Seguridad informática: principios y práctica

Capítulo 3 – Autenticación de usuarios por William Stallings y Lawrie Brown

Autenticación de usuario

- bloque fundamental de seguridad
  - base del control de acceso y la responsabilidad del usuario
- es el proceso de verificar una identidad reclamada por o para una entidad del sistema • tiene dos pasos: •
  identificación: especificar el identificador • verificación: vincular la entidad (persona) y el identificador
- distinto de la autenticación de mensajes

Medios de autenticación de usuarios

•cuatro medios para autenticar la identidad del usuario •basados en

•algo que tienes

- p. ej., una clave, un token, una tarjeta inteligente •algo que

sabes - p. ej., una contraseña, un PIN •algo que eres

- biometría estática (p. ej., huella dactilar, retina, rostro);
- biometría dinámica (p. ej., voz, mecanografía);

• alguien que conoces - la red social del usuario, CCS'06

• se puede utilizar solo o combinado

• todos pueden proporcionar autenticación de usuario •

todos tienen problemas

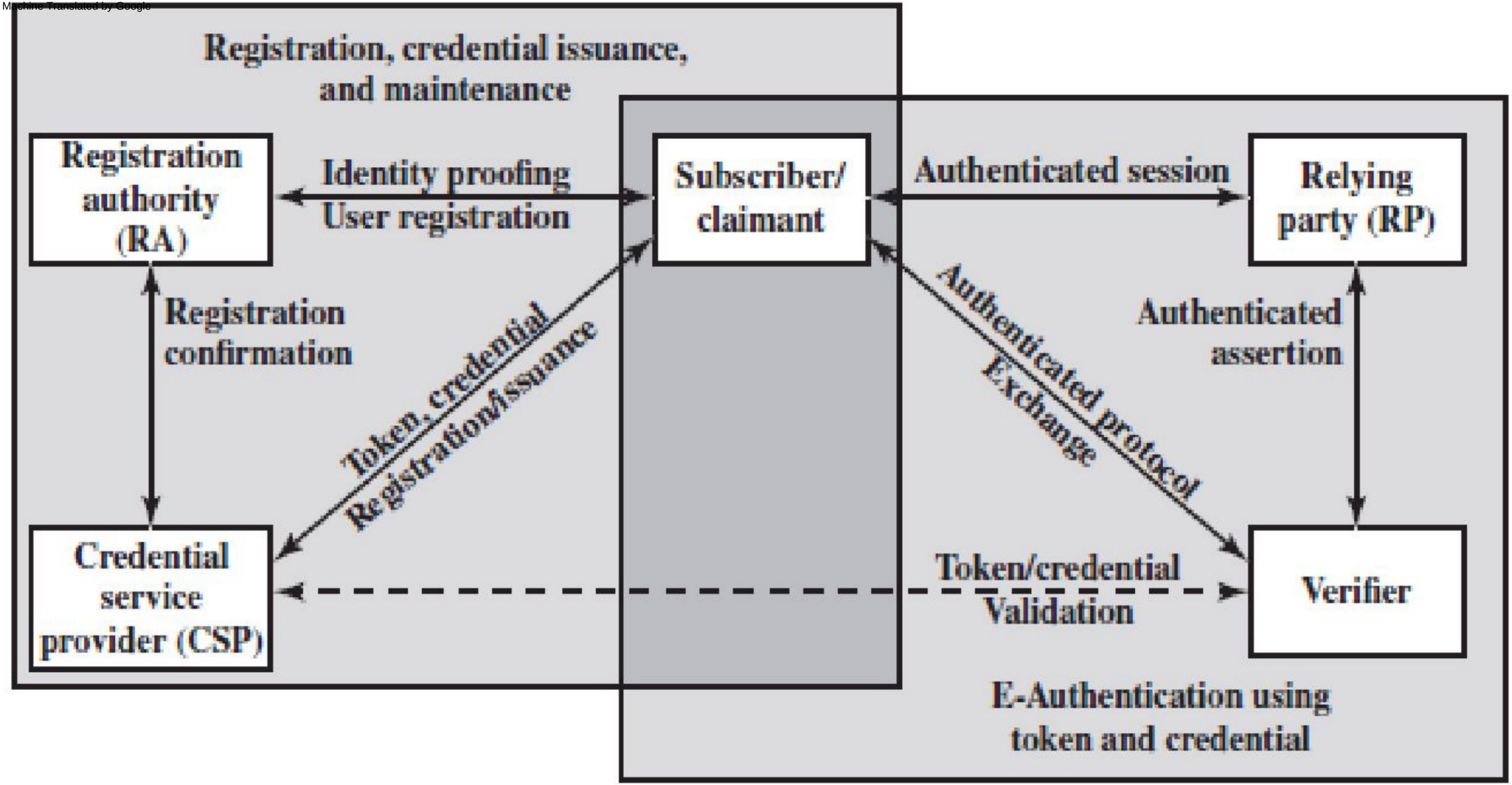


Figure 3.1 The NIST SP 800-63-2 E-Authentication Architectural Model

Autenticación de contraseña

- método de autenticación de usuario ampliamente utilizado • el
  usuario proporciona nombre/nombre de usuario y
  contraseña • el sistema compara la contraseña con la guardada para el inicio de sesión especificado
- autentica la identificación del usuario que inicia sesión y
  - que el usuario está autorizado a acceder al sistema
  - determina los privilegios del usuario •
    se utiliza en el control de acceso discrecional

Vulnerabilidades de contraseñas

• ataque de diccionario fuera de línea • ataque de cuenta específica • ataque de contraseña popular • secuestro de estación de trabajo • explotación de errores de usuario • explotación del uso de múltiples contraseñas • monitoreo electrónico

