UNIVERSIDAD PARAGUAYO ALEMANA

Ingeniería en Tecnologías de la Información Empresarial TIE

Seguridad en TICs

Prof.: Chrystian Ruiz Diaz

DISCLAIMER

Todo el contenido de esta presentación se proporciona **exclusivamente con fines didácticos y educativos en el ámbito académico**.

El uso inapropiado de las técnicas y/o conocimientos expuestos en esta presentación puede violar leyes nacionales e internacionales.

El autor y la institución educativa no se hacen responsables del uso indebido de la información contenida en esta presentación.

Se enfatiza que la información debe ser empleada únicamente para propósitos éticos, legales y con la debida autorización de las autoridades competentes.

Fundamentos Criptográficos

Una introducción a los conceptos básicos de la criptografía

1. Conceptos Básicos

- 1.1. **Cifrado y Descifrado**
- • Cifrado (Encriptación): El proceso de convertir información legible (texto plano) en una forma ilegible (texto cifrado) utilizando un algoritmo y una clave.
- • Descifrado (Desencriptación): El proceso inverso del cifrado, que convierte el texto cifrado de vuelta en texto plano utilizando un algoritmo y una clave.

- 1.2. **Claves Criptográficas**
- • Clave: Un valor secreto utilizado en los algoritmos de cifrado y descifrado. Las claves deben mantenerse confidenciales.
- o Clave Simétrica: La misma clave se utiliza para cifrar y descifrar los datos.
- o Clave Asimétrica: Se utiliza un par de claves; una clave pública para cifrar y una clave privada para descifrar.

- 1.3. **Algoritmos Criptográficos**
- • Algoritmo de Cifrado: Un conjunto de reglas matemáticas que se utilizan para realizar el cifrado y descifrado.
- o Cifrado Simétrico: Usa la misma clave para cifrar y descifrar. Ejemplos: AES (Advanced Encryption Standard), DES (Data Encryption Standard).
- o Cifrado Asimétrico: Usa un par de claves (pública y privada). Ejemplos: RSA (Rivest-Shamir-Adleman), ECC (Elliptic Curve Cryptography).

2. Criptografía Simétrica

- 2.1. **Características**
- • Usa una sola clave para tanto el cifrado como el descifrado.
- • Rápido y eficiente en términos de procesamiento.
- • La clave debe ser compartida de manera segura entre las partes comunicantes.

- 2.2. **Algoritmos Populares**
- • **AES** (Advanced Encryption Standard): Un estándar de cifrado simétrico adoptado por el gobierno de los Estados Unidos. Es conocido por su seguridad y eficiencia.
- • **DES** (Data Encryption Standard): Un algoritmo de cifrado más antiguo y menos seguro comparado con AES. Ha sido reemplazado en gran parte por AES debido a sus vulnerabilidades.

3. Criptografía Asimétrica

- 3.1. **Características**
- • Usa un par de claves: una clave pública (para cifrar) y una clave privada (para descifrar).
- • Permite una distribución más segura de las claves.
- • Es más lento y consume más recursos que la criptografía simétrica.

- 3.2. **Algoritmos Populares**
- • RSA (Rivest-Shamir-Adleman): Un algoritmo de cifrado asimétrico ampliamente utilizado para asegurar datos sensibles, como en transacciones bancarias y comunicaciones seguras.
- • ECC (Elliptic Curve Cryptography): Proporciona un nivel de seguridad comparable a RSA pero con claves más pequeñas, lo que resulta en un mejor rendimiento y menor consumo de recursos.

4. Funciones Hash

- 4.1. **Características**
- • Convierte datos de longitud variable en una cadena de longitud fija (valor hash).
- • Es unidireccional: no se puede derivar el texto original del valor hash.
- • Es fundamental para la integridad de los datos y la autenticación.

- 4.2. **Algoritmos Populares**
- • SHA (Secure Hash Algorithm):
- o SHA-1: Obsoleto debido a vulnerabilidades de seguridad.
- o SHA-256, SHA-3: Más seguros y ampliamente utilizados en aplicaciones modernas.

- 4.3. **Aplicaciones**
- • Verificación de Integridad: Los valores hash se utilizan para verificar que los datos no han sido alterados.
- • Autenticación: Las contraseñas se almacenan y verifican mediante valores hash para protegerlas de accesos no autorizados.

5. Firmas Digitales

- 5.1. **Características**
- • Proporcionan autenticidad y no repudio a los documentos digitales.
- • Utilizan criptografía asimétrica: el firmante usa su clave privada para crear la firma, y cualquier persona puede verificarla usando la clave pública del firmante.

- 5.2. **Proceso**
- 1. Creación de Firma: El documento se cifra con la clave privada del firmante para generar una firma digital.
- 2. Verificación de Firma: Cualquiera puede usar la clave pública del firmante para descifrar la firma y verificar la autenticidad del documento.

6. Certificados Digitales

- 6.1. **Características**
- • Certificados electrónicos que vinculan una clave pública con la identidad de su propietario.
- • Emitidos por una Autoridad de Certificación (CA) confiable.

- 6.2. **Aplicaciones**
- • HTTPS: Los sitios web utilizan certificados digitales para establecer conexiones seguras (SSL/TLS).
- • Correo Electrónico Seguro: Se utilizan para firmar y cifrar correos electrónicos.

7. Protocolos Criptográficos

- 7.1. **TLS/SSL** (Transport Layer Security / Secure Sockets Layer)
- • Protocolo que proporciona comunicación segura a través de una red, principalmente utilizada en navegadores web para conexiones HTTPS.
- • Utiliza una combinación de criptografía simétrica y asimétrica para asegurar la transferencia de datos.

- 7.2. **PGP** (Pretty Good Privacy)
- • Un programa utilizado para cifrar y firmar datos, proporcionando privacidad y autenticación.
- • Comúnmente usado para asegurar correos electrónicos.

- 7.3. **IPsec** (Internet Protocol Security)
- • Un conjunto de protocolos para asegurar las comunicaciones a través de redes IP mediante la autenticación y cifrado de cada paquete IP.

8. Criptografía Cuántica

- 8.1. **Características**
- • Utiliza principios de la mecánica cuántica para mejorar la seguridad criptográfica.
- • Promete seguridad incluso contra ataques de computadoras cuánticas, que podrían romper muchos de los algoritmos criptográficos actuales.

- 8.2. **Aplicaciones**
- • QKD (Quantum Key Distribution): Permite la distribución de claves seguras utilizando partículas cuánticas como fotones.

¿PREGUNTAS?

Actividad de Proceso

Referencias

ESCRIVA, G. R. (2013). *Seguridad informática*. España: Macmillan Iberia SA.

Muchas Gracias..!!