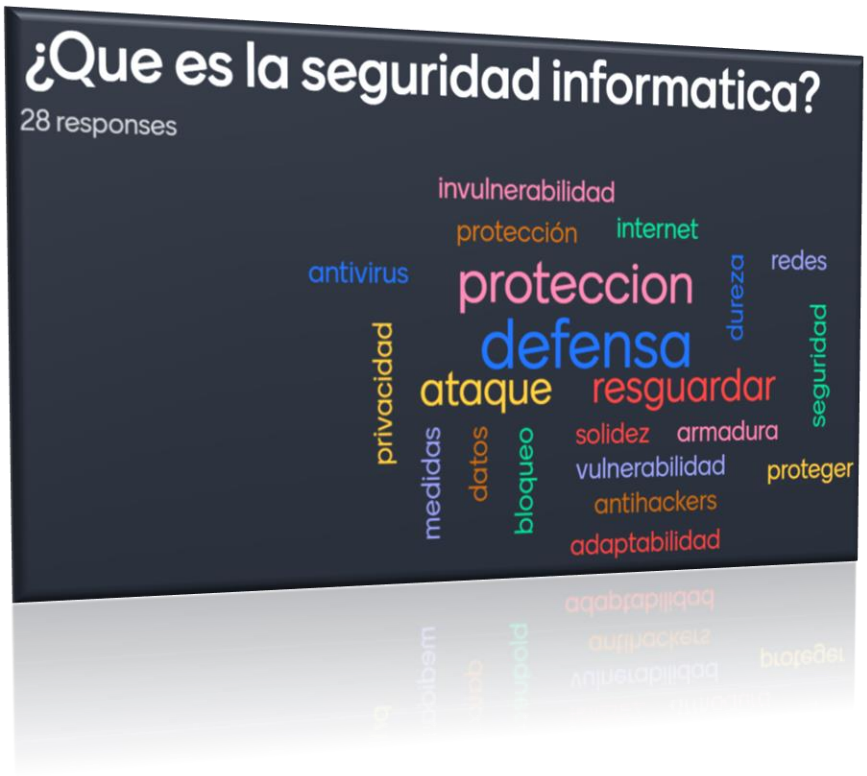
Universidad Paraguayo Alemana

UNIVERSIDAD PARAGUAYO ALEMANA
HEIDELBERG - ASUNCIÓN



Seguridad TICs

Prof.: Chrystian Ruiz Diaz

Contenido

Nota de Uso Académico

Este documento ha sido preparado exclusivamente para el uso académico del docente. Este documento no puede ser distribuido a ninguna otra parte ni utilizado para ningún otro propósito, diferente al establecido como alcance en el proyecto académico de la **UNIVERSIDAD PARAGUAYO ALEMANA**. El uso indebido del material fuera del ámbito académico no representa ninguna responsabilidad del docente.

Aleatoriedad, Contraseñas, Entropía, MFA y Gestores de Contraseñas

Introducción

La ciberseguridad es un campo crítico que abarca diversos aspectos esenciales para proteger sistemas y datos. Este material de lectura abarca los conceptos de aleatoriedad, contraseñas, entropía, autenticación multifactor (MFA) y gestores de contraseñas, proporcionando una guía comprensiva sobre cómo estos elementos contribuyen a la seguridad digital.

1. Randomness (Aleatoriedad)

Definición y Importancia

La aleatoriedad se refiere a la imprevisibilidad y la falta de patrones en una secuencia de datos. En ciberseguridad, es crucial para la generación de claves criptográficas y contraseñas. Los números aleatorios son fundamentales para crear elementos que sean difíciles de predecir o replicar, como contraseñas seguras, claves criptográficas y salidas de funciones hash.

Aplicaciones en Ciberseguridad

- **Generación de Claves:** Las claves criptográficas deben generarse de manera aleatoria para evitar que sean adivinadas por atacantes.
- **Contraseñas Seguras:** Las contraseñas creadas de forma aleatoria son más difíciles de romper que las que siguen patrones comunes.
- **Tokens y Salts:** Los tokens de sesión y los salts utilizados en hashing de contraseñas deben ser aleatorios para evitar ataques de precomputación como los ataques de diccionario o rainbow tables.

2. Passwords (Contraseñas)

Características de Contraseñas Seguras

Una contraseña segura es esencial para proteger las cuentas y la información personal de los usuarios. Debe ser:

- **Larga:** Al menos 12-16 caracteres. Cuanto más larga, mejor.
- **Compleja:** Incluir una combinación de letras mayúsculas y minúsculas, números y caracteres especiales.
- **Única:** No debe reutilizarse en múltiples sitios y servicios.
- **Impredecible:** No debe contener información personal fácilmente adivinable.

Buenas Prácticas

- **Gestores de Contraseñas:** Utilizar gestores de contraseñas para generar y almacenar contraseñas complejas.

- **Doble Factor de Autenticación (2FA):** Implementar 2FA para añadir una capa adicional de seguridad.
- **Cambio Periódico de Contraseñas:** Cambiar las contraseñas regularmente es una práctica recomendada en algunos entornos.

