Autenticación de usuarios

Curso 2013/14

Grado Gestión Informática Empresarial

Asignatura Auditoría y Seguridad Informática

Profesores Alfredo Cuesta Infante
alfredo.cuesta@ajz.ucm.es
Alberto Herrán González
aherran@ajz.ucm.es

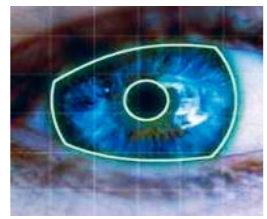
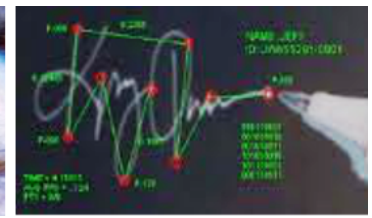
Contenidos

Un usuario se autentica...

...con algo que...

- **SABE**
  - Contraseña, PIN, respuestas a preguntas acordadas.
- **TIENE**
  - Llaves electrónicas o físicas, SmartCards
- **ES**
  - Reconocimiento de retina, huellas dactilares (biometría estática)
- **HACE**
  - Reconocimiento de voz o escritura (biometría dinámica)



Proceso de autenticación

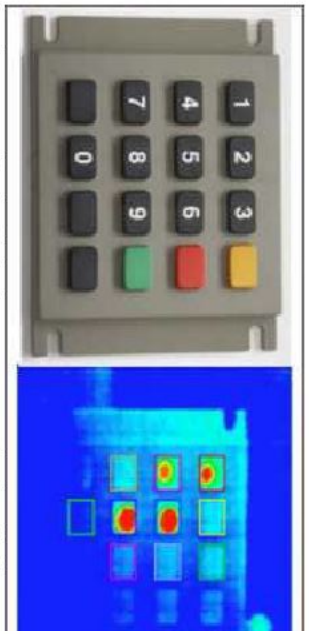
1. **Identificación.** Es el modo mediante el cual el usuario proporciona información propia reclamada por el sistema.
2. **Verificación.** Es el modo de establecer la validez de la identidad proporcionada.

Recortes de la prensa seria

Falsa seguridad con teclados de seguridad inseguros

De poco sirve instalar teclados con combinaciones de seguridad para controlar el acceso a lugares o sitios si son tan malos que las teclas se van gastando de modo que con el uso de los 10.000 posibles códigos la cosa queda reducida a 24:

Al asalto de cajeros automáticos con cámaras térmicas



A la izquierda el teclado de un cajero; a la derecha la ima
tomada con una cámara térmica después de haber sid

Dos de cada tres personas te revelan su contraseña a cambio de una chocolatina si haces una encuesta en la calle diciendo que es para un estudio. La prueba informal se llevó a cabo en las calles de Suecia y el 67 por ciento de la gente reveló su nombre, sitios de navegación habituales *y contraseña* al extraño entrevist … blemas. Por lo menos, la cosa h…

El tipo que se coló en el Banco de Francia con la clave «123456»

En este video se ve como se puede abrir una contraseña de esas que hay en los hoteles utilizando como contraseña 00000

Autenticación basada en contraseña (1/5)

