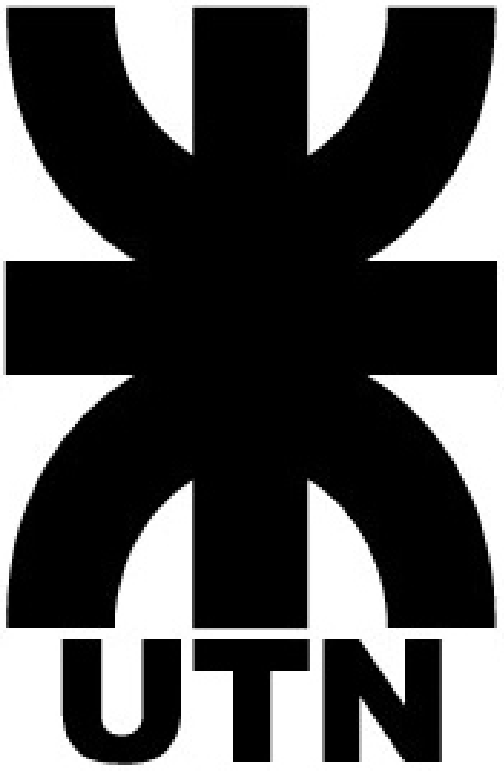
Actividad Semana 4

Autenticación-Autorización

UTN FRC - Integración de Aplicaciones en Entorno Web - 5K4



Cátedra: 5K4
Profesores:

- María Soledad Romero
- Rubén Aníbal Romero

Estudiante:

- 85828 Gutierrez, Santiago

Fecha: 08/09/2024

Índice

Conceptos básicos

Autenticación

La autenticación es el proceso mediante el cual se confirma la identidad de un usuario o dispositivo. Esto se realiza mediante una prueba de esta identidad, es decir, un **factor de autorización.** Este puede ser simple, autenticación de dos factores o de múltiples factores.

Autorización

La autorización es el proceso mediante el cual se verifica el derecho de acceso de un usuario a distintos recursos, o que acciones puede realizar. Es importante destacar que la autorización no implica la verificación de la identidad del usuario, aunque el mecanismo utilizado para manejar la autorización pueda contener información sobre la identidad del usuario.

Mecanismos

Autenticación

- Autenticación Multifactor (MFA): Requiere múltiples formas de verificación (como contraseña y código enviado al móvil) para acceder a un recurso, aumentando la seguridad.
- Sin Contraseña (Passwordless): Utiliza enlaces mágicos enviados por correo electrónico para acceder a recursos sin necesidad de una contraseña.
- Por Redes Sociales: Permite iniciar sesión usando cuentas de redes sociales como Facebook, Twitter o Google, facilitando el acceso sin registro manual.
- Autenticación API: Verifica la identidad del usuario a través de métodos como autenticación básica por HTTP, Core API y OAuth.
- Autenticación Biométrica: Utiliza huellas dactilares para validar la identidad, común en lugares de trabajo y dispositivos móviles.

Autorización

- Autorización HTTP: Requiere que el usuario proporcione nombre de usuario y contraseña; el servidor responde con un mensaje de "Unauthorized" y detalles para la autorización.
- Autorización API: Usa una clave API y un token oculto para autenticar y autorizar el acceso a recursos.
- OAuth 2.0: Permite a las APIs acceder a recursos del sistema con el consentimiento del usuario, delegando acciones específicas.
- Autorización JWT: Transmite datos de forma segura usando un par de claves pública-privada, soportando autenticación y autorización.

Tipos

Autenticación

- Autenticación Basada en Contraseña: Ingreso de nombre de usuario y contraseña.
- Autenticación Basada en Token: Uso de un token para acceder a los recursos.
- Autenticación Biométrica: Uso de datos biométricos como huellas o rostro.
- Autenticación Multifactor (MFA): Combina varios métodos de autenticación.

Autorización

- Autorización Basada en Roles (RBAC): Permisos asignados según el rol del usuario.
- Autorización Basada en Atributos (ABAC): Permisos basados en atributos del usuario y contexto.
- Autorización Basada en Políticas (PBAC): Permisos basados en políticas definidas.
- Listas de Control de Acceso (ACL): Permisos específicos para cada recurso y usuario.

Protocolos

Para realizar la autorización y autenticación, existen diversos protocolos. Entre ellos se encuentran LDAP, Kerberos, SAML and SSO y OAuth.

LDAP (Light Weight Directory Access Protocol)

- Propósito: Acceso y autenticación de datos en directorios activos.
- Almacenamiento: Datos en formato jerárquico.
- Autenticación: Se usan credenciales para acceder a recursos.

KERBEROS

- Propósito: Autenticación segura en redes inseguras.
- Entidades: Cliente, servidor, servidor de distribución de claves.
- Proceso: Solicitud de acceso, emisión de tickets, autenticación mutua.

SAML (Simple Assertion Markup Language)

- Propósito: Intercambio de datos de autenticación entre proveedores de identidad y servicios.
- Entidades: Proveedor de identidad (IDP), proveedor de servicios (SP), agente de usuario.
- Proceso: Solicitud de acceso, autenticación, y uso de tokens firmados para acceder a recursos.

OAuth (Open Authorization)

- Propósito: Autorización para acceder a recursos en nombre de un usuario.
- Proceso: Solicitud de acceso, autenticación del usuario, obtención de tokens para acceder a recursos.

Empresas

Existen varias empresas que ofrecen su infraestructura para proveer servicios de autenticación y autorización. Ejemplos de estas son:

- Okta: Ofrece servicios de gestión de identidades y accesos, incluyendo autenticación multifactor y soluciones de Single Sign-On (SSO).
- Auth0: Proporciona una plataforma de autenticación y autorización que soporta múltiples métodos de autenticación y personalización.
- Microsoft Azure Active Directory: Ofrece gestión de identidades y accesos con soporte para autenticación multifactor y acceso condicional.
- Ping Identity: Proporciona soluciones de identidad y acceso para autenticación, autorización y gestión de identidades en la nube.
- OneLogin: Ofrece soluciones de gestión de identidades y accesos, incluyendo autenticación multifactor y administración de acceso a aplicaciones.

Multifactor

La autenticación multifactor busca resolver el dilema que surge cuando un factor de autenticación se encuentra comprometido o roto. Esto lo hace mediante la utilización de métodos de autenticación de categorías independientes de credenciales para verificar la identidad del usuario. Estas categorías independientes son:

- Lo que el usuario **sabe**: **factor de conocimiento.**
- Lo que **tiene** el usuario: **factor de posesión.**
- Qué **es** el usuario: **factor de inherencia.**

Al basarse MFA en dos o más factores de autenticación de categorías independientes, al estar comprometido uno, todavía está presente al menos una barrera o más que debe romper el atacante previó a cumplir con su objetivo.

Bibliografía

Auth0. (s.f.). *Autenticación frente a autorización*. Auth0. https://auth0.com/es/intro-to-iam/authentication-vs-authorization

Fernández, L. (2023, febrero 13). *Qué significa autenticación y la autorización*. RedesZone. https://www.redeszone.net/tutoriales/seguridad/diferencias-autenticacion-autorizacion/

ComputerWeekly. (s.f.). *Autenticación multifactor o MFA*. https://www.computerweekly.com/es/definicion/Autenticacion-multifactor-o-MFA

Goel, U. (2022, mayo 16). *Things to know about authentication/authorization protocols*. Medium. https://medium.com/@surfd1001/things-to-know-about-authentication-authorization-protocols-addff3654d97