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.

Aleatoriedad, Contraseñas, Entropía, MFA y Gestores de Contraseñas

Proporcionar una comprensión comprensiva de los conceptos clave de ciberseguridad y su aplicación para proteger sistemas y datos.

Aleatoriedad (Randomness)

- **Definición y Importancia**:

- Imprevisibilidad y falta de patrones en una secuencia de datos.

- Fundamental para la generación de claves criptográficas y contraseñas.

- **Aplicaciones**:

- Generación de Claves: Prevención de adivinación de claves.

- Contraseñas Seguras: Dificulta ataques de fuerza bruta.

- Tokens y Salts: Prevención de ataques de precomputación.

Contraseñas (Passwords)

Características de Contraseñas Seguras:

- - Larga: Al menos 12-16 caracteres.
- - Compleja: Letras mayúsculas y minúsculas, números y caracteres especiales.
- - Única: No reutilizar en múltiples cuentas.
- - Impredecible: Evitar información personal.

Buenas Prácticas:

- - Uso de gestores de contraseñas.
- - Implementación de 2FA.
- - Cambio periódico de contraseñas.

Entropía (Entropy)

Definición y Cálculo:

- - Medida de imprevisibilidad o aleatoriedad de un conjunto de datos.
- - Mayor entropía significa mayor seguridad.

Aplicaciones:

- - Generación de Contraseñas: Alta entropía en contraseñas.
- - Algoritmos Criptográficos: Maximización de la entropía.

Entropía (Entropy)

Calcular valor Entropia

$$H = L \times \log_2(N)$$

H es la entropía en bits.

N es el número de posibles símbolos que pueden aparecer en cada posición de la contraseña.

L es la longitud de la contraseña.

eres (N)
L): 8
6 bits

- **Contraseña Compleja:**
  - Contraseña: "P@ssw0rd123!"
  - Número de posibles caracteres (N): 94 (letras mayúsculas y minúsculas, números y símbolos)
  - Longitud de la contraseña (L): 12
- Entropía: H = 12 * Log2 (94) = 78.6 bits

Se recomienda que una contraseña tenga al menos 75 bits de entropía

Relación entre Aleatoriedad, Contraseñas y Entropía

Conexiones:

- - Aleatoriedad: Base para contraseñas y claves impredecibles.
- - Contraseñas Seguras: Deben ser aleatorias y con alta entropía.
- - Entropía: Mide la seguridad y previsibilidad de contraseñas y claves.

Autenticación Multifactor (MFA)

Definición: Requiere dos o más factores de verificación para acceder a un recurso.

Factores de Autenticación:

- 1. *Algo que sabes* (Conocimiento): Contraseña, PIN.
- 2. *Algo que tienes*(Posesión): Teléfono móvil, tarjeta inteligente.
- 3. *Algo que eres* (Inherencia): Datos biométricos.

Ejemplos de MFA

1. Contraseña y OTP(One-Time Password):

- - Ventajas: Seguridad adicional con OTP.

2. Contraseña y Token de Hardware:

- - Ventajas: Alta seguridad con token físico.

3. Biometría y Contraseña:

- - Ventajas: Uso de datos biométricos únicos.

4. Tarjeta Inteligente y PIN:

- - Ventajas: Combinación de dispositivo físico y PIN.

Implementación y Buenas Prácticas de MFA

Configuración y Mantenimiento:

- - Actualización de políticas de seguridad.

Experiencia del Usuario (UX):

- - Balance entre seguridad y usabilidad.

Redundancia:

- - Métodos alternativos de autenticación.

Gestores de Contraseñas

Definición: Aplicación para almacenar y organizar contraseñas de manera segura.

Funciones Clave:

- 1. Almacenamiento Seguro
- 2. Generación de Contraseñas
- 3. Autocompletado
- 4. Sincronización
- 5. MFA

Ventajas de Usar Gestores de Contraseñas

Seguridad Mejorada:

- - Generación de Contraseñas Fuertes.
- - Almacenamiento Cifrado.

Conveniencia:

- - Memorización de Múltiples Contraseñas.
- - Acceso Rápido.

Prevención de Ataques Comunes:

- - Phishing.
- - Reuse de Contraseñas.

Cómo Crear una Contraseña Segura Propia

Características de una Contraseña Segura:

- - Larga: Al menos 12-16 caracteres.
- - Compleja: Letras mayúsculas y minúsculas, números y caracteres especiales.
- - Única: No reutilizar en múltiples cuentas.
- - Impredecible: No usar información personal.

Pasos para Crear una Contraseña Segura:

- 1. Selecciona una Frase Base.
- 2. Utiliza las Iniciales.
- 3. Añade Complejidad.
- 4. Asegúrate de la Longitud.

Buenas Prácticas para Mantener la Seguridad de tus Contraseñas

1. No Reutilizar Contraseñas.
2. Utilizar un Gestor de Contraseñas.
3. Habilitar Autenticación Multifactor (MFA).
4. Actualizar Regularmente las Contraseñas.
5. Evitar Información Personal.
6. Monitorizar Actividad de la Cuenta.

Ejemplo de Creación de una Contraseña Segura

1. **Frase Base**: "Mi gato tiene 2 ojos verdes y come 3 veces al día."
2. **Iniciales**: "Mgt2ovyc3vad."
3. **Añadir Complejidad**: "Mgt2Ov&yc3v@d."
4. **Asegurar Longitud**: "Mgt2Ov&yc3v@d2024."

Conclusión

Comprender y aplicar los conceptos de aleatoriedad, contraseñas y entropía es esencial para asegurar sistemas y proteger la información. Utilizar herramientas como gestores de contraseñas y prácticas de seguridad como MFA puede significar la diferencia entre un sistema seguro y uno vulnerable. Crear contraseñas seguras y adoptar buenas prácticas es un paso esencial en la protección de la información personal y la integridad de los sistemas en el mundo digital.

UPA
UNIVERSIDAD PARAGUAYO ALEMANA
HEIDELBERG - ASUNCIÓN

¿PREGUNTAS?

Actividad de Proceso

Referencias

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

UPA
UNIVERSIDAD PARAGUAYO ALEMANA
HEIDELBERG - ASUNCIÓN

Muchas Gracias..!!