**Passwordless Authentication Systems**

1. Intro

enfoque de seguridad que elimin el uso de contraseñas tradicionales por metodos mas comodos y seguros.

por que cambiar el modelo actual?

contraseñas dificiles de recordar, reutilizar contrs-aseñas, son vulnerables a ataques., la experiencia de usuario suele ser frustrante.

ventajas del modelo passwordless:

* seguidad mejorada
* mejor experiencia de usuario
* menor coste de soporte
* mayor cumplimiento normativo: alineado con estandares modernos

1. Métodos

biometria

ventajas:

* caracteristicas unicas del usuario
* experiencia de usuario sencilla
* no se puede robar, perder
* identificacion unipersonal

inconvenientes:

* riesgos en privacidad
* falsos positivos/negativos

autenticación mediante dispositivo exeterno (USB)

ventajas:

* evitan el phishing
* funcionan sin acceso a internet
* 2FA: elemento + PIN

descentajas:

* no tan comodo
* llevar usb se puede perder

Credenciales basadas en PKI

ventajas:

* alta seguridad por longitud de claves
* escalable

desventajas:

* complejo de gestionar, coste elevado, requiere elemento externo

usos: firma dni, vpns

passkeys y autentication fido2 sin dispositivos externos

aplicacion que se encarga de guardar passkeys que emulan o sobreescriben los accesos a todo.

ventajas:

* sincronizacion multiplataform
* recuperacion simplificada
* sencillo

invoncenientes:

* problemas de ocmpatibilidad ente ecosistemas
* brechas de seguridad comptemeten todas las plataformas

OTPs. contraseñas de un solo uso limitada en el tiempo, no puede reutilizarse.

* HOTP (hash based): secret key (compartido)+moving factor/counter(actualizado en el client y server) = (hash)HOTP → OTP
* TOTP (time based): el moving factor es el tiempo → secret key + moving factor/time = (time)TOTP → OTP .No se suele hacer, pero en el server-side se podría mirar el time-step anterior y posterior para diferencias horarias. Expira con el tiempo, as resistente para fuerza bruta.

1. Tipos de envio de OTPs

SMS, email: se puede interceptar

messaging apps

hardware keys: requieren el dispositivo fisico

atuhenticator apps

Ventajas

* mayor seguridad
* faciles de usar
* evrsatibilidad, lo podemos usar como un segundo factor de autenticacion

descentahas

* dependencia de la entrega
* phishing, interceptacion de mensajes
* secretos compartidos: si el servidor es comprometido puede ir en contra de nuestra seguridad

Futuro

* integracion con biometria
* autneitcacion sin contraseñas permite que sea vaya cambiando
* IA y ML: mirar los patrones de uso y si hay anomalias bloquearlo

Futuro o presente?

el 65% de las plataformas usan OTP, esta muy presente. desaparecen tokens fisicos, se usa para realidad aumentada.

tecnologias emergentes

IA y ML adaptativo → croptografia postcuantica → identidades desentralizadas (SSI como blockchain) → biometria comportamental y continua

tendencias de mercado y adopcion empresarial

* bancos
* integracion con arquitecturas zero-trust
* expansion de ecosistemas passwordless

consideraciones futuras

* framentacion tecnologica
* legacy systems y costes de migracion: costoso adoptar estas nuevas tecnologías
* etica y privacidad de biometria
* educacion y formacion del usuario final: hoy en dia hay usuarios que siguen siendo desconfiados