Contramedidas

• Detener el acceso no autorizado al archivo de

contraseñas • Medidas de detección de intrusiones

• mecanismos de bloqueo de cuentas

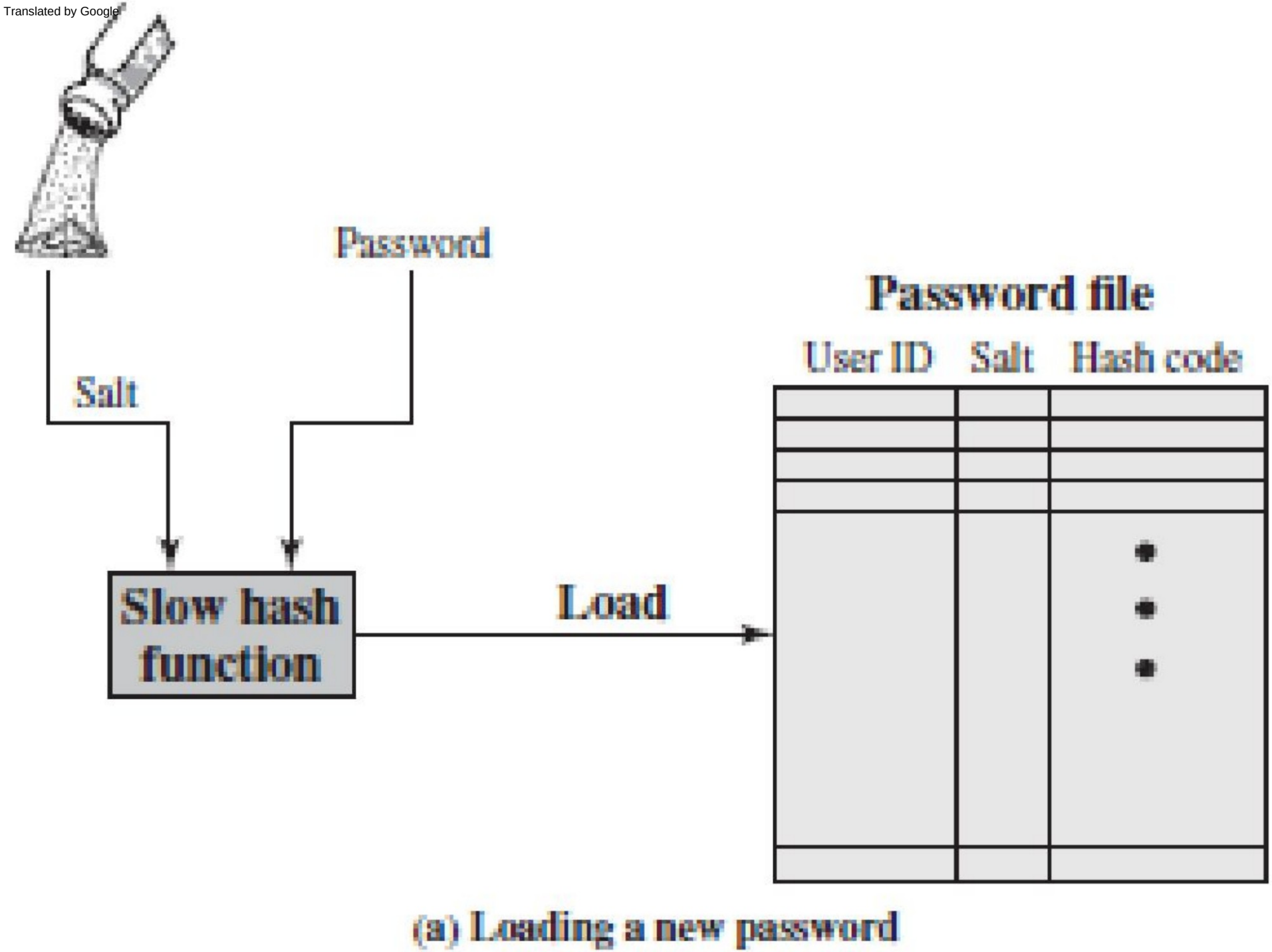
• políticas contra el uso de contraseñas comunes, sino más bien contraseñas difíciles de adivinar •