Usuario = ID + Contraseña , **Sistema** = Fichero de contraseñas

Seguridad proporcionada

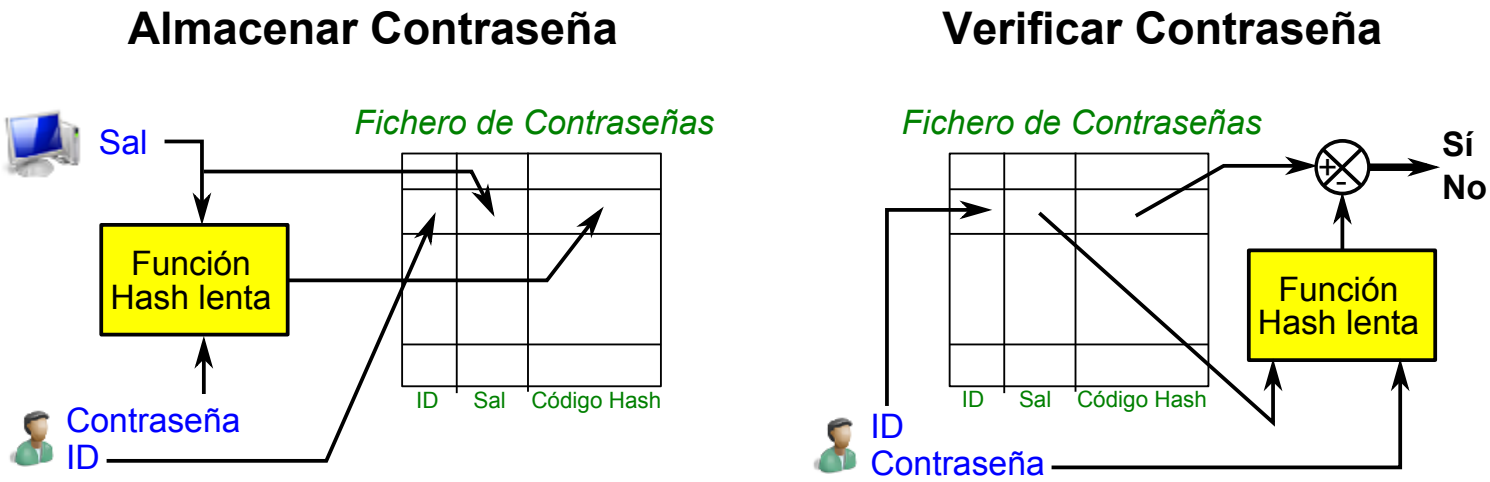
- El ID determina si el usuario está autorizado para acceder al sistema.
- El ID determina los privilegios del usuario.
  Ej: Superusuarios, invitados anónimos, ...
- Mediante el listado de los IDs de un sistema por parte de un usuario, este puede conceder permisos a otros usuarios sobre sus archivos y carpetas.

Vulnerabilidades de las contraseñas

- Ataque offline con diccionarios.
  - Lograr llegar a copiar el fichero de claves.
  - Después, offline, se compara cada clave con un listado de claves generado con el mismo algoritmo que se denomina *diccionario*.
- Ataque a una cuenta específica.
  - Si se conoce el nombre de usuario se puede intentar adivinar su contraseña.
  - Se suelen probar contraseñas fáciles o populares.
  - A veces el atacante intenta averiguar dicha contraseña con *ingeniería social*.
- Secuestro de la sesión.
  - El atacante espera a que la estación de trabajo quede desatendido y ocupa el puesto.
  - No es muy elaborada pero es efectiva si no hay una desconexión automática.
- Sacar partido a errores del usuario.
  - No cambiar las contraseñas por defecto.
  - Anotar la contraseña en un sitio visible, público o de fácil acceso.
  - Usar la misma contraseña en muchos procesos distintos.
- Si la contraseña se comunica a través de una red, esta debe estár encriptada para evitar posibles robos por monitorización.

Autenticación basada en contraseña (2/5)

El fichero de contraseñas



¿Qué es la *sal*?