3. Entropy (Entropía)

Definición y Cálculo

La entropía en ciberseguridad mide la imprevisibilidad o aleatoriedad de un conjunto de datos. Mayor entropía significa mayor seguridad, ya que indica que es más difícil predecir o adivinar los datos.

- **Bit Entropy:** La entropía se mide en bits. Por ejemplo, una contraseña de 8 caracteres con una variedad de 94 caracteres posibles (letras, números y símbolos) tendría una entropía de 8 * log2(94) ≈ 52.4 bits.

Cálculo de Entropía

La entropía de una contraseña o clave se puede calcular utilizando la fórmula de entropía de Shannon, que se expresa como:

H = L*log2 (N)

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

donde:

- 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.

Por ejemplo, si una contraseña tiene 8 caracteres y cada carácter puede ser una de 94 opciones posibles (letras mayúsculas y minúsculas, números y símbolos), la entropía sería:

H=8*Log2 (94) = 52.4 bits

Esto significa que una contraseña de 8 caracteres con una variedad de 94 caracteres posibles tiene una entropía de aproximadamente 52.4 bits.

Evaluación de Seguridad

Una contraseña con mayor entropía es más segura porque es menos predecible y más difícil de romper mediante ataques de fuerza bruta. Los ataques de fuerza bruta prueban todas las combinaciones posibles hasta encontrar la correcta, por lo que una mayor entropía significa más combinaciones posibles y, por lo tanto, más tiempo y recursos necesarios para romper la contraseña.

Aplicación en Ciberseguridad

- **Generación de Contraseñas:** Usar generadores de contraseñas que aseguren alta entropía es crucial para crear contraseñas fuertes y seguras. Los generadores de contraseñas aleatorias proporcionan cadenas de caracteres que son difíciles de predecir.
- **Algoritmos Criptográficos:** Los algoritmos criptográficos están diseñados para maximizar la entropía en las claves generadas. Esto asegura que las claves sean impredecibles y seguras contra ataques.

Ejemplos Prácticos de Entropía

1. **Contraseña Básica:**
    - Contraseña: "password"
    - Número de posibles caracteres (N): 26 (solo letras minúsculas)
    - Longitud de la contraseña (L): 8
    - Entropía: H = 8 * Log2 (26)=37.6 bits

        - Letras minúsculas: 26 (español “ñ” total 27)
        - Letras mayúsculas: 26
        - Números: 10
        - Caracteres especiales: 32

2. **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

Aplicaciones en Ciberseguridad

- **Generación de Contraseñas:** Usar generadores de contraseñas que aseguren alta entropía.
- **Algoritmos Criptográficos:** Los algoritmos criptográficos se diseñan para maximizar la entropía en las claves generadas.

4. Conexión entre Aleatoriedad, Contraseñas y Entropía

La relación entre estos términos es fundamental en ciberseguridad:

- **Aleatoriedad** proporciona la base para crear contraseñas y claves criptográficas impredecibles.
- **Contraseñas seguras** deben ser aleatorias y tener alta entropía para resistir ataques de fuerza bruta y adivinación.
- **Entropía** mide la seguridad de las contraseñas y claves generadas, indicando su imprevisibilidad.

5. Multi-Factor Authentication (MFA)

Definición

MFA es un método de autenticación que requiere que un usuario proporcione dos o más factores de verificación independientes para acceder a un recurso, como una aplicación, una cuenta en línea o una VPN.

Factores de Autenticación

1. **Algo que sabes (Conocimiento):** Contraseña, PIN, respuesta a una pregunta de seguridad.
2. **Algo que tienes (Posesión):** Dispositivo físico como un teléfono móvil, tarjeta inteligente, token de hardware.
3. **Algo que eres (Inherencia):** Datos biométricos como huellas dactilares, reconocimiento facial, reconocimiento de voz.

Ejemplos de MFA

1. Autenticación con Contraseña y OTP (One-Time Password)

- **Descripción:** Contraseña (Algo que sabes) y OTP (Algo que tienes).
- **Ventajas:** Aumenta la seguridad ya que un atacante necesitaría tanto la contraseña como acceso al dispositivo físico.

2. Autenticación con Contraseña y Token de Hardware

- **Descripción:** Contraseña (Algo que sabes) y token de hardware como YubiKey (Algo que tienes).
- **Ventajas:** Alta seguridad debido a la necesidad de poseer el token físico.

3. Autenticación con Biometría y Contraseña

- **Descripción:** Contraseña (Algo que sabes) y huella dactilar, reconocimiento facial o de voz (Algo que eres).
- **Ventajas:** Añade una capa adicional de seguridad utilizando datos biométricos únicos del usuario.

4. Autenticación con Tarjeta Inteligente y PIN

- **Descripción:** Tarjeta inteligente (Algo que tienes) y PIN (Algo que sabes).
- **Ventajas:** Alta seguridad mediante la combinación de un dispositivo físico y un PIN.

