   Ocultar información en los coeficientes de algoritmos de compresión (ej. la DCT o Transformada de Coseno Discreta en archivos JPEG). Esta es más robusta ya que el mensaje sobrevive mejor a la compresión y edición del archivo.

3. Inyección en Metadatos:
   Ocultar datos en campos de metadatos de archivos (ej. EXIF en imágenes o etiquetas ID3 en archivos MP3) o en espacios no utilizados del encabezado del archivo.

Estegoanálisis

Es la contraparte de la Esteganografía, buscando detectar la presencia de mensajes ocultos. Los analistas buscan anomalías estadísticas o artefactos inusuales en la distribución de ruido o color del archivo que delaten la manipulación.

3. Aplicación en Sistemas Operativos y Redes

Ambas disciplinas son esenciales para construir una defensa en profundidad en cualquier infraestructura tecnológica.

Aplicación en el Sistema Operativo (SO).

Disciplina	Mecanismo de Aplicación	Detalle Técnico
Criptografía	Cifrado de Disco Completo (FDE)	Herramientas como BitLocker (Windows) y FileVault (macOS) cifran todo el volumen de almacenamiento. Si un dispositivo es robado o perdido, los datos permanecen inaccesibles sin la clave o contraseña correcta.
	Almacenamiento de Contraseñas	Las contraseñas de usuario no se guardan en texto plano, sino como hashes criptográficos (ej. bcrypt, PBKDF2). El SO compara el hash de la entrada del usuario con el hash almacenado para la autenticación.
	Control de Integridad de Archivos	El SO puede usar hashing para verificar la integridad de archivos críticos del sistema o software al ser instalados, protegiendo contra rootkits o manipulación maliciosa.
Esteganografía	Canales Encubiertos de Malware	Los atacantes pueden esconder comandos maliciosos o la fase final de la carga útil de un malware dentro de imágenes o archivos temporales de apariencia inocente en el disco.
	Marcas de Agua Digital	Se utiliza para incrustar información de propiedad o rastreo en archivos para identificar la fuente de una filtración (función más forense que de protección activa).

Aplicación en Redes.

Disciplina	Mecanismo de Aplicación	Detalle Técnico
Criptografía	Comunicaciones Seguras (TLS/SSL)	El protocolo TLS (Transport Layer Security, sucesor de SSL) cifra el tráfico HTTP (creando HTTPS), utilizando criptografía asimétrica para el intercambio inicial de claves y simétrica para la transferencia de datos en masa.
	Redes Privadas Virtuales (VPN)	Utiliza protocolos como IPSec o OpenVPN, que emplean cifrado de extremo a extremo para encapsular todo el tráfico de red, creando un "túnel" seguro sobre una red pública (Internet).
	Certificados Digitales	Basados en la criptografía asimétrica, son emitidos por Autoridades de Certificación (CA) para verificar la identidad de un servidor o dispositivo en la red.
Esteganografía	Canales Encubiertos de Red	Utilización de campos no esenciales o no utilizados de los protocolos de red (ej. el campo de identificación o padding en los paquetes TCP/IP) para transmitir secretamente datos robados (exfiltración), evadiendo la detección de Firewalls o IDS/IPS.
	Infiltración Oculta	El comando inicial para que un malware se conecte a su servidor de control y comando (C2) se oculta dentro del contenido de un archivo multimedia descargado (ej. una imagen GIF).

4. Infografía

5. La Seguridad y el Papel del Usuario

Introducción: La Seguridad como Pilar de la Era Digital

La seguridad informática ha trascendido su definición original de mero control de acceso para convertirse en un ecosistema complejo que garantiza la continuidad y fiabilidad de los sistemas de información. En la actualidad, la seguridad se define bajo los principios de la tríada CIA: Confidencialidad (protección contra el acceso no autorizado), Integridad (prevención de la modificación no autorizada de datos) y Disponibilidad (asegurar el acceso a los recursos cuando se necesiten).