capacitación y aplicación de políticas • cierre

de sesión automático de la estación de

trabajo • enlaces de red cifrados

Uso de contraseñas cifradas



(a) Loading a new password

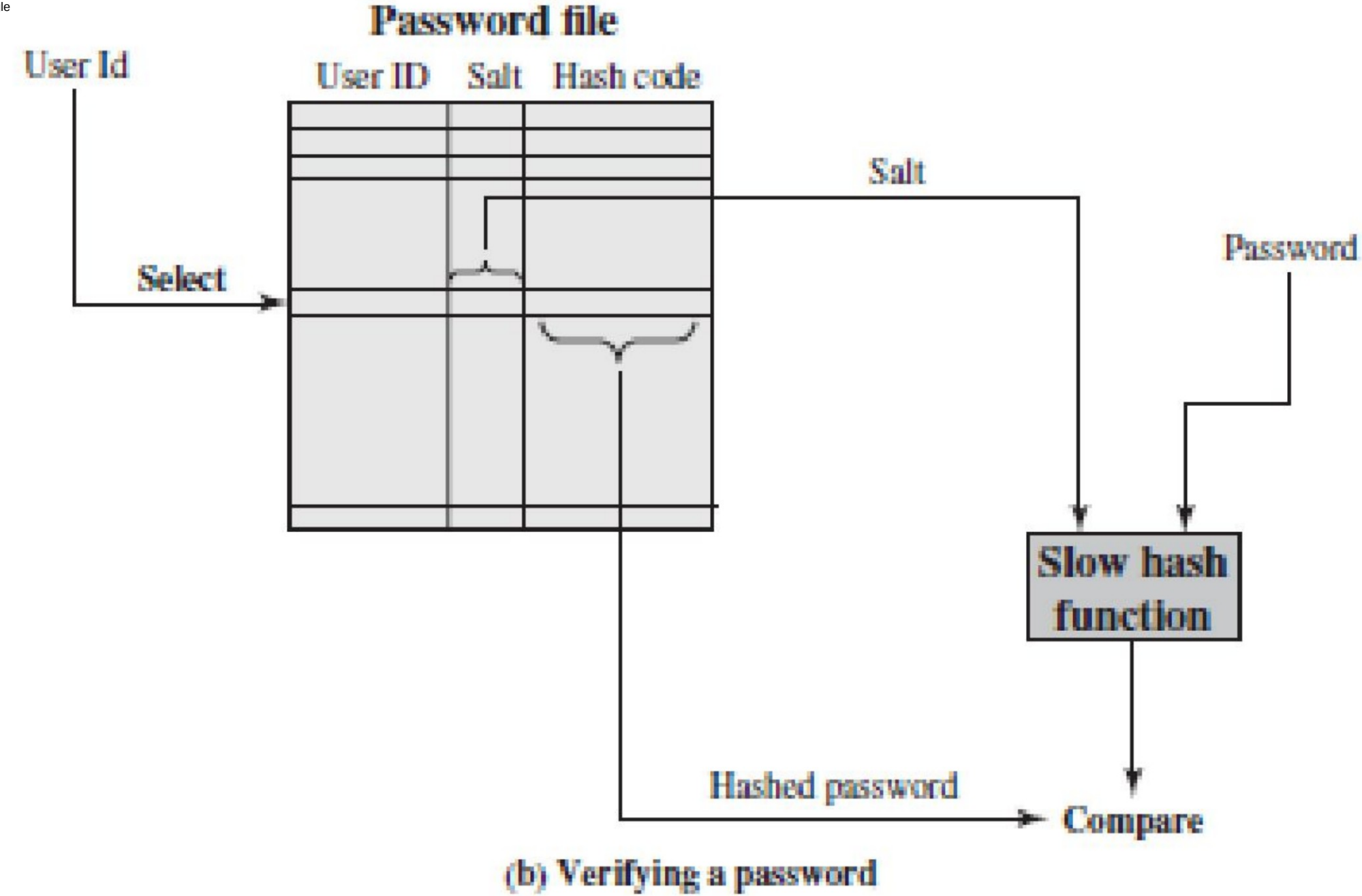


Figure 3.2 UNIX Password Scheme

Implementación de UNIX

- esquema original
  - Contraseña de 8 caracteres en formato de clave

    de 56 bits • Sal de 12 bits utilizada para modificar el cifrado DES en una función hash

    unidireccional • Ceros de 64 bits como entrada inicial, la salida se cifra aún más, … se repite durante 25 veces
  - salida final traducida a una secuencia de 11 caracteres
- ahora se considera lamentablemente inseguro
  - p. ej. supercomputadora, 50 millones de pruebas, 80 min
- A veces todavía se utiliza por compatibilidad.

Implementaciones mejoradas

- tienen otras variantes de hash/salt más fuertes •

muchos sistemas (Solaris, Linux) ahora usan MD5

- con sal de 48 bits
- La longitud de la contraseña es

ilimitada • Se codifica con un bucle interno de 1000

veces • Produce un hash de 128 bits

•OpenBSD utiliza un algoritmo hash basado en cifrado de bloques Blowfish llamado

Bcrypt •

utiliza sal de 128 bits para crear un valor hash de 192 bits

Métodos para descifrar contraseñas

- ataques de diccionario •

  probar cada contraseña posible y luego las variantes obvias en un diccionario grande contra el hash en el archivo de contraseñas

- •ataques de mesa arcoiris

  - precalcular tablas de valores hash de todas las contraseñas posibles para todas las posibles sales
  - una tabla gigantesca de valores hash
  - Por ejemplo, la tabla de 1,4 GB descifra el 99,9 % de las contraseñas alfanuméricas de Windows en 13,8 segundos
  - no es factible si se utilizan valores de sal mayores

Opciones de contraseña

- Los usuarios pueden elegir contraseñas cortas.
  - p. ej. el 3% tenía 3 caracteres o menos, lo que se adivina fácilmente • el sistema puede rechazar opciones que sean demasiado cortas
- los usuarios pueden elegir contraseñas fáciles de adivinar • por lo que los piratas informáticos utilizan listas de contraseñas probables • por ejemplo, un estudio de 14000 contraseñas cifradas adivinó casi 1/4 de ellas • tomaría alrededor de 1 hora en los sistemas más rápidos calcular todas las variantes, y solo

¡Necesito un descanso!

Control de acceso a archivos con contraseña

- puede bloquear ataques de adivinación fuera de línea al denegar el acceso a contraseñas cifradas
  - ponerlas a
    disposición solo de usuarios privilegiados • a
    menudo utilizando un archivo de contraseñas shadow separado (de los ID de usuario)
- todavía tiene vulnerabilidades •
    explotar un error del
    sistema operativo • accidente con los permisos que lo hacen
    legible • usuarios con la misma contraseña en otros
    sistemas • acceso desde medios de respaldo
    desprotegidos • rastrear contraseñas en tráfico de red desprotegido

Usar mejores contraseñas

• tienen problemas evidentes con las contraseñas • el objetivo es eliminar las contraseñas fáciles de adivinar • aunque sigan siendo fáciles de recordar para el usuario

• técnicas: •
    educación del usuario
    • contraseñas generadas por computadora
    • verificación reactiva de contraseñas
    • verificación proactiva de contraseñas

Educación del usuario

- Una buena técnica: usar la primera letra de cada palabra de una frase; sin embargo, no elijas una frase conocida.
  - Una manzana al día mantiene alejado al médico (aaadktda)
  - Mi hermana Peg tiene 24 años (mspi24yo)
- Las pautas pueden ignorarse…

Contraseñas generadas por computadora

- FIPS PUB 181 define uno de los generadores de contraseñas automatizados mejor diseñados •
  Genera palabras formando sílabas pronunciables •En

general, los esquemas de contraseñas generados por computadora tienen poca aceptación por parte de los usuarios.