Implementación y Buenas Prácticas

- **Configuración y Mantenimiento:** Actualizar regularmente las políticas de seguridad y la formación de los usuarios.
- **User Experience (UX):** Equilibrar la seguridad con la experiencia del usuario.
- **Redundancia:** Proporcionar métodos de autenticación alternativos.

6. Gestores de Contraseñas

¿Qué es un Gestor de Contraseñas?

Un gestor de contraseñas es una aplicación que almacena y organiza contraseñas de manera segura. No solo almacenan contraseñas, sino que también pueden generar contraseñas fuertes y únicas, completarlas automáticamente en sitios web y aplicaciones, y sincronizarlas entre dispositivos.

Funciones Clave

1. **Almacenamiento Seguro:** Mantiene todas las contraseñas cifradas en una bóveda digital.
2. **Generación de Contraseñas:** Crea contraseñas complejas y únicas para cada cuenta.
3. **Autocompletado:** Rellena automáticamente los campos de inicio de sesión en sitios web y aplicaciones.
4. **Sincronización:** Permite acceder a las contraseñas desde múltiples dispositivos.
5. **Autenticación Multifactor (MFA):** Añade una capa adicional de seguridad para acceder al gestor de contraseñas.

Por Qué Se Recomienda Usar un Gestor de Contraseñas

Seguridad Mejorada

- **Generación de Contraseñas Fuertes:** Los gestores de contraseñas generan contraseñas largas, complejas y únicas para cada cuenta.
- **Almacenamiento Cifrado:** Las contraseñas se almacenan de forma cifrada.

Conveniencia

- **Memorización de Múltiples Contraseñas:** Los usuarios solo necesitan recordar una contraseña maestra.
- **Acceso Rápido:** Los gestores de contraseñas pueden autocompletar información de inicio de sesión.

Prevención de Ataques Comunes

- **Phishing:** Verifican que las URLs coincidan con las guardadas.
- **Reuse de Contraseñas:** Evitan el uso de la misma contraseña en múltiples sitios.

Riesgos Asociados y Mitigación

Pérdida de la Contraseña Maestra

Impacto: La contraseña maestra es la clave para acceder a todas las contraseñas almacenadas. **Mitigación:**

- **Mecanismos de Recuperación:** Preguntas de seguridad, autenticación biométrica o claves de recuperación.
- **Copia de Seguridad de la Contraseña Maestra:** Guardar en un lugar seguro.
- **Autenticación Multifactor (MFA):** Añadir una capa extra de seguridad.

Compromiso del Gestor de Contraseñas

Impacto: Todas las contraseñas almacenadas podrían estar en riesgo. **Mitigación:**

- **Uso de Gestores de Contraseñas Confiables:** Seleccionar proveedores confiables.
- **Actualizaciones Regulares:** Mantener actualizado el gestor de contraseñas.
- **Revisión de Actividad:** Monitorear la actividad del gestor de contraseñas.

Recomendaciones de Gestores de Contraseñas

1. **LastPass:** Almacenamiento seguro, autocompletado, sincronización entre dispositivos, MFA.
2. **1Password:** Almacenamiento cifrado, generación de contraseñas, sincronización, MFA.
3. **Dashlane:** Almacenamiento seguro, generación de contraseñas, autocompletado, monitoreo de la web oscura.
4. **Bitwarden:** Almacenamiento cifrado, generación de contraseñas, sincronización, MFA.

7. Cómo Crear una Contraseña Segura Propia

Características de una Contraseña Segura

1. **Larga:** Al menos 12-16 caracteres.
2. **Compleja:** Combinación de letras mayúsculas y minúsculas, números y caracteres especiales.
3. **Única:** No reutilizar en múltiples cuentas.
4. **Impredecible:** No usar información personal fácilmente adivinable.

Pasos para Crear una Contraseña Segura

Paso 1: Selecciona una Frase Base

Empieza con una frase base fácil de recordar pero difícil de adivinar. Ejemplo: "Mi perro se llama Fido y tiene 4 años".

Paso 2: Utiliza las Iniciales

Toma las iniciales de cada palabra para crear una cadena de caracteres. Ejemplo: "MpdlFyta4a".

Paso 3: Añade Complejidad

Introduce mayúsculas, números y caracteres especiales. Ejemplo: "MpdL4FyTa!"

Paso 4: Asegúrate de la Longitud

Añade más caracteres si es necesario para alcanzar al menos 12-16 caracteres. Ejemplo: "MpdL4FyTa!2024".

Buenas Prácticas para Mantener la Seguridad de tus Contraseñas

1. **No Reutilizar Contraseñas:** Utilizar una contraseña única para cada cuenta.
2. **Utilizar un Gestor de Contraseñas:** Para generar y almacenar contraseñas seguras.
3. **Habilitar Autenticación Multifactor (MFA):** Añadir una capa extra de seguridad.
4. **Actualizar Regularmente las Contraseñas:** Especialmente después de posibles compromisos de seguridad.
5. **Evitar Información Personal:** No usar nombres, fechas de nacimiento u otra información fácilmente accesible.
6. **Monitorizar Actividad de la Cuenta:** Revisar regularmente la actividad para detectar accesos no autorizados.

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.

