¿Qué es la autenticación (Authentication)?

> **En resumen**: La autenticación (Authentication) responde a la pregunta “¿Qué identidad posees?”

Aquí hay algunos ejemplos típicos de autenticación (Authentication):

- Inicio de sesión con nombre de usuario y contraseña
- Inicio de sesión social (por ejemplo, Iniciar sesión con Google)
- Máquina a máquina (Machine-to-machine) autenticación (Authentication) (por ejemplo, API keys)

No usamos la frase **“¿Quién eres?”** porque:

- En el ámbito de Gestión de identidades y access (Identity and access management, IAM) , la autenticación (Authentication) se trata de verificar la propiedad de una identidad, no de identificar a la persona o entidad. Por ejemplo, cuando uno de tus familiares utiliza tus credenciales para acceder a tu cuenta, no son tú, pero la identidad para el sistema es la misma.
- La identidad puede ser un usuario, un servicio o un dispositivo. Por ejemplo, un servicio puede autenticarse ante otro servicio utilizando API keys.

Diferencia entre autenticación (Authentication) y autorización (Authorization)

Estos dos términos a menudo se confunden, pero son fundamentalmente diferentes: Autorización (Authorization) responde a la pregunta “¿Qué puedes hacer?”. Además, la autenticación (Authentication) es un requisito previo para la autorización (Authorization) ya que el sistema necesita conocer la identidad antes de decidir qué acciones puede realizar.

Factores de autenticación (Authentication)

La autenticación (Authentication) se puede realizar utilizando uno o más factores. Aquí hay algunos factores comunes:

- **Factor de conocimiento**: Algo que sabes (por ejemplo, contraseña, PIN)
- **Factor de posesión**: Algo que tienes (por ejemplo, smartphone, token de seguridad)
- **Factor de inherencia**: Algo que eres (por ejemplo, huella dactilar, reconocimiento facial)

Autenticación multifactor (Multi-factor authentication, MFA) es una práctica común que combina múltiples factores para aumentar la seguridad. Por ejemplo, cuando inicias sesión en tu cuenta bancaria, es posible que necesites proporcionar una contraseña (factor de conocimiento) y un código único de una aplicación autenticadora (factor de posesión).

Llave de acceso (Passkey) es un factor de autenticación (Authentication) moderno que puede combinar múltiples factores y es resistente a ataques de phishing.

Marcos de autenticación (Authentication) (protocolos)

En lugar de construir un sistema de autenticación (Authentication) propio, se recomienda usar marcos y protocolos establecidos ya que han sido probados en batalla y revisados por expertos en seguridad. Existen diversos marcos y protocolos de autenticación (Authentication) que definen cómo se debe realizar la autenticación (Authentication). Dos comunes son:

- OpenID Connect (OIDC) : Una capa de identidad construida sobre OAuth 2.0 que agrega capacidades de autenticación (Authentication). Es relativamente moderno y ampliamente utilizado para nuevas aplicaciones.
- Lenguaje de marcado para declaraciones de seguridad (Security Assertion Markup Language, SAML) : Un protocolo para el intercambio de datos de autenticación (Authentication) y autorización (Authorization) entre partes. Se utiliza comúnmente en entornos empresariales.

La elección del marco depende de tu caso de uso y requisitos. Para nuevas aplicaciones, se recomienda OIDC debido a su diseño moderno y soporte para JSON Web Token (JWT) .

Sin embargo, trabajar directamente con estos protocolos puede ser complejo y llevar tiempo. Ambos protocolos tienen curvas de aprendizaje pronunciadas y requieren una implementación cuidadosa para garantizar la seguridad. En su lugar, usar un Proveedor de identidad (Identity

provider, IdP) que apoye o esté construido sobre estos protocolos puede simplificar en gran medida el proceso de autenticación (Authentication). Un buen proveedor de identidad también proporcionará características adicionales como Autenticación multifactor (Multi-factor authentication, MFA) y Inicio de sesión único (Single Sign-On, SSO) para tus necesidades futuras.

Revisión #2
Creado 2024-11-11 18:07:15 UTC por Marluan Espiritusanto
Actualizado 2024-11-13 14:07:04 UTC por Marluan Espiritusanto