Universidad de Oviedo

Departamento de Informática

Campus de Gijón

Autenticación de Usuarios (Local)

Presentación

Daniel F. García

Introducción a la autenticación

Definición

Proceso de verificación de una identidad reclamada por una entidad

Fases

1) Fase de identificación

2) Fase de verificación

Medios

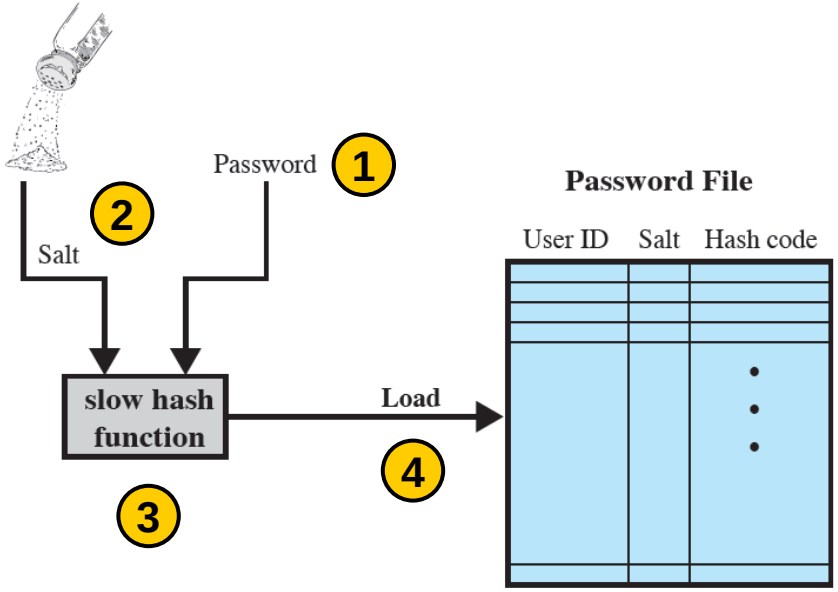
- Algo que el usuario conoce
- Algo que el usuario posee
- Algo que el usuario es
- Algo que el usuario hace

Autenticación basada en contraseñas

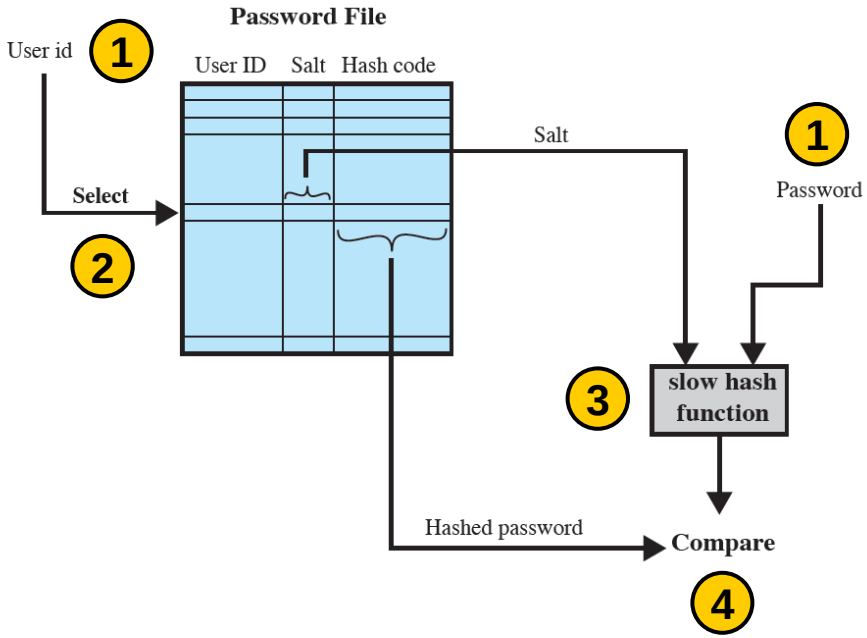
Para acceder a un sistema . . .