Comprobación reactiva de contraseñas

• El sistema ejecuta periódicamente su propio descifrador de contraseñas para encontrar contraseñas fáciles de adivinar. • Descifrador de contraseñas John the Ripper • Consume muchos recursos, es vulnerable hasta que se identifica

Comprobación proactiva de contraseñas

- aplicación de normas más asesoramiento a los usuarios, por ejemplo
  - 8+ caracteres, mayúsculas/minúsculas/numéricos/puntuación •
  - puede no ser suficiente
- usar un descifrador de contraseñas para rechazar contraseñas incorrectas •
  - problemas de tiempo y espacio •

modelo de Markov • genera

  - contraseñas que se pueden adivinar • por lo
  - tanto, rechaza cualquier contraseña que pueda generar • filtro Bloom
- se usa para crear una
  - tabla basada en un diccionario usando hashes • verifica la contraseña deseada
  - con esta tabla

Autenticación biométrica

- autenticar
  Usuario basado
  en una de
  sus
  características físicas.

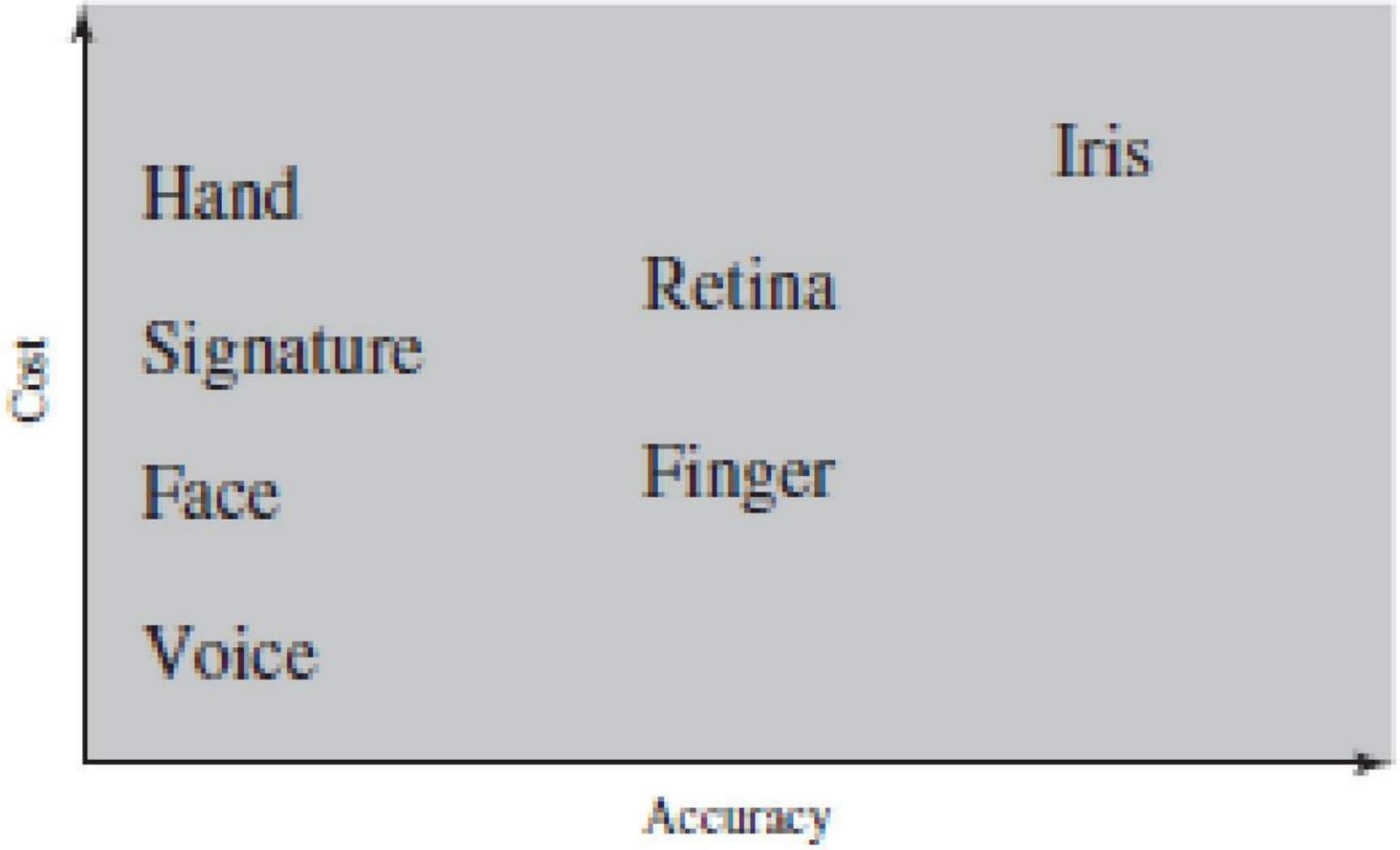


Figure 3.7 Cost versus Accuracy of Various Biometric Characteristics in User Authentication Schemes

