Autorización y Autenticación

Angel Martinez

angel.martinez@wizeline.com

Acerca de mí

Angel Martínez

Staff Software Engineer

- 8 años de experiencia
- 5 años en Wizeline
- Diseño de arquitectura y soluciones

Puntos importantes

Identifícate en Zoom utilizando tu nombre y apellido.

Mantén tu micrófono apagado durante el transcurso de la sesión.

Utiliza el chat para hacer tus preguntas durante la sección de Q&A.

Procura enfocar tus preguntas al tema presentado.

Apaga tu cámara en caso de tener problemas con tu conexión.

Código de conducta

Sé respetuoso, no hay malas preguntas o ideas.

Sé cordial y paciente.

Sé cuidadoso con tus palabras.

Objetivo

Al final de esta sesión podrás:

- Reconocer la importancia y la diferencia entre autenticación y autorización.

Tabla de Contenidos

Introducción

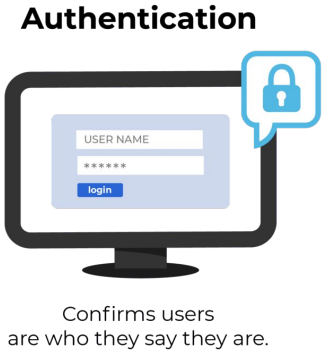
En 2018, Cambridge Analytica obtuvo información personal sin consentimiento de los usuarios.

Tabla de Contenidos

Autenticación

¿Qué es autenticación?

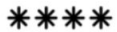
- Mecanismo seguro para determinar que **un usuario es quien dice ser** a través de la validación de **credenciales.**
- La validación puede ser mediante:
  - Contraseñas (`Pa$$w0Rd!`)
  - PIN (1234)
  - Contraseña de un solo uso (OTP) (123456)
  - Información biométrica (Huella dactilar)
  - Pregunta de seguridad (¿Cuál es el nombre de tu mascota?)



Métodos de autenticación

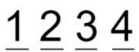
Factor de conocimiento

(Algo que sabes)



Password

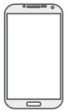
Security Question



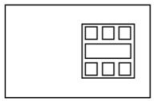
PIN

Factor de posesión

(Algo que posees)



Smartphone



Smart Card

Hardware Token

Factor de inherencia

(Algo que eres)

Fingerprint

Retina Pattern

Face Recognition

Tipos de autenticación

2FA

- Autenticación de dos factores (2FA)
- Capa extra de seguridad
- **Contraseña + factor independiente**
  - Código via correo
  - Mensaje de texto
  - PIN
  - OTP
  - Pregunta de seguridad
  - Hardware
  - Factor biométrico
  - Push notification

MFA

- Autenticación multi factor (MFA)
- **Contraseña + factores independientes**
- **Autenticación robusta** comparada con 2FA

SSO

- **Múltiple login** con **autenticación única**
- Se establece confianza mediante un Proveedor de Identidad (IdP) y un Proveedor de Servicio (SP)
- Tipos de SSO:
  - SAML
  - OAuth (Open Authentication)
  - OIDC (OpenID)
  - Kerberos

Tipos de autenticación

Federado

- Similar a SSO
- Acceso a un **grupo federado** a través de **múltiples organizaciones y dominios**
- *Cada SSO es una instancia de un acceso federado, pero no cada accesso federado is una instancia de SSO*