1. Sistema: pide identificador + contraseña
2. Sistema: compara contraseña proporcionada con contraseña almacenada

Almacenamiento de la contraseña



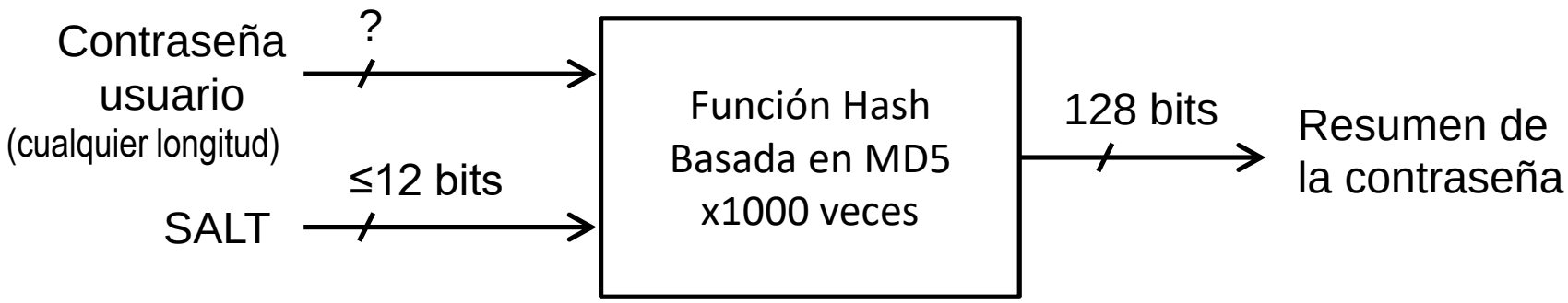
Verificación de la contraseña



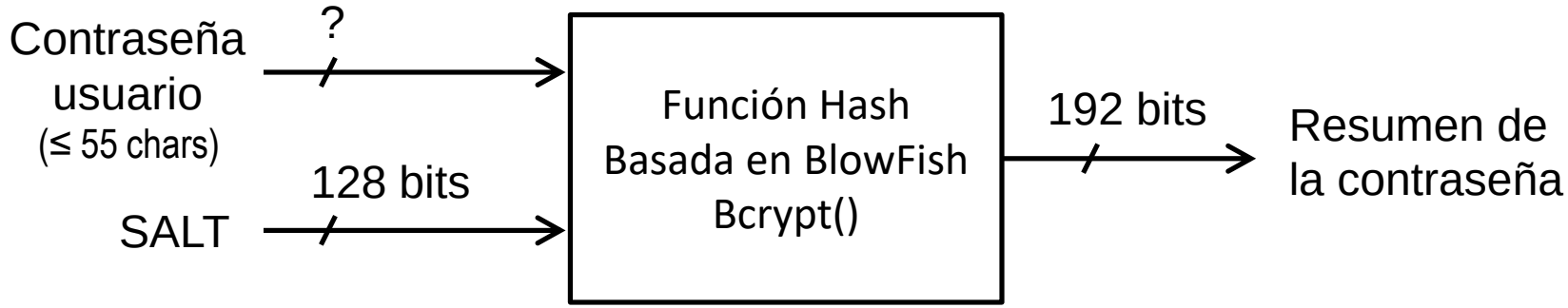
Objetivos del SALT

Implementaciones de contraseñas resumidas

Esquema típico en un UNIX actual (Linux, Solaris, FreeBSD)



Esquema típico en un UNIX muy seguro (OpenBSD)



Ataques a contraseñas (1)

Ataque de diccionario

NO se usa SALT

Contra1dic → F. Hash → ResumContra1dic == ResumContra1fich? …
…
ContraMdic → == ResumContraNfich?

Si coincide alguna → Contraseña adivinada

SI se usa SALT

Contra1dic →
SALTuser1fich → F.Hash → ResumContra1dic_user1 == ResumContra1fich
…
Contra1dic →
SALTuser2fich →
…

Si coincide → Contraseña User1 adivinada

¡El SALT obliga al atacante a resumir cada contraseña del diccionario específicamente para cada usuario!

