# Sicurezza

## CdL in Informatica – L31

## Lezione 2 – Autenticazione degli utenti

Prof. Emiliano Casalicchio
Department of Computer Science
Sapienza University of Rome

SAPIENZA
UNIVERSITÀ DI ROMA

NIST SP 800-63-3 (*Digital Authentication Guideline*, October 2016) defines digital user authentication as:

"The process of establishing confidence in user identities that are presented electronically to an information system."

Il processo per stabilire la fiducia nelle identità degli utenti che sono presentate elettronicamente a un sistema informativo

# Differenza tra identificazione e autenticazione

- Identificazione: l'utente fornisce un identità presunta
- Autenticazione: modo per stabilire la validità dell'identità presunta

# Auth utenti vs Auth messaggi

- Autenticazione dei messaggi è una procedura che permette alle parti comunicanti di verificare
  - che il contenuto di un messaggio ricevuto non sia stato alterato
  - che la fonte sia autentica

# Uso dell'identità autenticata

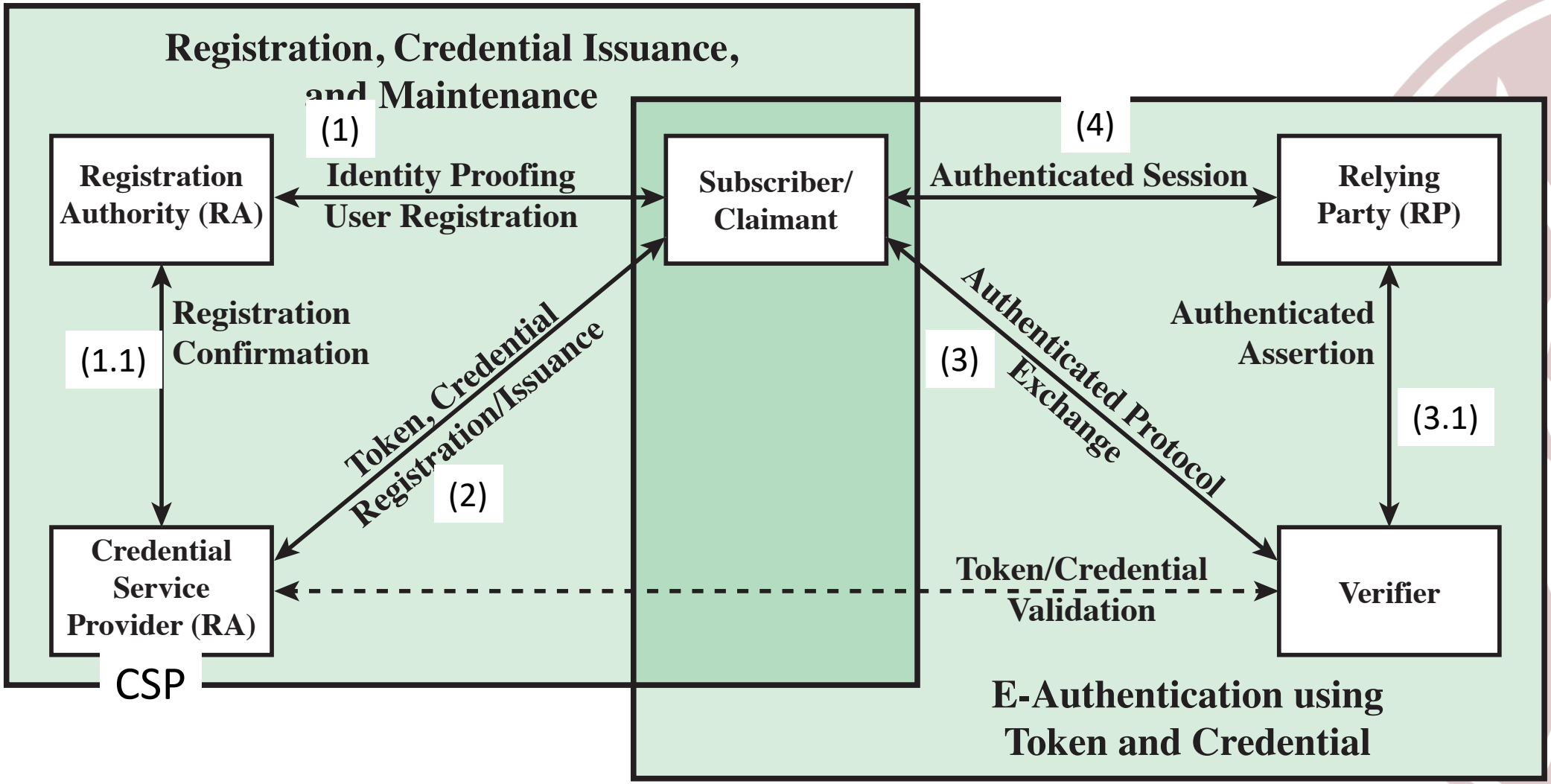
- Autorizzare transazioni / funzionalità
- Autorizzare l'accesso a particolari risorse
  - File
  - Processi
  - Dispositivi