Este ensayo examina los mecanismos de protección implementados en el Sistema Operativo (SO) y las redes, además de analizar el papel indispensable que juega el usuario en la orquestación efectiva de esta defensa. La tesis central es que la seguridad es un ejercicio de defensa en profundidad, donde la sofisticación tecnológica es inútil sin la adecuada gestión de la variable humana.

I. Seguridad y Protección en el Sistema Operativo: La Primera Barrera Lógica
El Sistema Operativo es el kernel de la seguridad, el guardián de los recursos del endpoint (servidor, PC o móvil). Sus mecanismos de protección se centran en el control estricto de quién accede a qué recursos y bajo qué condiciones.

1. Control de Acceso y Gestión de Privilegios

El mecanismo fundamental es el Control de Acceso Discrecional (DAC), donde el SO asigna permisos específicos a usuarios y grupos sobre archivos y directorios (lectura, escritura, ejecución). Este control se basa en el Principio del Mínimo Privilegio, que dicta que un usuario, proceso o aplicación solo debe tener los permisos estrictamente necesarios para cumplir su función. Por ejemplo, en Windows, la característica UAC (User Account Control) previene que un programa realice cambios a nivel de sistema sin la elevación explícita de privilegios por parte del usuario, mitigando el daño potencial de un proceso comprometido.

2. Cifrado y Aislamiento (Sandboxing)

La criptografía se aplica directamente en el SO mediante el Cifrado de Disco Completo (FDE), con herramientas como BitLocker (Windows) o FileVault (macOS). Esto transforma todos los datos del disco duro en texto cifrado persistente. Si el dispositivo es robado, el atacante no puede acceder a los datos sin la clave de descifrado, garantizando la confidencialidad en reposo.

Además, el SO moderno utiliza técnicas de sandboxing o contenedorización. Estos procesos ejecutan aplicaciones o servicios en un entorno virtual aislado (como una "caja de arena"). Si una aplicación maliciosa explota una vulnerabilidad dentro de su sandbox, el daño se limita a ese contenedor, impidiendo que el ataque se propague al kernel del SO o a otros recursos críticos.

II. Seguridad y Protección en la Red: La Defensa de Tráfico y Perímetro

La red es el conducto por el que viajan los datos. La seguridad de red se enfoca en tres aspectos clave: filtrado de tráfico, monitoreo y comunicaciones cifradas.

1. Filtrado Perimetral y Monitoreo Activo

Los Firewalls actúan como puertas de control, inspeccionando el tráfico entrante y saliente. Los firewalls de nueva generación utilizan DPI (Deep Packet Inspection) para no solo revisar las cabeceras (puertos y direcciones IP), sino también el contenido (payload) del paquete, permitiendo detectar malware o patrones de ataques de Denegación de Servicio (DoS).
A su vez, los sistemas IDS (Intrusion Detection Systems) y IPS (Intrusion Prevention Systems) monitorean constantemente la red, buscando firmas de ataques conocidos o anomalías en el comportamiento del tráfico. Un IPS puede bloquear automáticamente el tráfico cuando detecta una actividad maliciosa.

2. Criptografía en Redes y el Modelo Zero Trust

La criptografía es la base de las comunicaciones de red seguras. Protocolos como TLS/SSL (que habilita HTTPS) garantizan que las conexiones web sean cifradas. Las VPNs (Redes Privadas Virtuales), a menudo basadas en protocolos como IPSec, extienden este cifrado para crear "túneles" seguros a través de redes públicas, asegurando la confidencialidad de la conexión en su totalidad.

La seguridad de red moderna se ha movido hacia el paradigma Zero Trust (Confianza Cero). Este modelo elimina el concepto de "perímetro de red confiable". Bajo Zero Trust, ningún usuario o dispositivo es inherentemente confiable, ni siquiera si está dentro de la red corporativa. Cada solicitud de acceso debe ser autenticada, autorizada y validada de forma continua, asegurando que la seguridad no dependa únicamente de un muro exterior (el firewall).