Optimización del ataque de diccionario

Utilizando tablas arco iris (*Rainbow Tables*)

Contramedidas

Proteger al máximo el acceso al fichero de contraseñas

Ataques a contraseñas (2)

Ataque a una cuenta (*account*) específica

Seleccionar una cuenta y probar contraseñas hasta descubrir la correcta

Limitar el número de intentos fallidos consecutivos

Ataque a una contraseña popular

Elegir una contraseña popular y probar todos los identificadores de usuario

Impedir que los usuarios elijan contraseñas fáciles de adivinar

Adivinar la contraseña de un usuario específico

El atacante usa información del usuario para adivinar la contraseña

Aplicar una política de contraseñas robustas (*strong passwords*)

Explotar los errores del usuario

Anotarla en papel / Compartirla / Revelarla (Ing. Social)

Proporcionar formación y usar un sistema de selección de contraseñas

Explotar el uso múltiple de una misma contraseña

Los usuarios usan la misma contraseña (o similar) para múltiples dispositivos

Aplicar una política que impida usar la misma contraseña en varios dispositivos

Elección de contraseñas seguras (1)

PROBLEMAS

1º La longitud de las contraseñas debe ser razonable

2º Las contraseñas no deben adivinarse fácilmente

Objetivo: Desarrollar una estrategia que permita una libertad de elección intermedia

- Eliminar contraseñas sencillas pero permitir contraseñas memorizables
- Mantener el tamaño del conjunto de contraseñas posibles muy grande

Técnicas básicas → { Educación del usuario; Generación de contraseñas por computador; Comprobación de contraseñas reactiva y proactiva

Elección de contraseñas seguras (2)

Educación del Usuario

Concienciar → (*hard-to-guess passwords*)
Directrices → (*strong passwords*)

Hay infinidad de páginas que indican como elegir contraseñas seguras y memorizables:

https://www.mit.edu/afs/sipb/project/doc/passwords/passwords.html

https://computing.cs.cmu.edu/security/security-password.html

ISO/IEC 27002
5.17 Información de Autenticación

Características elementales de una contraseña segura (*safe password*)

- No se puede encontrar en un diccionario
- Contiene números y caracteres especiales
- Contiene una mezcla de mayúsculas y minúsculas
- Tiene una longitud mínima de 10 caracteres
- No se puede adivinar basándose en datos del usuario:
  Fecha de nacimiento, Código postal, Número de teléfono, …

Hay muchas herramientas que ayudan a generar y comprobar contraseñas

Elección de contraseñas seguras (3)

Comprobación Reactiva

El sistema ejecuta su propio comprobador de contraseñas periódicamente

Hay múltiples herramientas disponibles en Internet:
(***password cracking software tools***)

John the Ripper https://www.openwall.com/john

Hash Suite https://hashsuite.openwall.net/

Comprobación Proactiva

El usuario selecciona su contraseña y el sistema comprueba si es aceptable

Paso 1º - Cumplir reglas

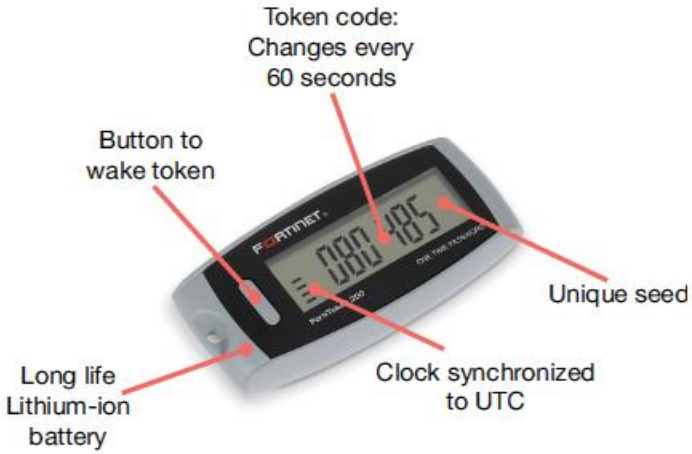
Paso 2º - Adivinar la contraseña

Autenticación basada en token

Token = Objeto que posee un usuario para su autenticación

Tienen múltiples formatos:

1) Hardware



2) Software

Ej. Contraseña o código recibido/generado en un móvil

3) Tarjeta inteligente

Autenticación basada en token

Conectividad con el computador

1) Tokens SIN conexión

Se obtiene una Autenticación de 2 factores

2) Tokens CON conexión

Métodos de autenticación

Contraseña estática

Contraseña dinámica

- Generada síncronamente (***time-synchronized***)
- Generada asíncronamente (***mathematical-algorithm-based***)