Funcionamiento de un Biométrico Sistema

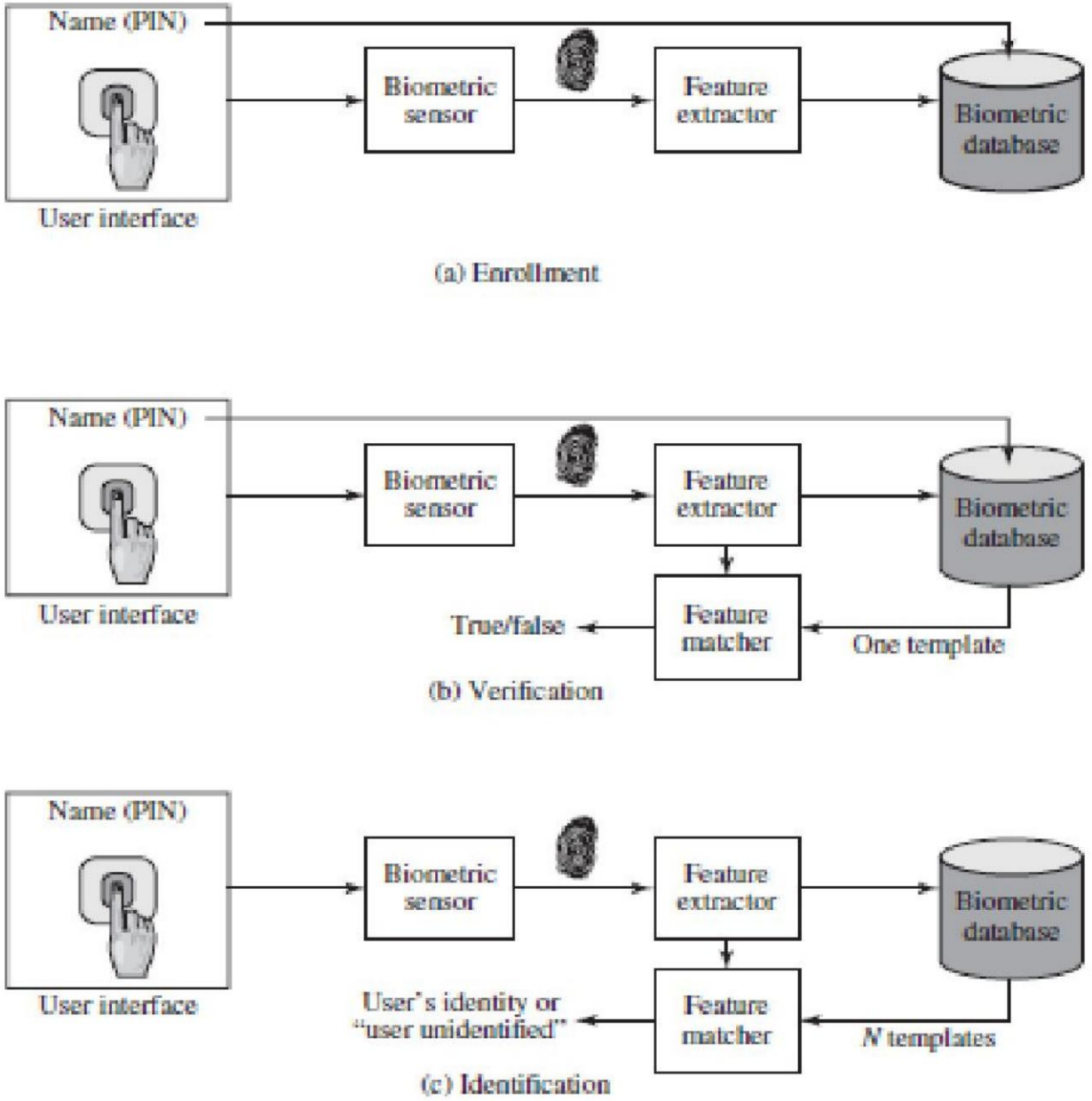


Figure 3.8 **A Generic Biometric System** Enrollment creates an association between a user and the user's biometric characteristics. Depending on the application, user authentication either involves verifying that a claimed user is the actual user or identifying an unknown user.