III. El Papel del Usuario: La Variable Humana y la Ingeniería Social

Por muy robusto que sea un sistema operativo o una red, el eslabón más débil en la cadena de seguridad sigue siendo, invariablemente, el ser humano. La ciberdelincuencia ha encontrado que es más fácil explotar la confianza o la curiosidad de un empleado que el fallo técnico en un firewall. Esto es la Ingeniería Social.

1. La Amenaza de la Ingeniería Social

La Ingeniería Social se define como el arte de manipular a las personas para que revelen información confidencial. El Phishing es la técnica más exitosa, donde los atacantes envían correos electrónicos que simulan ser entidades legítimas para robar credenciales. El usuario, por falta de atención o conocimiento, hace clic en un enlace o descarga un archivo malicioso, neutralizando instantáneamente todas las capas de seguridad tecnológica. Un solo clic puede introducir ransomware o spyware en el SO o abrir un canal encubierto para la exfiltración de datos a través de la red.

2. Responsabilidad del Usuario y Conciencia de Seguridad

Para que la defensa en profundidad funcione, el usuario debe transformarse de una vulnerabilidad a una capa de seguridad activa. Sus responsabilidades incluyen:

- Gestión de Identidad Fuerte: Utilizar contraseñas complejas y únicas, y, lo más importante, habilitar la Autenticación de Dos Factores (2FA). El 2FA, al requerir algo que el usuario sabe (contraseña) y algo que el usuario tiene (código del teléfono), minimiza el impacto del robo de credenciales por phishing.

- Conciencia Situacional: Ser capaz de reconocer indicadores de ataques (URL sospechosas, errores gramaticales, tono de urgencia en correos). El usuario es el sensor humano más importante de la red y debe estar capacitado para reportar de inmediato cualquier anomalía.

- Higiene Digital: Mantener el software y el sistema operativo actualizados para eliminar vulnerabilidades. Abstenerse de instalar software de fuentes no confiables o de conectar dispositivos USB desconocidos a la red corporativa.

Conclusión

La seguridad y la protección de los sistemas de cómputo y las redes son el resultado de una meticulosa estrategia de defensa en capas. La criptografía proporciona la confidencialidad y la integridad a través del cifrado de disco y el protocolo TLS. Los sistemas operativos implementan un riguroso control de acceso y el aislamiento de

procesos. Las redes filtran y monitorean el tráfico bajo modelos de confianza rigurosos como Zero Trust. Sin embargo, todas estas herramientas tecnológicas son meras fortificaciones. La seguridad final reside en la disciplina y conciencia del usuario. La capacitación continua y la promoción de una cultura de seguridad son la inversión más crucial para cerrar la brecha de la Ingeniería Social, asegurando que el individuo se convierta en la primera y más efectiva línea de defensa.

6. Resumen de una obra (Black Mirror: Cállate y Baila)

Resumen de la Trama

El episodio se centra en Kenny, un adolescente que trabaja en un restaurante. Tras un breve encuentro en línea, un hacker anónimo toma el control de su computadora y, sin su conocimiento, graba un momento privado comprometedor a través de la webcam.

El hacker procede a chantajear a Kenny y a otros individuos. Les envía una serie de instrucciones a través de mensajes de texto encriptados, obligándolos a realizar tareas degradantes y delictivas bajo la amenaza de difundir el material comprometedor. Kenny se une a Hector, otro chantajeado, para cumplir una misión final que parece ser un robo. Al final, la misión culmina en una confrontación en un campo abierto, donde se revela que todos los chantajeados estaban siendo utilizados para un objetivo mayor y que sus momentos comprometidos eran variados y a menudo vergonzosos o ilegales. La escena final muestra cómo el hacker revela públicamente el secreto de Kenny, demostrando su control total sobre las vidas de sus víctimas.

- Análisis de Seguridad Informática y Ética

El capítulo “cállate y baila" es un estudio de un caso dramático y aterrador sobre las fallas de seguridad y la Ingeniería Social:

1. Malware y Vigilancia Invasiva (Spyware)

El punto de partida del chantaje es la inyección de malware de vigilancia (Spyware) en el equipo de Kenny. Este malware no solo espía sus actividades, sino que también toma el control remoto de los periféricos, específicamente la cámara web y el micrófono.