Desafío-Respuesta (*Challenge-Response*)

Tarjetas

Tarjetas de memoria (*memory cards*)

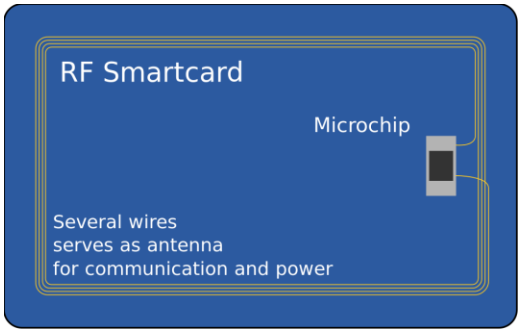
Tarjetas inteligentes (*smart cards*)

Características físicas → ISO/IEC 7810:2003
Características eléctricas, de comunicación, funcionalidad → ISO/IEC 7816-1 a 7816-15

Tarjetas inteligentes CON contactos

Transmisión a nivel de:
caracteres (T=0) o bloques (T=1)

Tarjetas inteligentes SIN contactos



Características definidas en
ISO/IEC 14443-1 a 14443-4

Tarjetas: DNIe

Objetivo DNIe: Identificación personal

Información contenida en el microchip:

distribuida en 3 zonas con diferentes condiciones de acceso

ZONA PÚBLICA, Accesible en lectura sin restricciones:

- Certificado CA intermedia emisora
- Claves Diffie-Hellman
- Certificado x509 de componente

ZONA PRIVADA, Accesible en lectura por el ciudadano, mediante la utilización de la Clave Personal de Acceso o PIN:

- Certificado de Firma
- Certificado de Autenticación

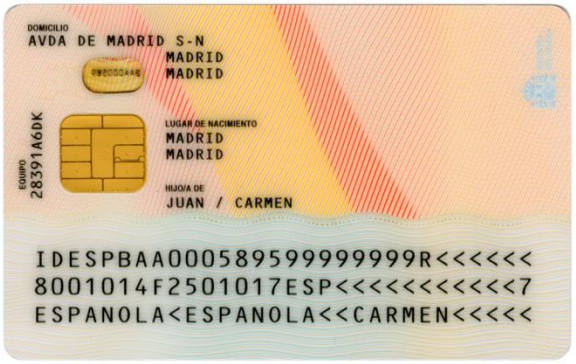
ZONA DE SEGURIDAD, Accesible en lectura por el ciudadano, en los Puntos de Actualización del DNIe:

- Datos de filiación del ciudadano (los mismos que están en el soporte físico)
- Imagen de la fotografía
- Imagen de la firma manuscrita

Características del Chip:

- Modelo del Chip: st19wl34 y ICC ST19wl34
- Sistema operativo: DNIe v1.1
- Capacidad: 34Kbytes Eeprom.

