AUTENTICACIÓN DE USUARIOS

ALBERTO DANIEL NUÑEZ AGURTO

AUTENTICACIÓN DE USUARIOS

¿Qué es la autenticación de usuarios?

La autenticación de usuarios es el proceso mediante el cual un sistema verifica la identidad de un usuario antes de concederle acceso a recursos o servicios. Este proceso es fundamental para la seguridad informática, ya que protege los datos y sistemas frente a accesos no autorizados.

Factores de Autenticación

Los factores de autenticación son métodos utilizados para verificar la identidad de un usuario. Se clasifican en las siguientes categorías:

1. Algo que el usuario sabe.
2. Algo que el usuario tiene.
3. Algo que el usuario es.
4. Algo que el usuario hace.
5. Ubicación del usuario.

Algo que el usuario sabe:

Este factor se basa en información conocida únicamente por el usuario. Es el método más tradicional y ampliamente utilizado.

Ejemplos:

- **Contraseñas:** Secuencias de caracteres que el usuario debe memorizar. Pueden ser simples (alfabéticas) o complejas (con combinación de caracteres especiales, números y mayúsculas).
- **PIN (Personal Identification Number):** Secuencia numérica, usualmente de 4 a 8 dígitos.
- **Respuestas a preguntas de seguridad:** Respuestas predefinidas a preguntas como "¿Cuál es el nombre de tu primera mascota?".

Ventajas:

- Fácil de implementar y de usar.
- No requiere hardware adicional.

Desventajas:

- Vulnerable a ataques de fuerza bruta, phishing y robo.
- Requiere políticas estrictas de renovación y complejidad para evitar la reutilización o exposición.

Algo que el usuario tiene

Este factor utiliza objetos físicos o digitales que el usuario debe poseer para autenticarse.

Ejemplos:

- **Tokens físicos:** Dispositivos generadores de códigos únicos, como RSA SecurID.
- **Tarjetas inteligentes (Smart Cards):** Incorporan chips que almacenan credenciales de usuario.
- **Dispositivos móviles:** Aplicaciones como Google Authenticator o Microsoft Authenticator generan códigos temporales.
- **Códigos enviados por SMS o correo electrónico:** Aunque populares, son vulnerables a ataques como SIM swapping.

Ventajas:

- Añade una capa extra de seguridad.
- Fácil integración con sistemas existentes.

Desventajas:

- Dependencia del dispositivo; si se pierde o es robado, el usuario queda bloqueado.

Algo que el usuario es.

Este factor depende de características biométricas únicas del usuario.

Ejemplos:

- **Huellas dactilares:** Común en smartphones y sistemas de acceso físico.
- **Reconocimiento facial:** Usado en dispositivos como iPhones (Face ID) y cámaras de seguridad.
- **Reconocimiento del iris:** Más preciso que el escaneo de retina, utilizado en sistemas de alta seguridad.
- **Reconocimiento de voz:** Implementado en asistentes como Alexa o Google Assistant.

Ventajas:

- Difícil de replicar o falsificar.
- Conveniencia, ya que no requiere recordar información o llevar dispositivos adicionales.

Desventajas:

- Requiere hardware especializado.
- Problemas de privacidad; los datos biométricos, si se filtran, son irreemplazables.
- Posibles errores de autenticación debido a condiciones ambientales o cambios físicos.

Algo que el usuario hace.

Se basa en el comportamiento o acciones del usuario, como patrones de uso o gestos.

Ejemplos:

- **Patrones de escritura:** Análisis de la velocidad y presión al teclear.
- **Gestos en dispositivos táctiles:** Reconocimiento de movimientos específicos en la pantalla.
- **Interacción con el mouse:** Seguimiento de movimientos y clics.

Ventajas:

- Proporciona autenticación continua mientras el usuario interactúa con el sistema.
- Difícil de replicar por atacantes.

Desventajas:

- Requiere algoritmos avanzados de aprendizaje automático.
- Puede tener alta tasa de falsos positivos o negativos en condiciones no ideales.