Precisión biométrica

- nunca se obtienen plantillas

idénticas • problemas de falsa coincidencia / falsa no coincidencia

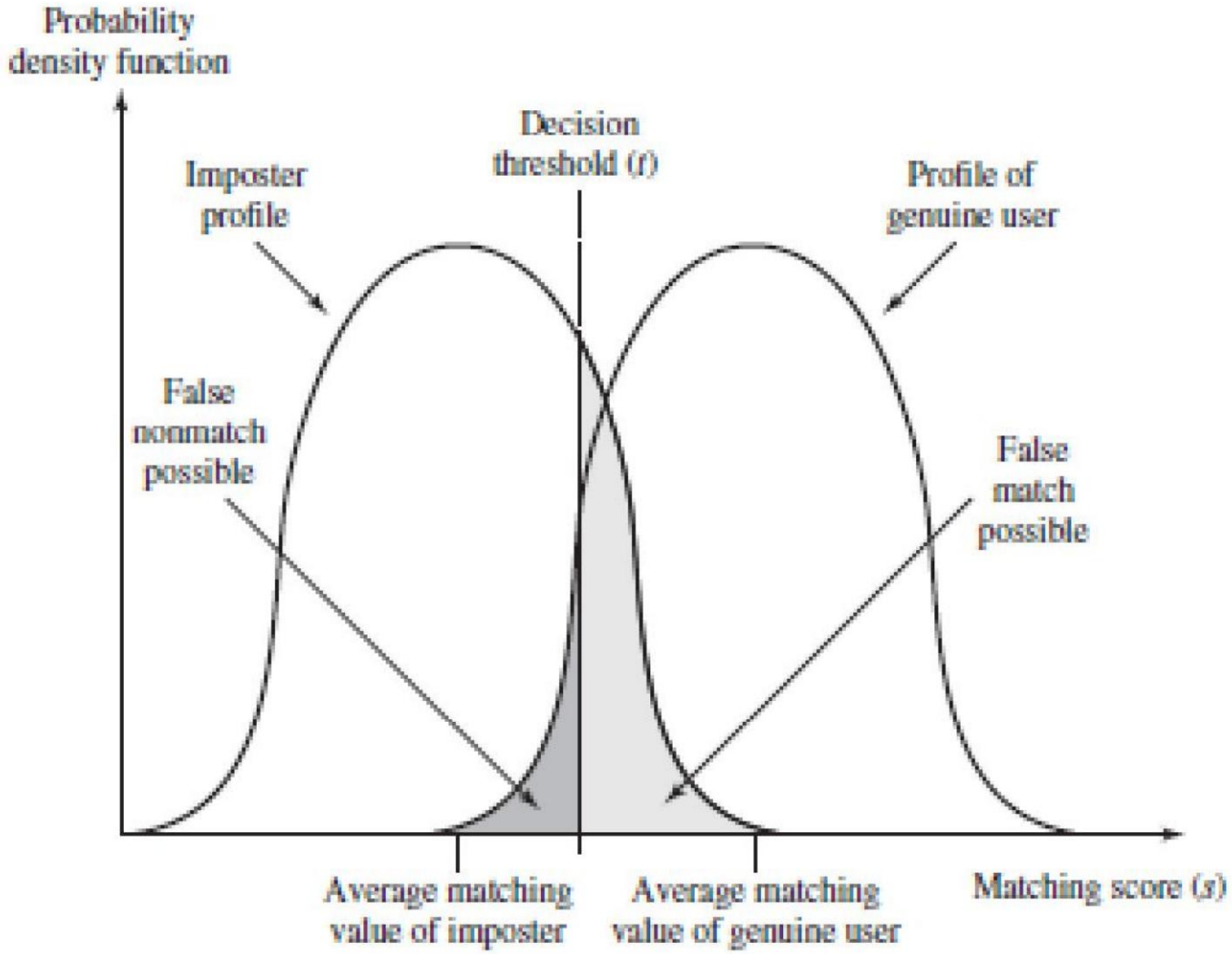


Figure 3.9 **Profiles of a Biometric Characteristic of an Imposter and an Authorized User** In this depiction, the comparison between the presented feature and a reference feature is reduced to a single numeric value. If the input value (s) is greater than a preassigned threshold (t), a match is declared.

Precisión biométrica

- puede
  trazar una curva característica
- seleccionar tasas
  de error de equilibrio del umbral

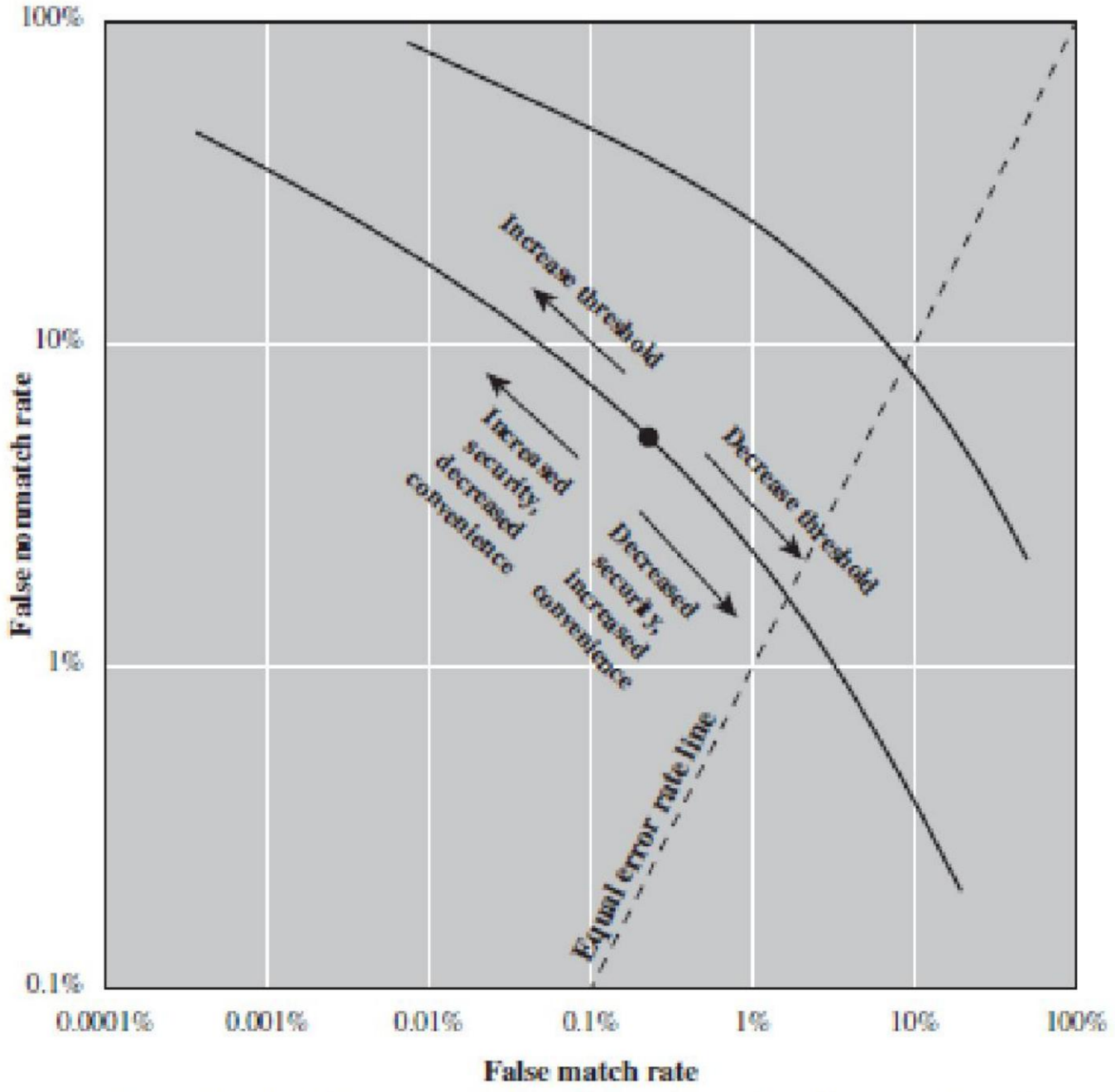


Figure 3.10 Idealized Biometric Measurement Operating Characteristic Curves (log-log scale)