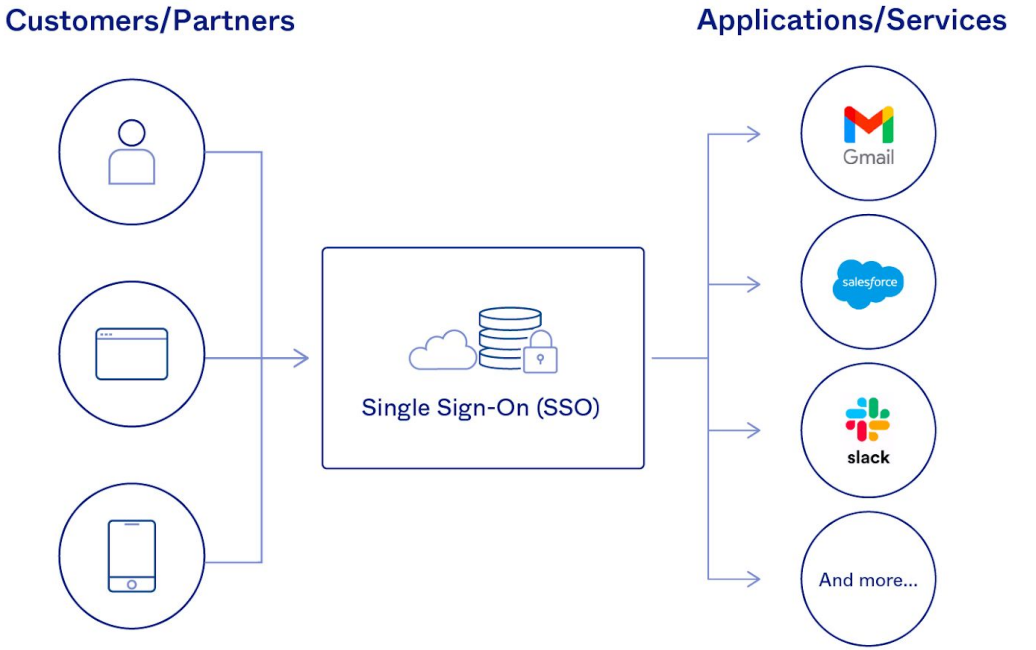
SSH llave pública

- Credenciales SSH
- Ofrece cifrado robusto
- Es un SSO aplicado a servidores SSH
- Autenticación ***Passwordless***
- Llaves SSH
  - Pública
  - Privada

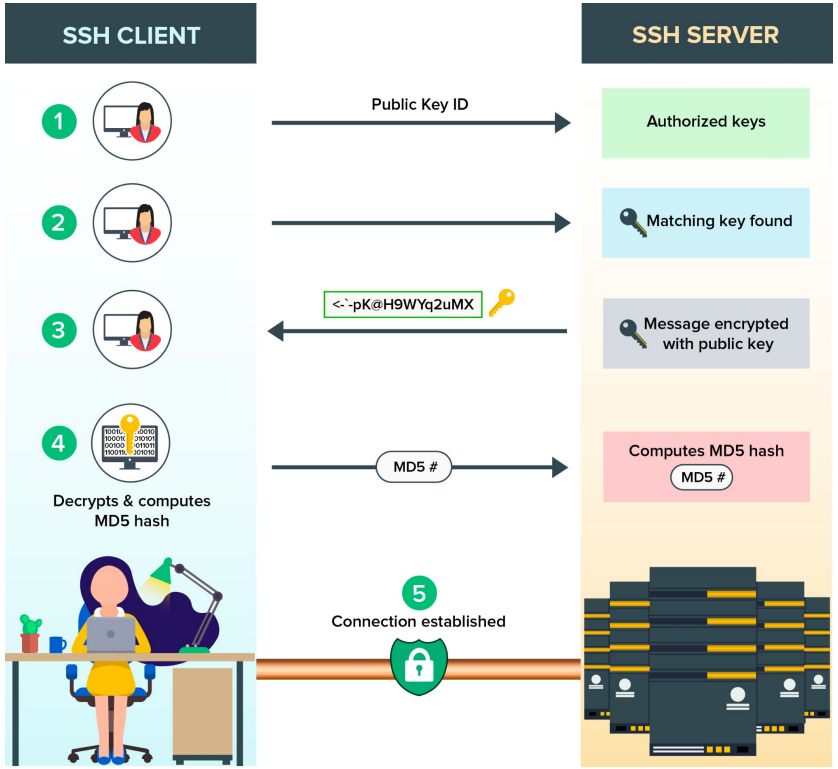
Certificado

- Demostrar la identidad mediante documentos electrónicos (**certificados digitales**)
- Confirmar la propiedad de una clave privada
- Un certificado digital contiene:
  - Datos de identificación
  - Información sobre la clave pública
  - Firma digital derivada del PK de la autoridad de certificación (CA)

