UNIVERSIDAD
COMPLUTENSE
MADRID

Autenticación

Gestión de la Información en la Web
Enrique Martín - emartinm@ucm.es
Grados de la Fac. Informática

¿Qué es?

- La autenticación es el acto de **comprobar** que un **usuario** es exactamente quien dice ser.
- Es una acción que se produce continuamente en aplicaciones web y de escritorio, *apps*, etc.
- Se pueden seguir diferentes enfoques:
  - Algo que sabes
  - Algo que tienes
  - Algo que eres

Algo que sabes

- Es el método preferido, y el que más veces habréis utilizado: preguntar al usuario algún **secreto** que **únicamente él debería conocer**.
- El ejemplo más conocido son las contraseñas o las preguntas de verificación (*¿Dónde nació tu abuela?*).
- Tiene aspectos positivos y negativos.

Algo que sabes

- El principal aspecto **positivo** es su **sencillez**:
  - Son muy sencillos de implementar e integrar en una aplicación. ***¿Qué se necesita?***
  - Son fáciles de entender y utilizar por parte de los usuarios. No hay que explicarles nada nuevo.
- Sin embargo no todo son ventajas...

Algo que sabes

- Aspectos negativos:
  - Los secretos escogidos por los usuarios pueden ser **débiles** (fáciles de adivinar o descubrir) o **inadecuados** para resistir ataques.
  - El secreto se debe reutilizar en cada autenticación.
    - Se puede utilizar One Time Passwords (OTP) proporcionando una lista al usuario, pero nunca se la aprenderá.

Algo que tienes

- Se basa en utilizar algo que únicamente el usuario tiene.
- Ejemplos:
  - **Dispositivos OTP** que devuelven la siguiente contraseña a utilizar (o *apps* en el móvil)
  - **Tarjetas de coordenadas** del banco
  - **Tarjetas inteligentes** con chip como el DNIe o las tarjetas de crédito actuales. Suelen necesitar PIN para acceder a su contenido.
  - **Tarjetas con banda magnética**. Menos seguras, pues la banda se puede leer en cualquier lector.

Algo que tienes

- Proporcionan seguridad extra durante la autenticación aunque tienen algunos aspectos negativos:
  - El elemento debe estar **disponible** a la hora de autenticar.
  - El **método de generación de claves** OTP debe estar bien diseñado y no poder predecirse.
  - Se necesitan **dispositivos adicionales** para leer tarjetas inteligentes o bandas magnéticas.

Algo que eres

- Utilizando distintas técnicas **biométricas**:
  - Huella dactilar
  - Palma de la mano
  - Iris
  - Escáner de retina
  - Reconocimiento de voz
  - Reconocimiento de cara
  - Dinámica de la firma

Algo que eres

- En teoría son los que proporcionan la mayor seguridad:
  - Los aspectos que miden son únicos, y nadie podrá suplantarte
  - Nunca dejas de ser como eres*****, no lo puedes dejar olvidado en casa.
- Sin embargo tienen aspectos **negativos**

Algo que eres

- Aspectos **negativos**:
  - Requieren **dispositivos adicionales complejos** para realizar la autenticación
  - Pueden dar lugar a **falsos negativos/positivos**
  - Según la técnica puede resultar **intrusiva** o molesta, y en algunas ocasiones no está **socialmente aceptada**.
  - Si un atacante obtiene una **copia** del aspecto medido (p.ej. de la huella digital) no es posible asignar una nueva al usuario legítimo.