# Requisiti di sicurezza per servizi di identificazione e autenticazione NIST 800-171

| **Basic Security Requirements**: | |
|---|---|
| **1** | Identify information system users, processes acting on behalf of users, or devices. |
| **2** | Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. |

| **Derived Security Requirements**: | |
|---|---|
| **3** | Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. |
| **4** | Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts. |
| **5** | Prevent reuse of identifiers for a defined period. |
| **6** | Disable identifiers after a defined period of inactivity. |
| **7** | Enforce a minimum password complexity and change of characters when new passwords are created. |
| **8** | Prohibit password reuse for a specified number of generations. |
| **9** | Allow temporary password use for system logons with an immediate change to a permanent password. |
| **10** | Store and transmit only cryptographically-protected passwords. |
| **11** | Obscure feedback of authentication information. |

# Modello generale autenticazione utenti NIST SP 800-63-3



# Mezzi di autenticazione

| Something the individual knows | Something the individual possesses (token) | Something the individual is (static biometrics) | Something the individual does (dynamic biometrics) |
|---|---|---|---|
| • Password, PIN, answers to prearranged questions | • Smartcard, electronic keycard, physical key | • Fingerprint, retina, face | • Voice pattern, handwriting, typing rhythm |

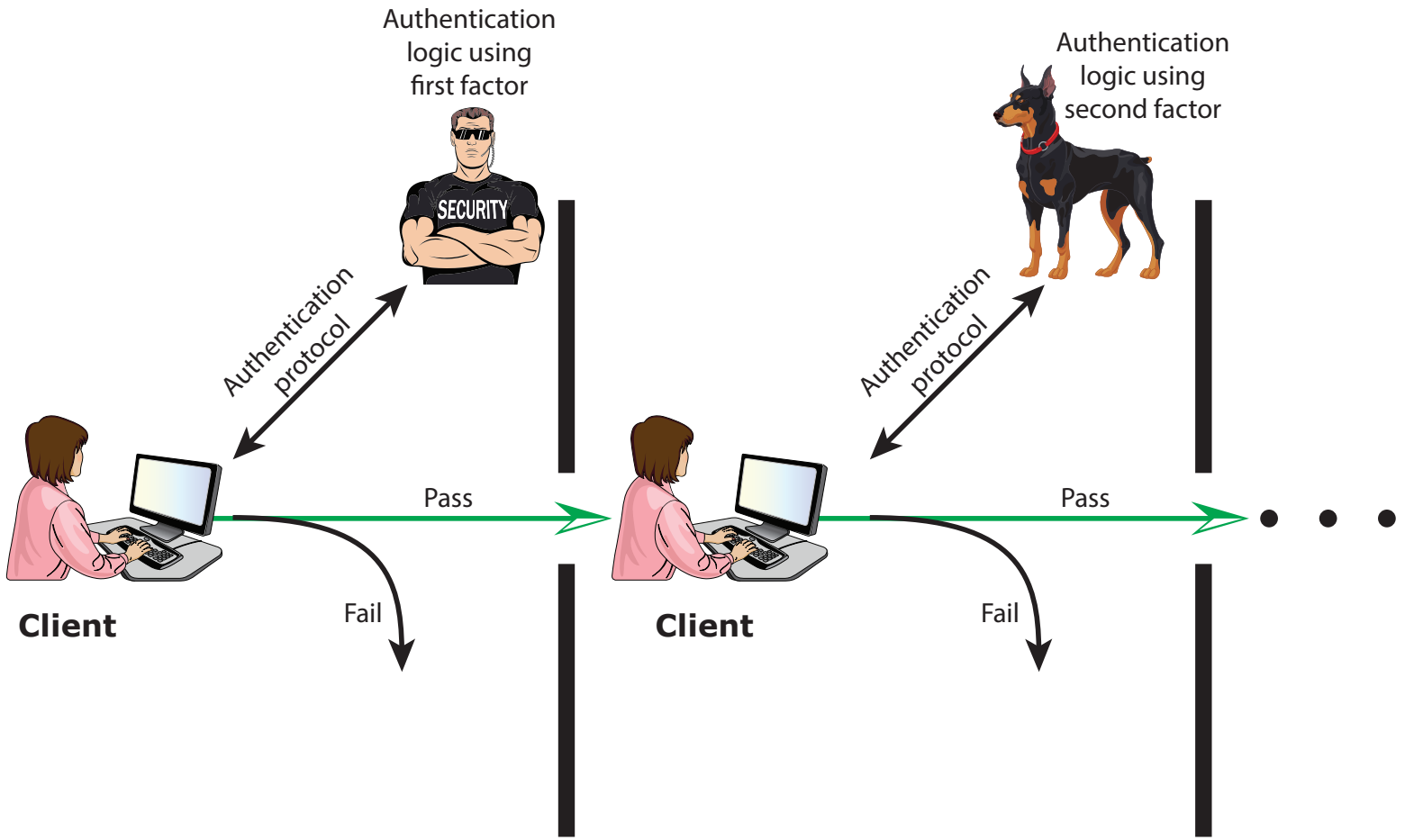
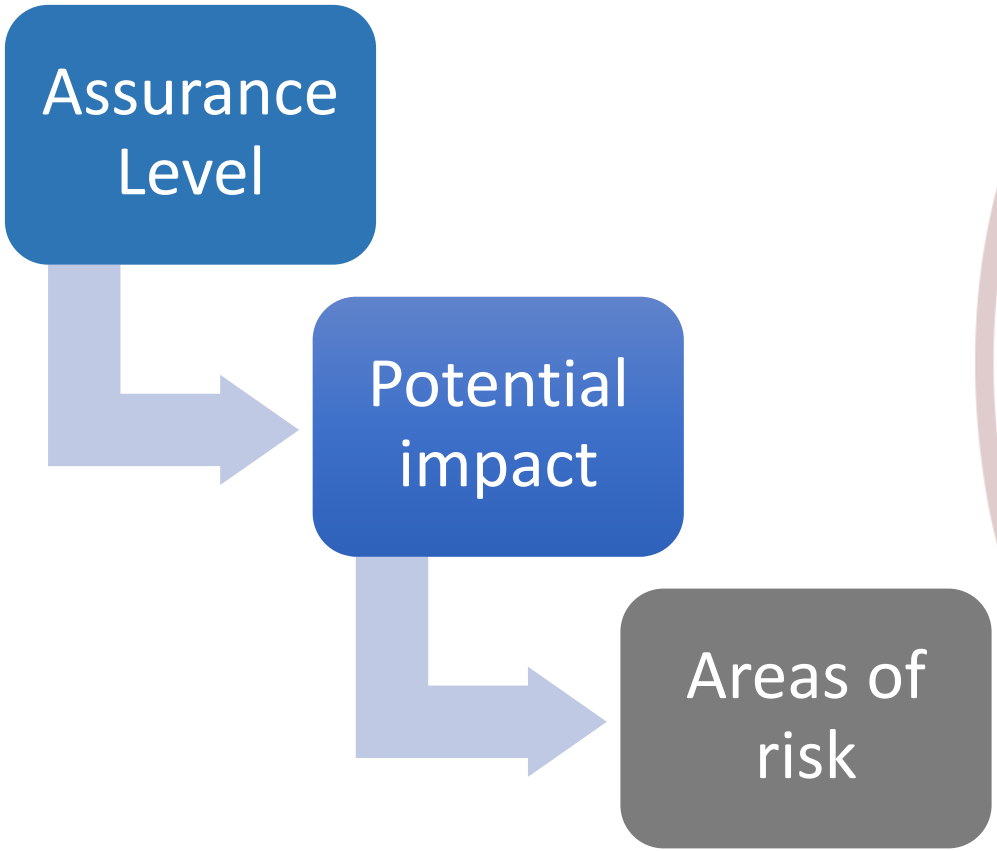