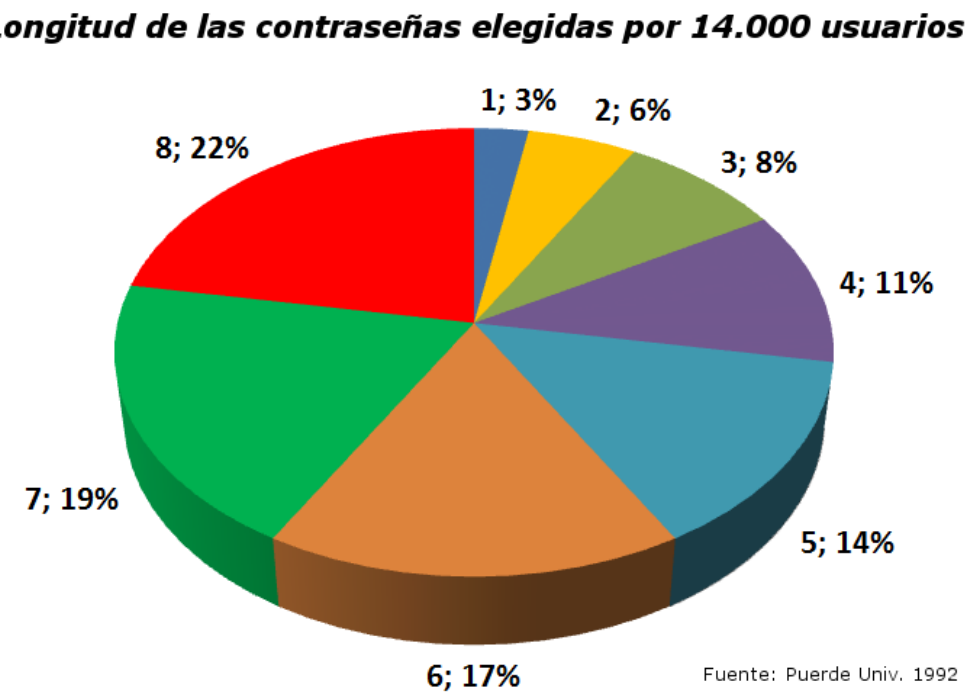
- Se trata de una cadena binaria de longitud fija que se utiliza para *condimentar* la contraseña, que puede tener cualquier longitud.
- Ambas son procesadas por una función hash, de ejecución lenta.
  (Cuanto más rápido se calcule más viable resulta reventarla con fuerza bruta)
- El resultado (código Hash) también tiene un tamaño fijo que se almacena con el ID y el valor de la sal usado para generarlo.
- Impide que 2 contraseñas se vean iguales en el fichero contraseñas.
- Si la sal tiene b bits hay 2^b posibilidades diferentes de almacenar una contraseña.
- Es casi imposible averiguar si se está utilizando la misma contraseña para acceder a diferentes sistemas.

Autenticación basada en contraseña (3/5)

Estrategia de selección de contraseñas

MEJOR cuanto más LARGA y más DIFÍCIL de adivinar

Parece evidente pero...

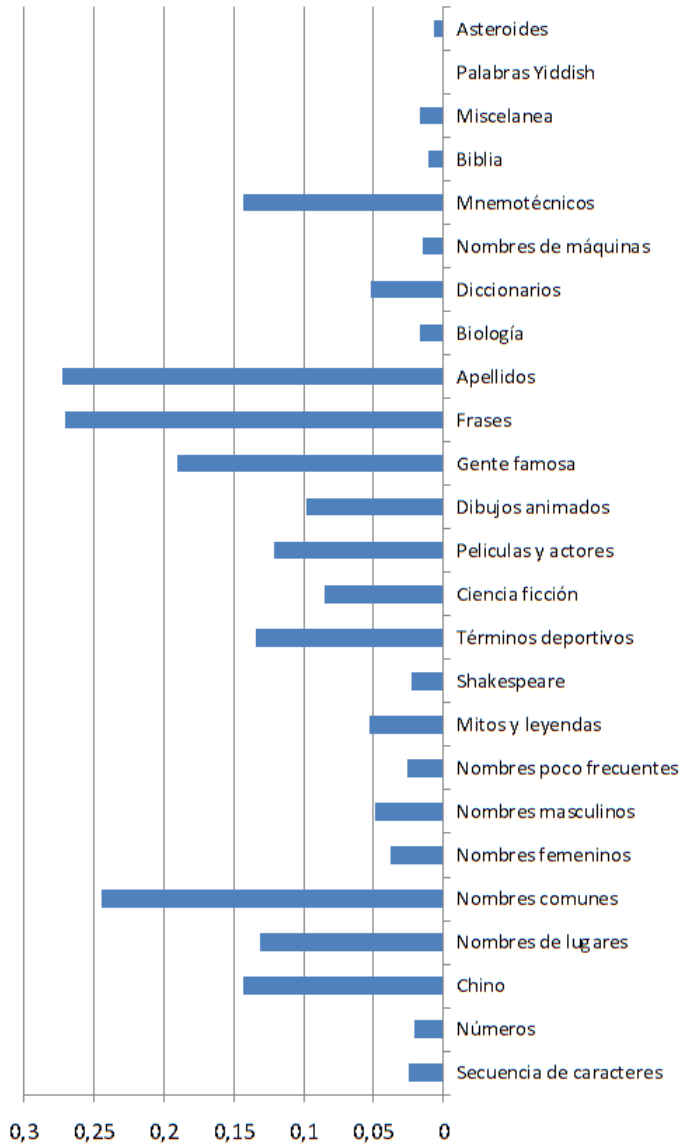


- Se debe forzar al sistema a RECHAZAR longitudes menores de 8 bits.