Ubicación del usuario.

Se utiliza el contexto geográfico del usuario para validar su autenticidad.

Ejemplos:

- **GPS:** Verificación de la ubicación a través de dispositivos móviles.
- **Dirección IP:** Comprobación de la ubicación geográfica aproximada.
- **Geofencing:** Definición de áreas específicas donde un usuario puede autenticarse.

Ventajas:

- Añade un nivel adicional de contexto y seguridad.
- Útil para detectar actividades sospechosas, como intentos de acceso desde países no permitidos.

Desventajas:

- La ubicación puede ser falsificada con herramientas como VPNs.
- No siempre es precisa, especialmente en redes móviles.

Soluciones más comunes de Autenticación de Usuarios

Autenticación por contraseña

Consiste en el uso de una cadena secreta (contraseña) que un usuario debe proporcionar para demostrar su identidad. Es el método más tradicional y extendido.

Ventajas:

- Fácil de implementar y utilizar.
- Compatible con casi todos los sistemas existentes.

Desventajas:

- Vulnerable a ataques como fuerza bruta, phishing y reutilización de contraseñas.
- Las políticas de contraseñas complejas pueden ser difíciles de gestionar.

Ejemplo práctico:

Un sistema solicita una contraseña con al menos 8 caracteres, incluyendo mayúsculas, números y símbolos. El usuario debe actualizar la contraseña cada 90 días.

Autenticación mediante tokens

Implica el uso de dispositivos físicos o digitales que generan códigos de un solo uso (One-Time Password, OTP). Los tokens pueden ser hardware, como dispositivos USB, o software, como aplicaciones en el móvil.

Ventajas:

- Más seguro que las contraseñas estáticas.
- Los OTP tienen un tiempo de validez limitado, reduciendo riesgos.

Desventajas:

- Requiere hardware o software adicional.
- Si el dispositivo se pierde o es robado, el acceso queda comprometido.

Ejemplo práctico:

Una aplicación bancaria solicita un código OTP generado por Google Authenticator al realizar transferencias.

Autenticación biométrica

Utiliza características físicas o comportamentales únicas del usuario, como huellas dactilares, reconocimiento facial o escaneo de iris.

Ventajas:

- Difícil de falsificar.
- Conveniente para el usuario, ya que no requiere recordar credenciales.

Desventajas:

- Requiere hardware especializado.
- Si los datos biométricos son comprometidos, no pueden ser cambiados.

Ejemplo práctico:

Un empleado utiliza un escáner de huellas dactilares para acceder a un sistema restringido.

Autenticación multifactor (MFA)

Combina dos o más factores de autenticación, como algo que el usuario sabe (contraseña), algo que tiene (token) y algo que es (biometría).

Ventajas:

- Significativamente más segura que los métodos de un solo factor.
- Reduce el impacto de ataques basados en un único punto de fallo.

Desventajas:

- Puede ser menos conveniente para los usuarios.
- Incrementa la complejidad de implementación y mantenimiento.

Ejemplo práctico:

Un usuario inicia sesión en su correo con una contraseña y confirma un OTP enviado a su móvil.

Certificados digitales

Los certificados digitales basados en infraestructura de clave pública (PKI) autentican usuarios mediante claves privadas almacenadas en dispositivos o tarjetas inteligentes.

Ventajas:

- Alta seguridad gracias al cifrado asimétrico.
- Escalable en entornos empresariales.

Desventajas:

- Requiere una infraestructura PKI compleja.
- La gestión de certificados (emisión, revocación) puede ser costosa.

Ejemplo práctico:

Un usuario utiliza un certificado digital para iniciar sesión en una intranet corporativa mediante su navegador.

Autenticación basada en contexto

Analiza el contexto de la autenticación, como ubicación, dispositivo, hora del día o comportamiento del usuario, para determinar si la solicitud es legítima.

Ventajas:

- Proporciona autenticación continua y adaptable.
- Puede bloquear actividades sospechosas automáticamente.