**Figure 3.2 Multifactor Authentication**

# Valutazione dei rischi per l'autenticazione degli utenti

- There are three separate concepts:



# Assurance Level (Livello di garanzia)

Describes an organization's degree of certainty that a user has presented a credential that refers to his or her identity

More specifically is defined as:

The degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued

The degree of confidence that the individual who uses the credential is the individual to whom the credential was issued

Four levels of assurance SP 800-63-3

Level 1 - Little or no confidence in the asserted identity's validity

Level 2- Some confidence in the asserted identity's validity

Level 3 - High confidence in the asserted identity's validity

Level 4 - Very high confidence in the asserted identity's validity

# Potential Impact (impatto potenziale)

- FIPS 199 defines three levels of potential impact on organizations or individuals should there be a breach of security (**fallimento autenticazione**):
  - Low
    - An authentication error could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals
  - Moderate
    - An authentication error could be expected to have a serious adverse effect
  - High
    - An authentication error could be expected to have a severe or catastrophic adverse effect

# Area of Risk (aree di rischio)

- Per un dato sistema informativo o risorsa di servizio, l'organizzazione a cui appartiene deve determinare il livello di impatto se si verifica un errore di autenticazione, usando le **Categorie di Impatto** o **Aree di Rischio** che destano preoccupazione

# Maximum Potential Impacts for Each Assurance Level

Tecnica per effettuare la valutazione dei rischi: un esempio

Livelli di garanzia

| Aree di rischio | Assurance Level Impact Profiles | | | |
|---|---|---|---|---|
| **Potential Impact Categories for Authentication Errors** | 1 | 2 | 3 | 4 |
| Inconvenience, distress, or damage to standing or reputation | Low | Mod | Mod | High |
| | Low | Mod | Mod | High |
| Financial loss or organization liability | None | Low | Mod | High |
| Harm to organization programs or interests | None | Low | Mod | High |
| Unauthorized release of sensitive information | None | None | Low | Mod/ High |
| Personal safety | | | | |
| Civil or criminal violations | None | Low | Mod | High |

# Password-Based Authentication

- Widely used line of defense against intruders
  - User provides name/login and password
  - System compares password with the one stored for that specified login
- The user ID:
  - Determines that the user is authorized to access the system
  - Determines the user's privileges
  - Is used in discretionary access control (**controllo degli accessi discrezionale**)

# Password Vulnerabilities

- Offline dictionary attack
- Specific account attack
- Popular password attack
- Password guessing against single user
- Workstation hijacking
- Exploiting user mistakes
- Exploiting multiple password use
- Electronic monitoring

# Offline dictionary attack

- Attaccante ottiene accesso al file delle password
- Confronto hash password con hash password uso comune
  - Se successo – uso ID/password trovata

- Contromisure
  - Controlli per prevenire accesso a file password
  - Intrusion detection per determinare accesso/compromissione del file password

# Specific account attack

- L'attaccante seleziona uno specifico account e tenta varie password

- Contromisura
  - Meccanismo di blocco account dopo n tentativi falliti

# Popular password attack

- L'attaccante seleziona una password usata comunemente e la testa contro una vasta gamma di ID