SSO/Federado



SSH llave pública



Certificado

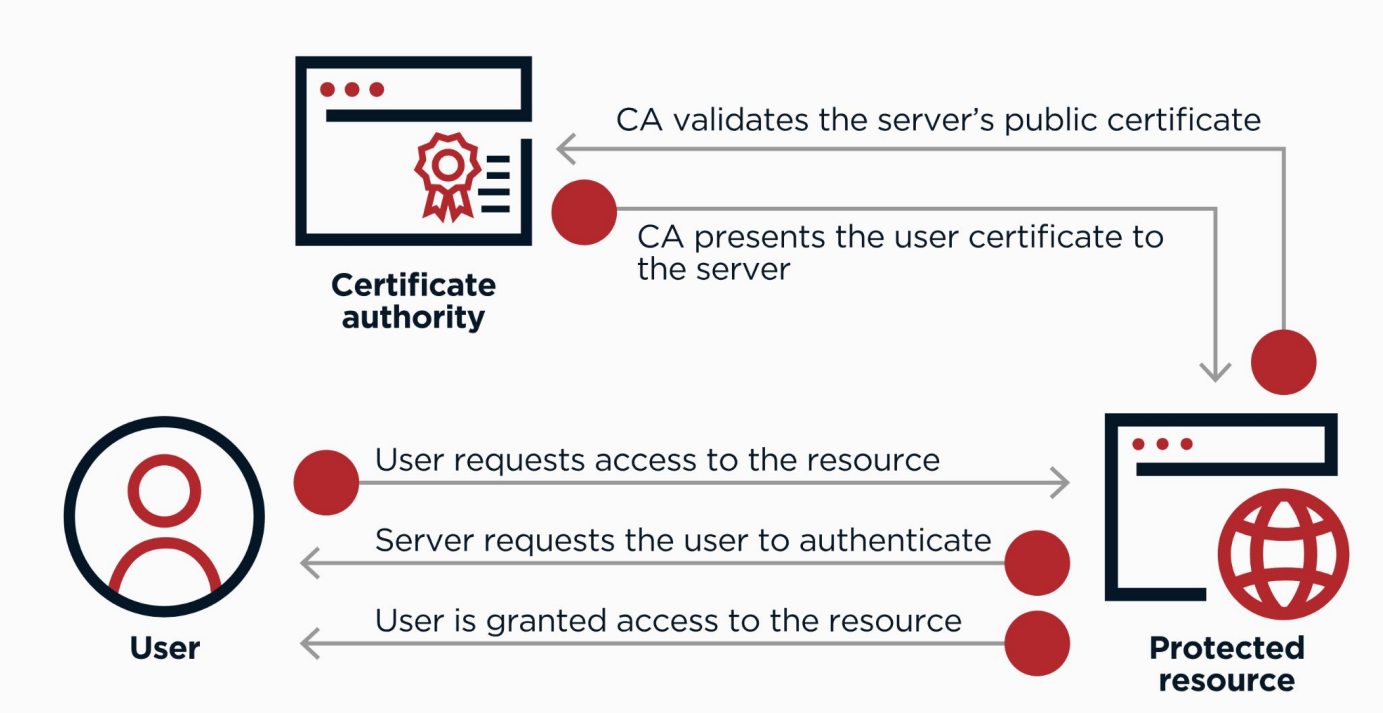
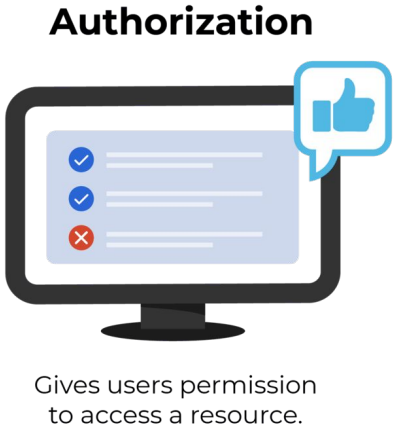


Tabla de Contenidos

Autorización

¿Qué es autorización?