Desventajas:

- Requiere sistemas avanzados de monitoreo.
- Puede generar falsos positivos que afecten la experiencia del usuario.

Ejemplo práctico:

Un sistema bloquea un intento de inicio de sesión desde un país donde el usuario nunca ha estado.

Autenticación por Single Sign-On (SSO)

Permite a los usuarios acceder a múltiples aplicaciones con una sola autenticación inicial.

Ventajas:

- Simplifica la experiencia del usuario.
- Reduce la cantidad de contraseñas que los usuarios deben recordar.

Desventajas:

- Un fallo en el sistema SSO puede comprometer múltiples servicios.
- Dependencia de un único punto de autenticación.

Ejemplo práctico:

Un empleado inicia sesión en su cuenta de Google y obtiene acceso a Gmail, Drive y otros servicios sin necesidad de autenticarse de nuevo.

Autenticación mediante enlaces mágicos (Magic Links)

El usuario recibe un enlace único por correo electrónico para iniciar sesión sin necesidad de contraseñas.

Ventajas:

- Elimina la necesidad de recordar contraseñas.
- Menor riesgo de reutilización de contraseñas.

Desventajas:

- Depende de la seguridad del correo electrónico del usuario.
- Más lento que otros métodos de autenticación.

Ejemplo práctico:

Una plataforma de e-learning envía un enlace mágico para iniciar sesión después de solicitar el correo del usuario.

Autenticación con redes sociales (Social Login)

Permite a los usuarios iniciar sesión utilizando sus cuentas de redes sociales como Facebook, Google o LinkedIn.

Ventajas:

- Experiencia rápida y sencilla para los usuarios.
- Menor probabilidad de abandono durante el registro.

Desventajas:

- Dependencia de proveedores externos.
- Cuestiones de privacidad relacionadas con el intercambio de datos.

Ejemplo práctico:

Un sitio web permite iniciar sesión con la cuenta de Google del usuario.

Autenticación basada en hardware (U2F y FIDO)

Requiere el uso de dispositivos de hardware específicos, como llaves de seguridad USB (p. ej., YubiKey).

Ventajas:

- Proporciona autenticación robusta frente a ataques de phishing.
- Fácil de usar una vez configurado.

Desventajas:

- Requiere hardware adicional.
- El coste inicial puede ser un obstáculo.

Ejemplo práctico:

Un administrador de sistemas utiliza una llave USB FIDO2 para autenticarse en un servidor crítico.

CONTROL DE ACCESO

Modelos de control de acceso

- Modelo Bell-LaPadula (BLP)
- Modelo Biba
- Modelo Clark-Wilson

Modelo Bell-LaPadula (BLP)

Propósito: Garantizar la confidencialidad de los datos en sistemas clasificados, como los utilizados en entornos militares y gubernamentales.

Principios fundamentales:

- **No-Read-Up (NRU):** Un usuario con un nivel bajo de autorización no puede acceder a datos en un nivel más alto (por ejemplo, un empleado con autorización "Confidencial" no puede leer información "Secreta").
- **No-Write-Down (NWD):** Un usuario con un nivel alto de autorización no puede escribir datos en un nivel más bajo, evitando la filtración de información sensible.

Aplicaciones: Usado para proteger sistemas sensibles donde el acceso a la información debe ser estrictamente controlado

Modelo Biba

Propósito: Asegurar la **integridad** de los datos, es decir, prevenir la corrupción o modificación no autorizada de información.

Principios fundamentales:

- **No-Read-Down:** Los usuarios no pueden leer datos de niveles inferiores, para evitar contaminación con información no confiable.
- **No-Write-Up:** Los usuarios no pueden escribir en niveles superiores, previniendo la contaminación de datos críticos.

Uso práctico: Ideal para sistemas financieros o comerciales donde la integridad de las transacciones es prioritaria.

Modelo Clark-Wilson

Propósito: Mantener la integridad de los datos mediante un enfoque en transacciones autorizadas.

