Nombre: Jorge Manuel Oyoqui Aguilera
Matrícula: A01711783
Fecha: 28/04/2025
Materia: Construcción de Software y Toma de Decisiones
Grupo: 501
Profesores: Enrique Alfonso Calderón Balderas,
Denisse L. Maldonado Flores, Alejandro Fernández Vilchis

Tecnológico de Monterrey

Preguntas Laboratorio 18

- **¿Qué otras formas de autentificación existen?**

  Algunos ejemplos de otros métodos de autenticación serían:

  1. **Autenticación basada en contraseña (o Password-based Auth):** Qué es el método más tradicional, donde el usuario proporciona una contraseña que se compara con el valor almacenado en la base de datos que suele estar cifrado. Sólo que este método tiene varias desventajas, pues a las personas les resulta difícil crear y recordar su contraseña, aparte de que los hackers utilizan muchas tácticas para adivinar o robar contraseñas, por lo que aparte de este método se implementan otros para hacer este proceso de seguridad aún más seguro.

  2. **Autenticación por biometría:** Se basa en la lectura de alguna característica física única del individuo, como una huella dactilar, un escaneo del iris o incluso la voz. Esta es una forma muy efectiva para que los sistemas validen que la persona que solicita acceso es quien dice ser. (André Bessa, 2023).

  3. **Autenticación de dos factores:** La meta de este tipo de autenticación es agregar una capa más de seguridad para acceder a la aplicación o página. Por ejemplo, en un primer paso la aplicación solicita un pin. Además, reenvía un código que complementará la autenticación por algún canal de comunicación del usuario, como el número celular o el correo electrónico. Pero se debe tomar en cuenta que el usuario, para este tipo de autenticación, debe tener disponible el canal adicional en el proceso de inicio de sesión, como un celular por ejemplo para recibir algún código de verificación. (André Bessa, 2023).

  4. **Autenticación por token:** Aquí, tanto el dispositivo como el sistema generan un nuevo número singular llamado PIN temporal de un solo uso (TOTP) cada 30 segundos. Si los números coinciden, el sistema comprueba que el usuario tiene el dispositivo y se acepta la autenticación. (Microsoft, S.F).

5. **Autenticación basada en certificado:** Es un método cifrado que permite que los dispositivos y las personas se identifiquen en otros dispositivos y sistemas. Dos ejemplos frecuentes son las tarjetas inteligentes y el envío de certificados digitales a una red o servidor por parte del dispositivo de un empleado. (Microsoft, S.F).

6. **Contraseña de un solo uso:** Las contraseñas de un solo uso (OTP) son códigos generados para un evento de inicio de sesión específico que expiran al poco de expedirse. Se entregan mediante mensaje SMS, correo electrónico o un token de hardware. (Microsoft, S.F).

7. **Autenticación por voz:** donde la persona que intenta acceder a un servicio recibe una llamada telefónica en la que se les solicita introducir un código o identificarse de forma verbal.

8. **Autenticación multifactor:** Donde, para mejorar la seguridad, se implementan dos o más de los métodos mencionados anteriormente. Un procedimiento adecuado es requerir dos de los siguientes métodos: Algo que el usuario conozco, como una contraseña; algo que el usuario posea, como un dispositivo de confianza que no se duplique fácilmente (como un teléfono o un token de hardware); o algo que el usuario sea, como una huella dactilar o un escáner facial.

André Bessa (2023). "Tipos de Autenticación: Contraseña, Token, JWT, Dos Factores, Más.". Recuperado de: https://www.aluracursos.com/blog/tipos-de-autenticacion

Microsoft (S.F.). "¿Qué es la autenticación?". Recuperado de: https://www.microsoft.com/es-mx/security/business/security-101/what-is-authentication