Protocolos de autenticación

• se utiliza para convencer a las partes de la comunicación de la identidad de cada una y para intercambiar claves de sesión •

puede ser unidireccional o mutua • las

cuestiones clave

son • confidencialidad: para evitar el enmascaramiento y proteger las claves de sesión • puntualidad: para evitar ataques de reproducción de mensajes

Autenticación remota de usuarios mediante Cifrado simétrico

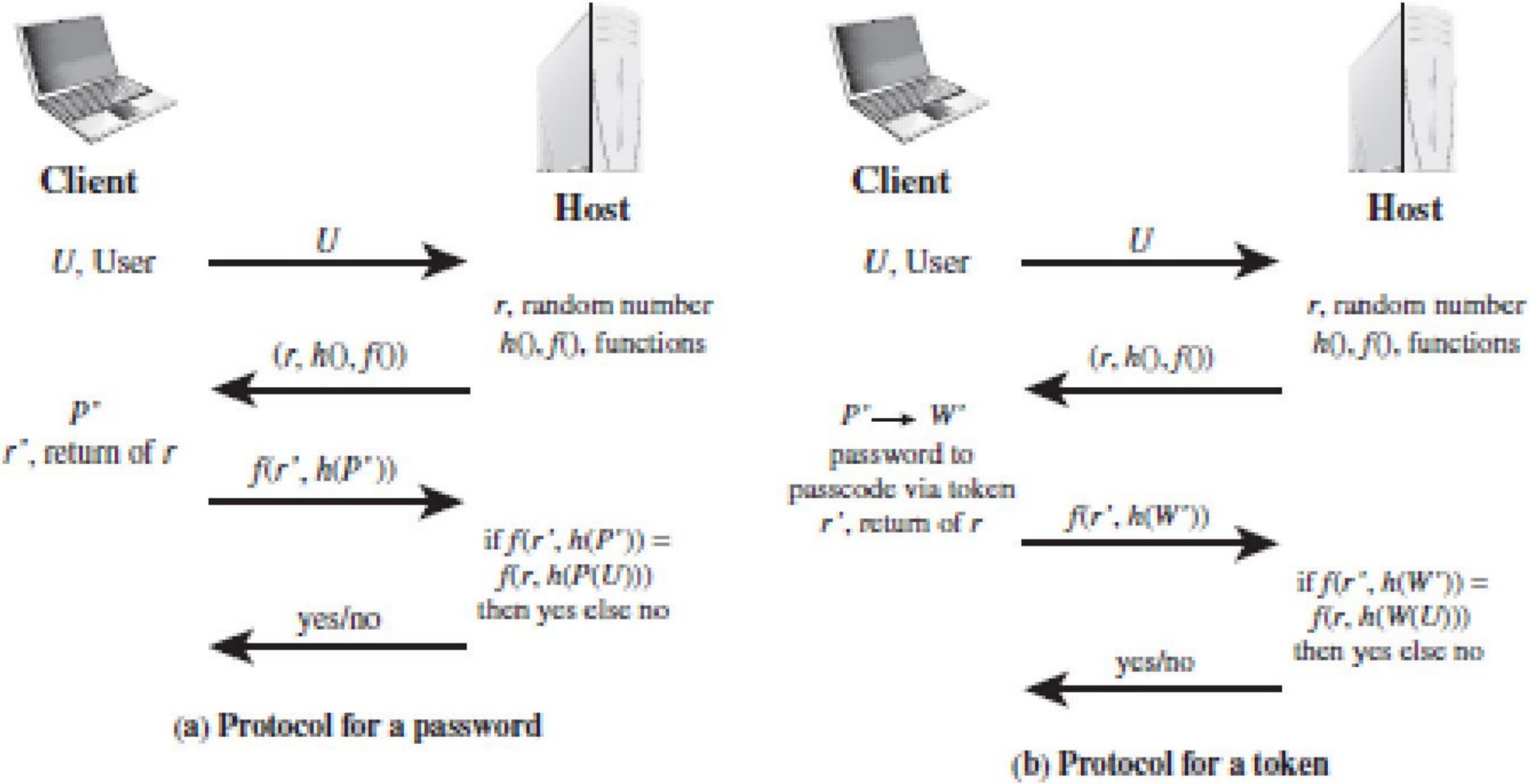
- utilizando KDC y jerarquía de claves (Protocolo Needham-Schroeder) •

vulnerable a un ataque de repetición si una clave de sesión antigua Ks ha sido comprometida, entonces el atacante X puede