Autenticación basada en contraseña (4/5)

¿y sobre la dificultad de adivinarlas?

- ¡ Un ataque probando 62727 palabras adivinó **1/4** de las contraseñas !
- Utilizando como contraseña el usuario de 138 cuentas se adivinaron 368 contraseñas! Evidentemente había usuarios que repetían su contraseña en varias cuentas.
- ¡¡ Relación *Beneficio/Coste* del **2.83** !!
- El resto de pruebas en el gráfico de la derecha.
- El gráfico muestra la relación Beneficio/Coste de otros intentos.
  MENOR relación significa que se necesitaron MÁS palabras para adivinarla



Autenticación basada en contraseña (5/5)

Para aumentar la seguridad

- Formación del usuario
  - ↓ Poca probabilidad de éxito aunque...
  - ↑ Hay trucos:
    - Usar iniciales de frases secretas; Ej: *Mi Perro Se Come 5 Filetes = MPSC5F*
    - Cambiar letras por números o símbolos; Ej: *profesorASI = pr0f3s0r451*
- Contraseñas generadas por ordenador
  - ↓ Dificil de recordar
  - ↑ Eficaz
- Comprobación automática de *agujeros*
  - ↓ Muy costoso para el PC
  - ↓ No tapa el agujero, sólo avisa
- Comprobación automática cuando se genera
  - ↑ Comprobación en el momento, asegurándo que es suficientemente larga y difícil.
  - ↑ El usuario elige su contraseña

Protección del fichero de contraseñas

- Separar la columna del código hash para cada contraseña en otro fichero: **shadow password file**
- Este fichero es accesible para un usuario privilegiado del sistema.

¿Qué es una función Hash?

- Es un algoritmo que recibe una cadena de elementos (caracteres, bytes, bits, etc) de cualquier longitud y genera una cadena de elementos de longitud fija.

entrada	C	l	a	v	e	S	e	c	r	e	t	a
salida	l			e			c			t		

entrada	C	l	a	v	e	S	e	c	r	e	t	a				
salida	a	l	C	a	S	e	v	S	r	c	e	r	a	t	e	a

- El objetivo de una función Hash es **ocultar**, no cifrar.
  La diferencia es que cifrar $\rightarrow$ es posible descifrar.
- Para ocultar no necesitamos una función *reversible*; pero sí debe tener algunas propiedades importantes:

1. **Inyectiva:** 2 entradas diferentes dan lugar a 2 salidas diferentes

$$k_1 \neq k_2 \rightarrow Hash(k_1) \neq Hash(k_2)$$

2. **Determinista:** Siempre que recibe la misma entrada produce la misma salida, es decir no hay aleatoriedad.
3. **Resistente a colisiones:** Una colisión se produce cuando dos entradas distintas dan lugar a dos salidas iguales.
4. **Efecto avalancha:** Un cambio muy pequeño en la entrada provoca cambios muy grandes en la salida.

* Ver ejemplos en la práctica de autenticación - ejercicio 1

Autenticación basada en objetos testigo (1/2)

Testigo (*Token*) es el objeto que el usuario posee para autenticarse.

Tarjeta convencional

- En inglés *Memory Card*
- Se debe combinar con una autenticación por contraseña
  Ej: Utilización de un cajero = Tarjeta + PIN (*Personal Identification Number*)

Presenta algunas **desventajas**:

- ↓ Precisa de un lector apropiado
- ↓ Si la contraseña no sigue las indicaciones vistas anteriormente, un testigo perdido, robado o duplicado puede suponer una brecha en la seguridad.
  Ej: El PIN es una contraseña de 4 dígitos → Sólo hay 10000 posibilidades.
- ↓ El usuario está acostumbrado a este método en pocos sistemas (cajeros y puertas restringidas); pero produce rechazo para acceder a un ordenador.

Su información está almacenada de manera fija.
La **tecnología** empleada ha variado en el tiempo haciendose cada vez más sofisticada

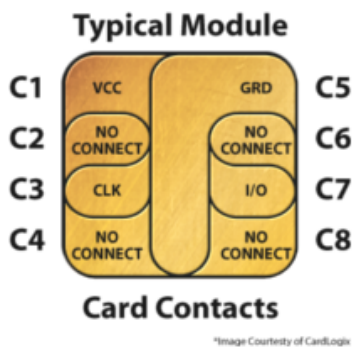
- Desde grabar los datos fisicamente, en **relieve** sobre la superficie de la tarjeta,
- posteriormente en una banda **magnética** adosada en la parte posterior,
- y finalmente insertando la tarjeta de memoria **dentro** de la tarjeta.