- Mecanismo seguro para validar las **capacidades del usuario,** mediante el uso de **políticas, permisos** y **roles.**
- Determina el acceso a **aplicaciones, archivos, características, datos** y **recursos** a los cuáles el usuario tiene acceso.
- **Es lógica de negocio** no visible al usuario
- *No puede existir autorización sin autenticación.*



Métodos de autorización

RBAC

- Control de acceso basado en **roles**
- Conjunto de permisos asignados a usuarios o grupos
- **Ejemplo:**
  Un **administrador** solamente puede ver la vista de reportes

ABAC

- Control de acceso basado en **atributos**
- Conjunto de permisos basado en características o propiedades
- **Ejemplo:**
  Usuarios que **son SRE** son capaces de desplegar nuevas versiones

-

Métodos de autorización

PBAC

- Control de acceso basado en **políticas**
- Conjunto de permisos asignados bajo condiciones específicas
- **Ejemplo:** Usuarios anónimos **pueden** ver productos **pero no** comprarlos

PAM

- Administración de acceso para usuarios privilegiados
- Capa adicional de seguridad en caso de ataque
- **Ejemplo:** El usuario **root** de Linux

Tabla de Contenidos

Ataques y prevención

Consecuencias

- Acceso no autorizado
- Violación de la privacidad
- Robo de información sensible
- Pérdida de reputación y confianza
- Vulnerable a ataques
- Responsabilidad legal y regulaciones incumplidas

Ataques

SQL Injection

- Conversión de ***inputs*** de formularios a ataques de inyección SQL para manipulación de la base de datos

XSS injection

- Cross-Site Scripting (XSS) inyección maliciosa de código o scripts en la aplicación

Acceso no autorizado

- Acceso a información, recursos y funcionalidades restringidas

Ataques

Secuestro de sesión (Hijacking)

- Acceso a sesiones de usuarios mediante una sesión legítima
- Actuar en nombre del usuario sin su consentimiento

Ataques de fuerza bruta

- Identificación de contraseñas de usuario mediante fuerza bruta

Ataques de diccionario

- Adivinación de contraseñas débiles o predecibles basado en una lista existente o diccionario

Ataques

Elevación de privilegios

- Intercambio de roles y permisos para obtener acceso a recursos restringidos

Suplantación de identidad (Identity Spoofing)

- Realización de acciones en nombre de un usuario sin consentimiento previo

Exposición de información confidencial

- Acceso a información sensitiva para divulgación sin autorización

Ataques

Manipulación de parámetros

- Manipulación de parámetros en peticiones HTTP para acceso a recursos restringidos

Omisión de autenticación (Authentication Bypass)

- Acceso a la aplicación sin proporcionar credenciales

Inundación (Flooding)

- Solicitud masiva para agotar los recursos del servidor hasta tirarlo o afectar el rendimiento

Técnicas de prevención

Acceso no autorizado/ Escalación de privilegios

- Implementación de controles de autenticación así como controles de acceso a recursos, funciones e información
- **ASP.NET Identity** para gestión de roles y políticas

Inyección de datos

- Uso de consultas parametrizadas o procedimientos almacenados
- Evitar la concatenación de cadenas
- Validación de inputs
- **Entity Framework**

Secuestro de sesiones

- Implementación de sesiones seguras
- Tokens anti-falsificación (CSRF)
- Tiempo de expiración
- **ASP .NET Application Security**

Técnicas de prevención

Mensajes genéricos

- Mostrar mensajes genéricos en lugar de indicar si un usuario existe o no o si la contraseña ingresada no es correcta

Ataques de fuerza bruta

- Bloqueos temporales
- Conteo de inicios fallidos
- Implementación de CAPTCHAs

Suplantación de identidad

- Implementación 2FA
- Indicar a los usuarios la importancia de mantener seguras sus credenciales
- **Google Authenticator**
- **ASP.NET Identity + Authy**

Técnicas de prevención

Exposición de información confidencial

- Cifrado de información almacenada en base de datosUso de conexiones seguras
- **Namespace System.Security. Cryptography**

Ataque de manipulación de parámetros

- Validación de parámetros así como autorización de los mismo antes de la ejecución de código

-

Tabla de Contenidos

Ejercicio de código

Recapitulación

Hemos hablado acerca de:

- Autorización
- Autenticación
- Consecuencias
- Ataques comunes
- Técnicas de prevención
- Ejemplo

¿Preguntas?

Retroalimentación

Déjanos saber tu retroalimentación

Gracias.