- Contromisura
  - Politiche per inibire la scelta di password comuni
  - Scansione IP e cockies da cui vengono richieste di autenticazione per monitorare sequenze di sottomissioni

# Password guessing against single user

- Attaccante acquisisce
  - Conoscenze sulle abitudini singolo utente
  - Politiche di gestione password
- Contromisure
  - Politiche di gestione delle password che le rendano difficili da indovinare

# Workstation hijacking

- Attaccante aspetta che una workstation con login attivo sia incostodita

- Contromisure
  - Logout automatico / blocco schermo
  - Intrusion detection per rilevare cambiamenti nel comportamento degli utenti

# Exploiting user mistakes

- Password scritte su fogli
- Condivisione password con colleghi
- Ingegneria sociale (phishing)
- Password preconfigurate

- Contromisure
  - Educazione utenti (awarness)
  - Intrusion detection
  - Autenticazione a più fattori

# Exploiting multiple password use

- Quanto si usa la stessa password o password simili per più servizi/dispositivi di rete

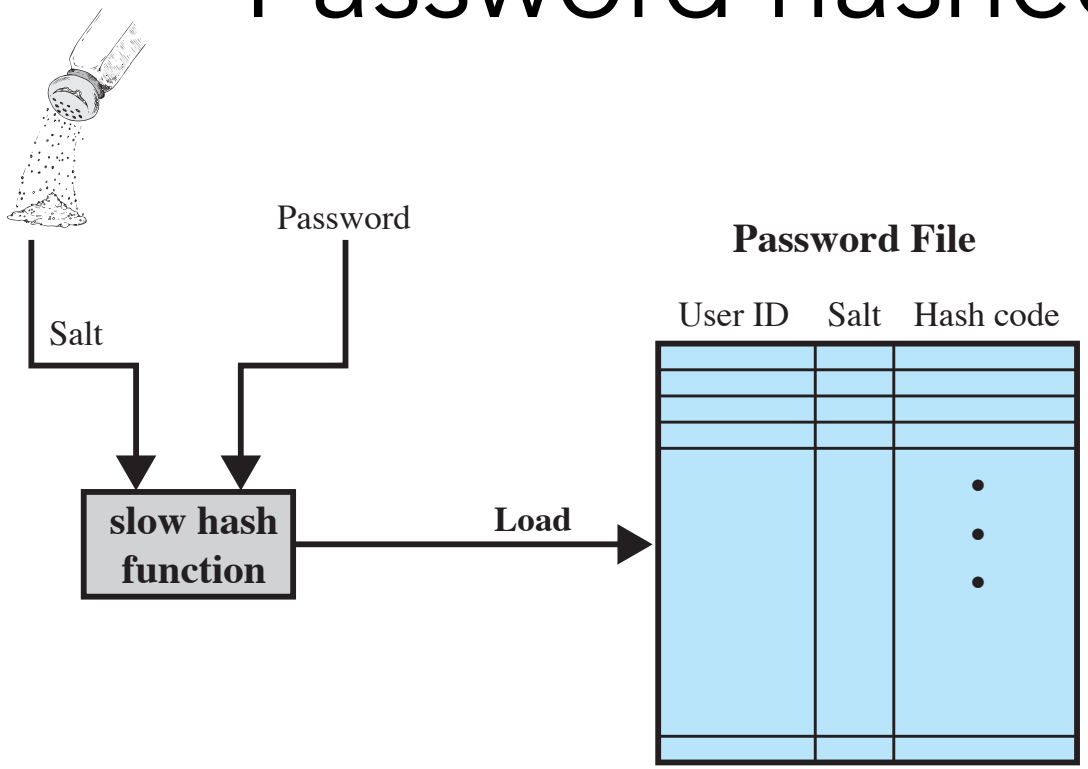
- Contromisure
  - Politiche per vietare l'uso di password uguali o simili