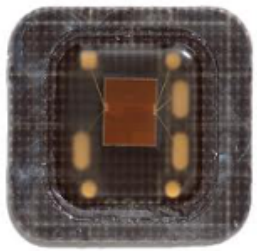
El avance de la tecnología ha permitido incluir cierta capacidad de procesado de la información, dando lugar a las tarjetas inteligentes.

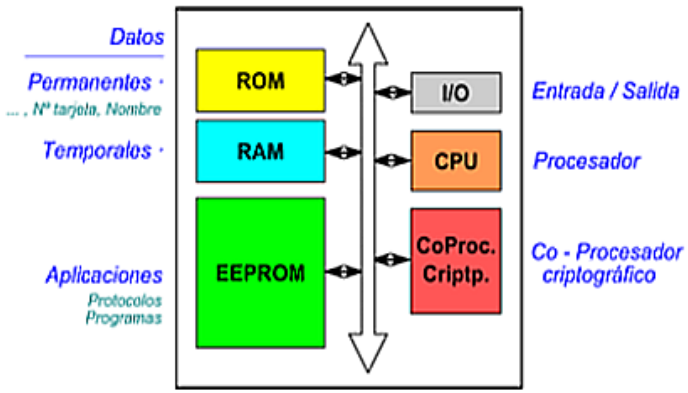
Autenticación basada en objetos testigo (2/2)