- Vulnerabilidad Explotada:
  Esto ilustra una vulnerabilidad común conocida como RAT (Remote Access Trojan), que permite a un atacante operar un equipo remotamente sin el

conocimiento del usuario. El hacker aprovecha la confianza o la falta de parches en el SO o el navegador para instalar el malware.

- Lección de Seguridad:
  Destaca la importancia de cubrir físicamente las cámaras web cuando no se usan y de mantener los sistemas operativos y los navegadores actualizados para prevenir la ejecución de exploits que facilitan la instalación de este tipo de troyanos.

2. Chantaje Digital y Coacción

El hacker utiliza el conocimiento adquirido a través de la vigilancia para ejercer un control psicológico completo. Este es un ejemplo de chantaje digital (aunque la naturaleza del contenido varía entre víctimas), donde la amenaza de la exposición pública es más potente que cualquier cifrado.

- Ingeniería Social en su Máxima Expresión:
  La metodología del chantaje es pura Ingeniería Social. El atacante no necesita hackear continuamente, sino que usa la miedo y la desesperación de la víctima para obligarla a violar la ley o realizar acciones que ponen en riesgo su seguridad física, convirtiendo a las víctimas en herramientas del crimen.

3. La Ilusión del anonimato y las consecuencias

El episodio juega con la idea del anonimato en línea y la falta de responsabilidad en la *dark web*. El atacante opera en las sombras, dejando un rastro digital que las víctimas no pueden seguir.

- Fallo de la Criptografía:
  Aunque el hacker usa mensajes de texto encriptados (como se menciona en el episodio) para enviar las órdenes, la criptografía aquí se utiliza como una herramienta del atacante para mantener su anonimato y la confidencialidad de sus comandos, no para proteger a las víctimas.

- Impacto Ético:
  El final del episodio enfatiza que en la era digital, la privacidad es una ilusión, y que las acciones privadas pueden tener consecuencias públicas devastadoras si son explotadas por terceros maliciosos. El usuario, al conectarse, asume un riesgo que ninguna herramienta de seguridad por sí sola puede mitigar.

Conclusión

"Cállate y baila" es una advertencia sobre la vulnerabilidad del endpoint y la peligrosidad de la Ingeniería Social. Ilustra que el malware no siempre busca robar dinero, sino que puede buscar información comprometedora para ejercer control. El capítulo subraya la lección de que el usuario debe ser extremadamente cauteloso con las fuentes de software y mantener una alta conciencia sobre lo que se hace frente a una cámara conectada a Internet, ya que la falla humana es la vulnerabilidad más fácil de explotar.

Bibliografía

CIS Informática. (s.f.). ¿Qué es la esteganografía en ciberseguridad?. Recuperado de https://www.cisinformatica.cat/es/que-se-la-esteganografia-en-ciberseguridad/

EsGeeks. (s.f.). Diferencia entre esteganografía y criptografía. Recuperado de https://esgeeks.com/diferencia-esteganografia-y-criptografia/

IBM. (s.f.). Criptografía. Recuperado de https://www.ibm.com/mx-es/think/topics/cryptography

MSMK University. (s.f.). ¿Qué es la esteganografía?. Recuperado de https://msmk.university/que-es-la-esteganografia-msmk-university/

Revista UNAM. (s.f.). Criptografía y Seguridad. Revista UNAM, 7(7). Recuperado de https://www.revista.unam.mx/vol.7/num7/art55/jul_art55.pdf.

Universidad de Murcia. (s.f.). Criptografía. Recuperado de https://www.um.es/adelrio/Docencia/Criptografia/Criptografia.pdf

Vaca, F. S. (2016, 26 de noviembre). 'Black Mirror': 'Shut Up and Dance', la intimidad no es una broma. Espinof. Recuperado de https://www.espinof.com/series-de-ficcion/black-mirror-shut-up-and-dance-la-intimidad-no-es-una-broma