- hacerse pasar por A y engañar a B para que use la antigua Ks reproduciendo el

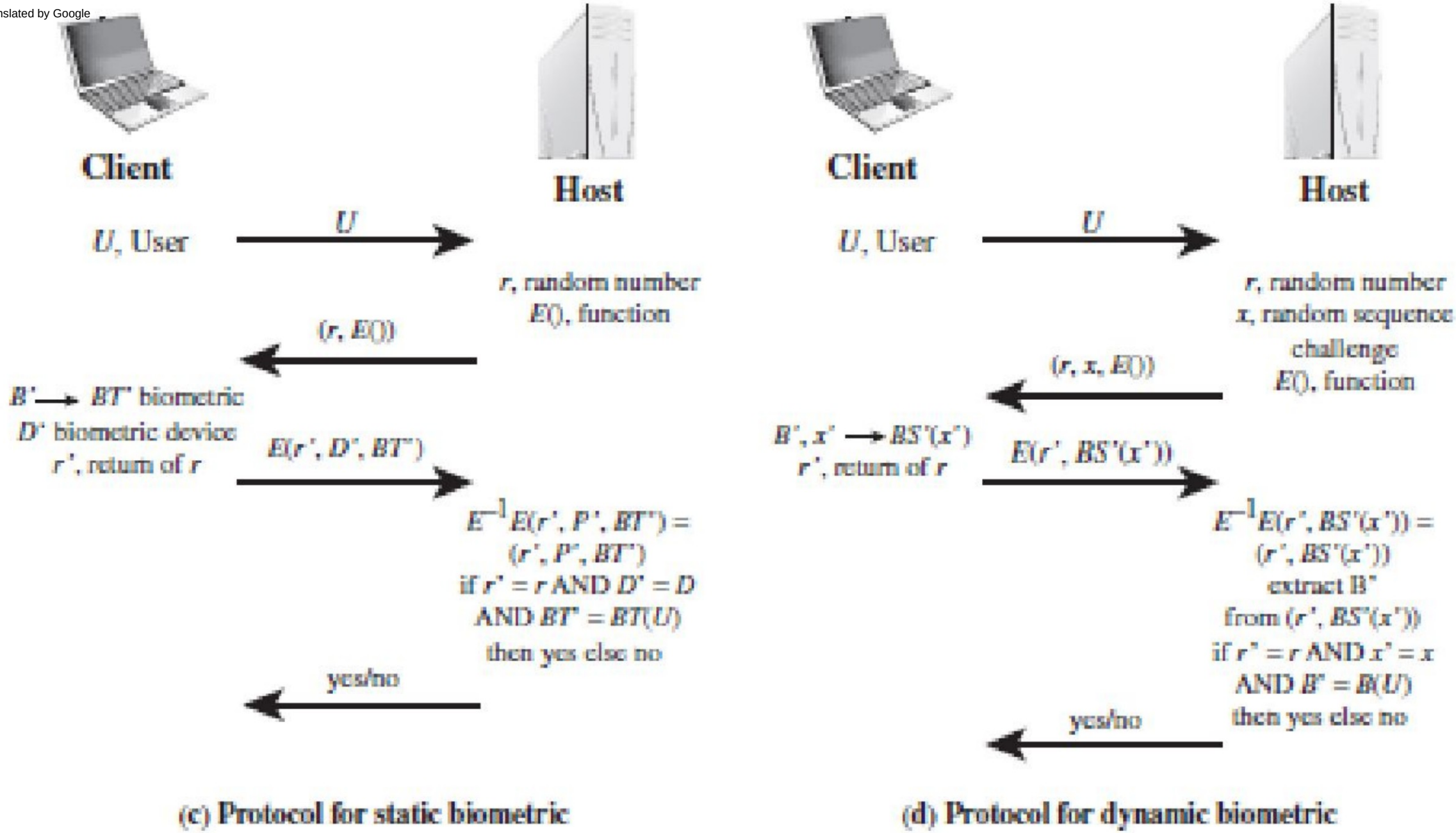
mensaje 3 • interceptar el mensaje 4, hacerse pasar por la respuesta de A en el mensaje 5

- hacerse pasar por A para una comunicación más segura



(a) Protocol for a password

(b) Protocol for a token



(c) Protocol for static biometric

(d) Protocol for dynamic biometric

Figure 3.12 Basic Challenge-Response Protocols for Remote User Authentication

Source: Based on [OGOR03].

Kerberos

- servicio de autenticación confiable del MIT
- proporciona autenticación mutua centralizada en una red distribuida
  - permite a los usuarios acceder a servicios distribuidos en la red
  - no se puede confiar en que una estación de trabajo identifique a su usuario • más bien, todos confían en un servidor de autenticación central
  - se basa exclusivamente en cifrado simétrico • requiere que el usuario demuestre su identidad para cada servicio invocado, también requiere que los servidores demuestren la identidad de su usuario
- dos versiones en uso: versión 4 (1988) y 5 (1994)

Requisitos de Kerberos

- requisitos en su primer informe publicado:
  - seguro
  - Arquitectura de servidor distribuida y confiable
  - transparente: los usuarios solo necesitan ingresar contraseñas •
    escalable: arquitectura distribuida
- Por lo tanto, un servicio de autenticación de terceros de confianza •
  Los clientes y servidores confían en Kerberos
- implementado utilizando un protocolo de autenticación basado en Needham-Schroeder

Descripción general de Kerberos v4

• un esquema básico de autenticación de terceros • tener un

servidor de autenticación (AS) • conoce las contraseñas

de todos los usuarios • los usuarios negocian

inicialmente con AS para identificarse • AS proporciona una credencial

de autenticación incorruptible (ticket que otorga tickets)

(TGT-T)

• tener un servidor de concesión de tickets (TGS) • los

usuarios presentan posteriormente el TGT al TGS para adquirir el ticket de concesión de servicios

(SGT) para acceder a servicios específicos

• utilizando un protocolo complejo basado en DES

Acciones en Kerberos v4

Problemas de seguridad de autenticación

- ataques de clientes
- ataques de host
- escuchas clandestinas
-

reproducción •

caballo de Troya • denegación de servicio

- phishing

PwdHash

- PwdHash (Ross, B., Jackson, C., Miyake, N., Boneh, D., Mitchell, JC: Autenticación de contraseñas más segura mediante extensiones de navegador. En: Actas del Simposio de seguridad de USENIX, 2005)
- Banco A
- Hash (PwdA, BankA) •

Banco A falsificado •

Hash (PwdA, SpoofedBankA)

- PwdHash
- (Extensión del navegador)
- Contraseña de texto sin formato:

PwdA • Contraseña del sitio: Hash (PwdA,

BankA) • Contraseña única por sitio (el nombre de dominio es la

sal) • Se centra en la protección contra ataques de phishing

Resumen

- Se introdujo la autenticación de usuarios.
  - utilizando contraseñas
  - utilizando tokens
  - utilizando biometría
- autenticación de usuario remoto
- Kerberos