Características:

- Impone el uso de **programas autorizados** para modificar datos.
- Introduce la separación de funciones para evitar conflictos de interés.

Ejemplo práctico: Sistemas bancarios que requieren múltiples autorizaciones para transferencias importantes.

Tipos de control de acceso

- DAC (Discretionary Access Control).
- MAC (Mandatory Access Control).
- RBAC (Role-Based Access Control).
- ABAC (Attribute-Based Access Control).

DAC (Discretionary Access Control)

El acceso está determinado por políticas de seguridad centralizadas.

Ventajas:

- Mayor seguridad en entornos sensibles.

Desventajas:

- Menos flexible.
- Requiere una planificación cuidadosa.

Ejemplo práctico: Sistemas clasificados donde los permisos se basan en niveles de seguridad.

MAC (Mandatory Access Control)

El acceso está determinado por políticas de seguridad centralizadas.

Ventajas:

- Mayor seguridad en entornos sensibles.

Desventajas:

- Menos flexible.
- Requiere una planificación cuidadosa.

Ejemplo práctico: Sistemas clasificados donde los permisos se basan en niveles de seguridad.

Modelo Basado en Roles (RBAC)

Propósito: Simplificar la gestión de permisos al asignarlos según roles predefinidos en la organización.

Ventajas:

- Escalable y fácil de administrar en organizaciones grandes.
- Reduce errores humanos al eliminar permisos individuales.

Ejemplo: Un empleado en el rol de "Contador" tiene acceso a sistemas financieros, pero no a sistemas de recursos humanos.

ABAC (Attribute-Based Access Control)

Las decisiones de acceso se basan en un conjunto de atributos (usuario, recurso, contexto).

Ventajas:

- Mayor granularidad y flexibilidad.
- Ideal para entornos dinámicos como la nube.

Ejemplo práctico: Permitir que un empleado acceda a datos solo durante su horario laboral y desde dispositivos autorizados.

Seguridad física

Seguridad Física

La seguridad física se refiere a las medidas implementadas para proteger los activos físicos, las instalaciones y los equipos de una organización contra amenazas como acceso no autorizado, vandalismo, robo, desastres naturales, entre otros. En este contexto, las estrategias de seguridad física son fundamentales para proteger también los datos, ya que los dispositivos que almacenan o procesan información están físicamente ubicados en un espacio.

Principales componentes de la seguridad física

- **Control de acceso físico:** Uso de sistemas como cerraduras electrónicas, tarjetas de proximidad, lectores biométricos, y barreras físicas.
- **Videovigilancia:** Cámaras de seguridad (CCTV) y sistemas de monitoreo remoto.
- **Protección contra desastres:** Sistemas contra incendios, detectores de humo, y soluciones para evitar daños por inundaciones o terremotos.
- **Guardias de seguridad y políticas de supervisión:** Personal capacitado para gestionar el acceso y supervisar las instalaciones.
- **Respaldo de energía y redundancia:** Generadores, baterías de respaldo y estrategias para garantizar la continuidad del negocio.

Modelo de Seguridad de Google

Google implementa un enfoque avanzado y altamente seguro en la protección de su infraestructura. Este modelo de seguridad está diseñado para abordar tanto amenazas físicas como cibernéticas y se basa en múltiples capas de defensa.

Principales elementos del modelo de seguridad de Google

Infraestructura altamente controlada:

- Los centros de datos de Google están ubicados estratégicamente en todo el mundo y cuentan con sistemas avanzados de control de acceso físico. Esto incluye medidas como cercas perimetrales, escáneres biométricos, detectores de metales y vigilancia continua.
- El acceso a las instalaciones está estrictamente limitado a personal autorizado.

Principio de defensa en profundidad:

- Se implementan varias capas de protección en los sistemas físicos y digitales. Cada capa debe ser superada para comprometer la seguridad del sistema en su conjunto.
- Ejemplo: Incluso si un atacante logra acceder físicamente a un dispositivo, los datos almacenados en él están cifrados y no pueden ser leídos sin las claves adecuadas.