Tarjeta Inteligente

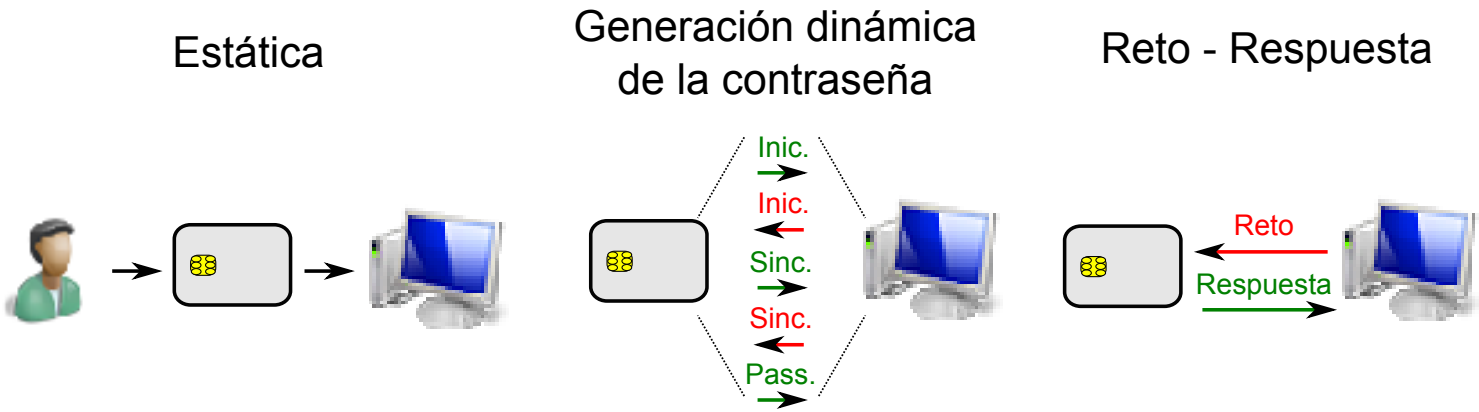
- En inglés *Smart Card*







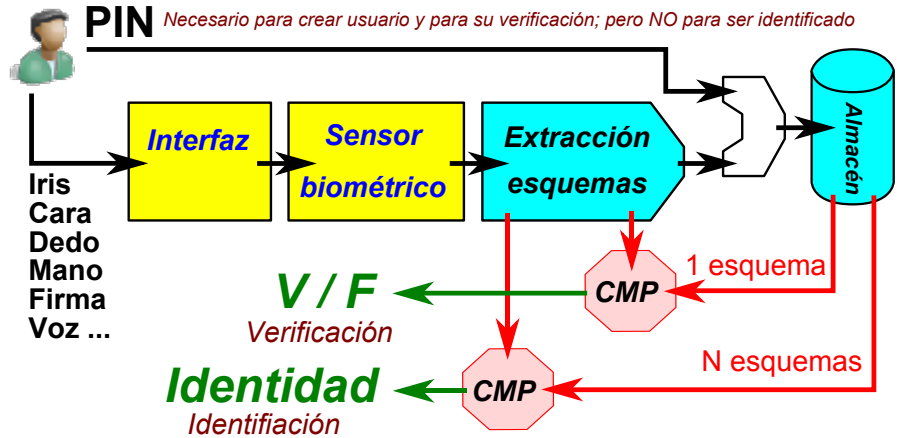
- **Nuevo:** Protocolos de autenticación



Autenticación basada en biometría

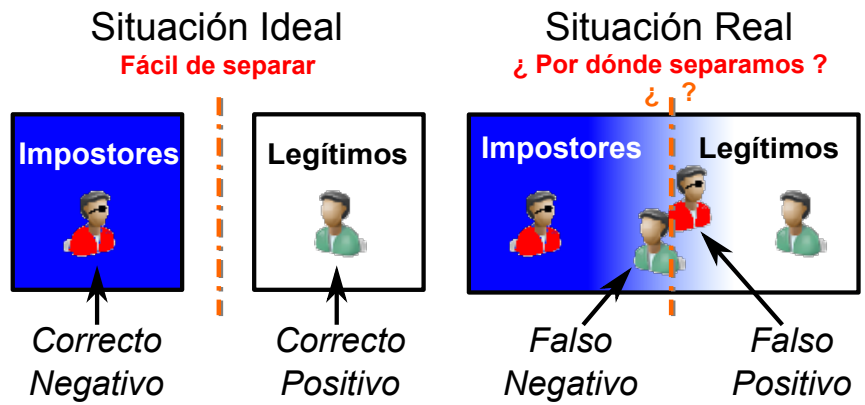
Operaciones

- **Crear usuario** (*Enrollment*)
- **Verificación** (*Verification*)
- **Identificación** (*Identification*)



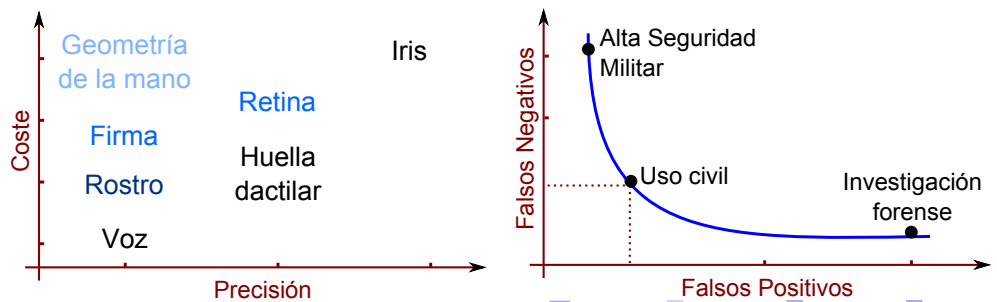
Dificultades

- Computacionalmente más complejo.
- Hacen falta métodos de IA.
- Se pueden producir 2 tipos de errores
  - Falsos positivos
  - Falsos negativos