DNIe 3.0 tiene el chip en el reverso

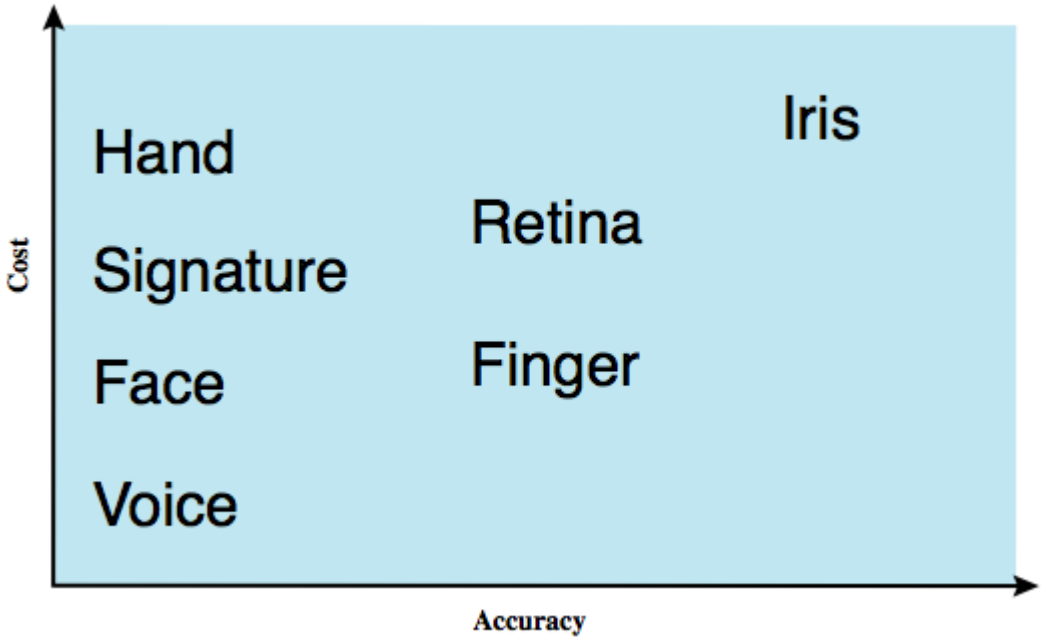


Autenticación biométrica (1)

Biometría → Identificar a un individuo basándose en sus características físicas

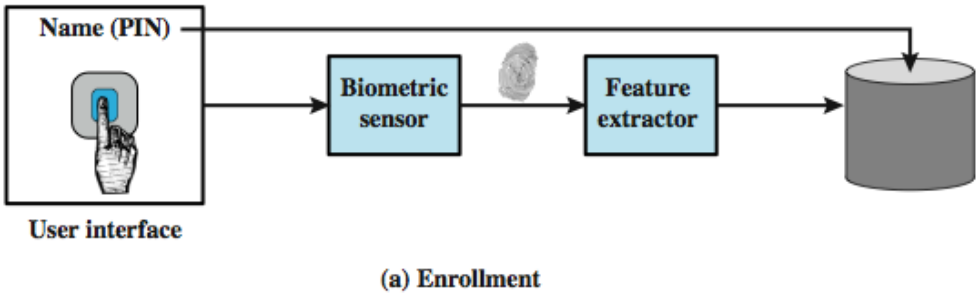
- Características estáticas
- Características dinámicas

Coste en función de la precisión

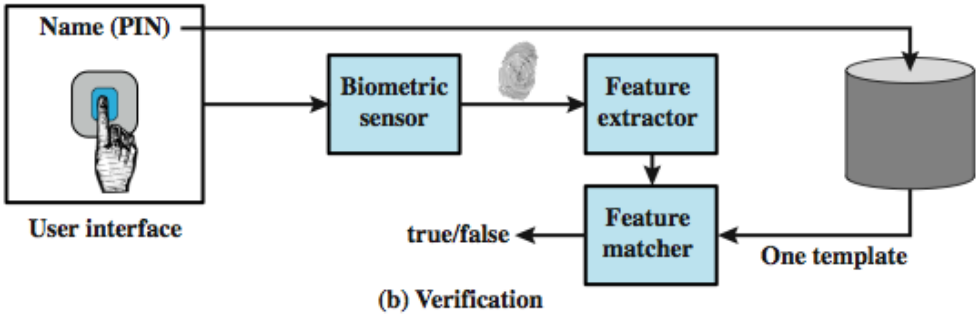


Autenticación biométrica (2)