Protección de datos y cifrado:

- Todos los datos que Google maneja están protegidos mediante cifrado tanto en tránsito como en reposo.
- Los sistemas están diseñados para minimizar la exposición de datos sensibles incluso en caso de fallas.

Seguridad del hardware personalizado:

- Google diseña y fabrica su propio hardware de servidor, lo que permite un control absoluto sobre la cadena de suministro y la integridad del hardware.
- Esto asegura que no existan componentes comprometidos o vulnerabilidades intencionales.

Respuesta ante incidentes:

- Los centros de datos de Google cuentan con equipos especializados en la gestión de incidentes de seguridad, capaces de responder rápidamente a cualquier amenaza detectada.

Modelo de Seguridad de Google

Protocolos criptográficos y sistemas de autenticación

Protocolos criptográficos

Los protocolos criptográficos son un conjunto de reglas matemáticas y procedimientos diseñados para garantizar la seguridad de la comunicación y el intercambio de información en entornos digitales. Se utilizan para proteger datos durante su transmisión o almacenamiento y son fundamentales para sistemas de autenticación que verifican la identidad de usuarios y dispositivos

TLS/SSL (Transport Layer Security / Secure Sockets Layer)

Primera generación: Cifrado básico

- Los primeros algoritmos criptográficos, como el **Cifrado César** o el **Cifrado de Vigenère**, se enfocaban en sustituir o permutar caracteres. Estos eran efectivos para proteger mensajes simples, pero vulnerables a métodos de análisis.
- Durante la Segunda Guerra Mundial, el uso de máquinas como la **Enigma** marcó un avance significativo.

Cifrado moderno: Simétrico y asimétrico

- En el siglo XX, surgieron estándares como el **DES (Data Encryption Standard)**, reemplazado luego por el **AES (Advanced Encryption Standard)** debido a las mayores demandas de seguridad.
- La invención del cifrado asimétrico (como **RSA**) permitió compartir claves públicas para cifrar datos, sin comprometer la clave privada utilizada para descifrar.

Protocolos de transporte seguro

- Protocolos como **SSL (Secure Sockets Layer)** y su sucesor, **TLS (Transport Layer Security)**, establecieron comunicaciones seguras en redes públicas como Internet.
- La criptografía moderna incluye algoritmos resistentes a computadoras cuánticas, como **lattice-based cryptography**.

Nuevas tecnologías y enfoques

- Protocolos recientes como **QUIC** (usado por Google) incorporan cifrado avanzado para mejorar la velocidad y seguridad de las conexiones.
- Los sistemas distribuidos y blockchain también emplean criptografía para garantizar la integridad y autenticidad de datos.

TLS/SSL y tecnologías de VPN

TLS y SSL son protocolos criptográficos diseñados para proporcionar **confidencialidad, integridad** y **autenticación** en la comunicación entre aplicaciones y servidores.

Usos comunes:

- Navegación segura (HTTPS).
- Transferencia de datos (IMAPS, SMTPS, FTPS).

Funcionamiento:

- **Cifrado de sesión**: Protege los datos mediante claves temporales generadas durante la conexión.
- **Certificados digitales**: Utilizados para verificar la identidad del servidor y establecer confianza.

VPN (Virtual Private Network)

Una VPN extiende redes privadas sobre una infraestructura pública, como Internet, utilizando túneles seguros que cifran el tráfico entre los puntos finales.

Protocolos de VPN comunes:

- **IPsec (Internet Protocol Security)**: Proporciona autenticación y cifrado a nivel de red.
- **OpenVPN**: Basado en SSL/TLS, ofrece una implementación flexible y segura.
- **WireGuard**: Más reciente, se destaca por su simplicidad y rendimiento.

Beneficios:

- Protección frente a espionaje y rastreo.
- Acceso remoto seguro para trabajadores y equipos distribuidos.