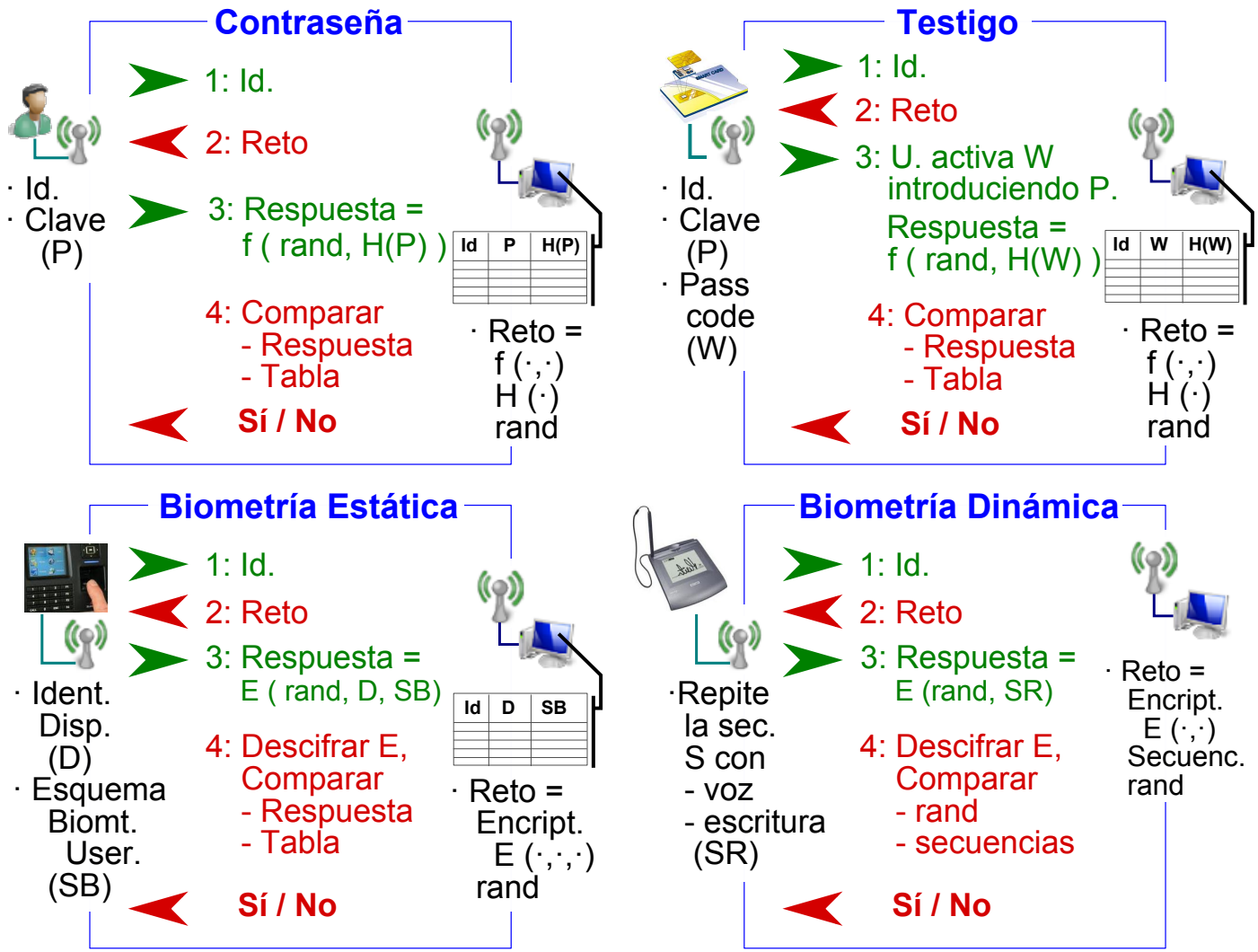
¿Cuál usar?

- Según el coste y la precisión
- Según el tipo y ratio de errores



Autenticación remota

Hasta ahora el acceso era local
¿Qué ocurre si se accede al sistema desde internet?
PROBLEMA Surgen nuevas amenazas debidas al ataques contra la transmisión.
SOLUCIÓN Utilización de protocolos *Reto-Respuesta*



Tipos de ataque y medios de defensa

Autenticador	Ejemplo de ataque	Defensa típica
Atacar al cliente		
Contraseña	Adivinar, Busqueda exhaustiva	Claves complejas, Limitar el número de intentos.
Testigo	Busqueda exhaustiva	
Biometría	Falso positivo	
Atacar al host		
Contraseña	Ataque con diccionario	Hashing, Claves complejas
Testigo	Robo del *passcode*	
Biometría	Robo de esquemas	Reto-Respuesta
Robar, copiar o espiar		
Contraseña	Navegar 'por encima del hombro' (*Shoulder surfing*)	Mantener la clave en secreto; Revocar las claves atacadas rapidamente
Testigo	Falsificación del Hw.	Testigos más resistentes
Biometría	Falsificar la biometría (*Spoofing*)	Detección de copias en el dispositivo;
Caballos de Troya		
Contraseña	Introduccir un cliente malicioso o un dispositivo de captura	Autenticación del cliente o del dispositivo
Testigo		
Biometría		