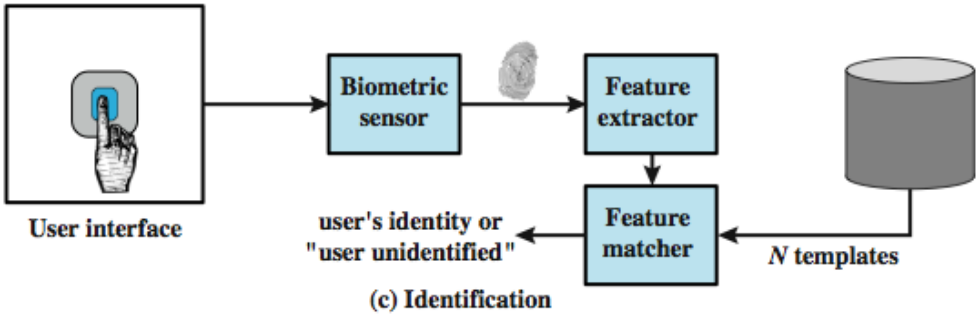
Fase 1
Inscripción



Fase 2
Verificación

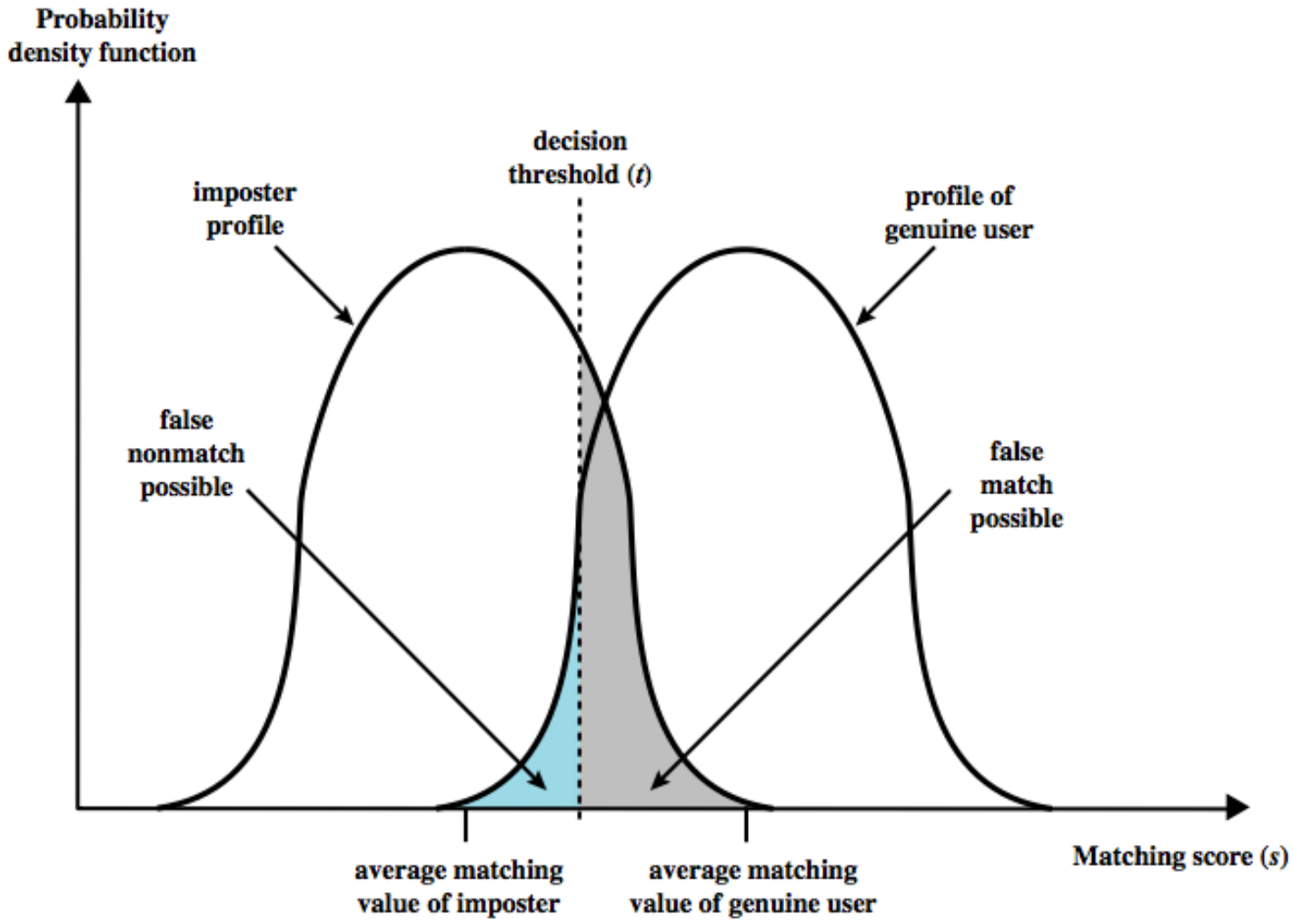


Fase 2
Identificación



Autenticación biométrica (3)

Precisión (*accuracy*) de la biometría



Autenticación biométrica (4)

Compromiso de funcionamiento de un sistema de autenticación biométrica