# Electronic monitoring

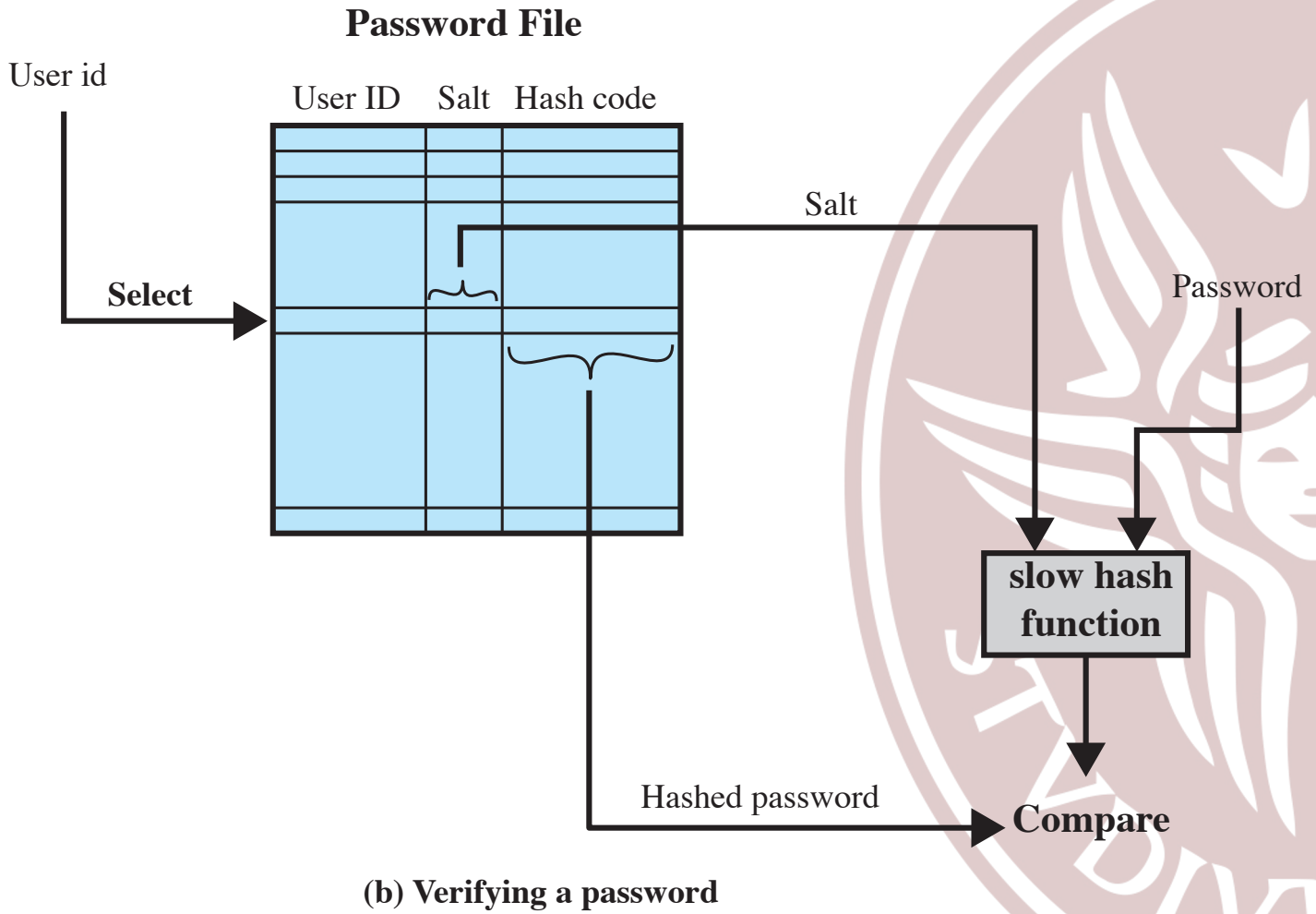
- L'attaccante intercetta una password che viene trasmessa via rete per accedere ad un sistema remoto

- Contromisure
  - La sola cifratura della password non basta
  - Protocolli di comunicazione sicura

# Password hashed (Schema Unix)




(a) Loading a new password

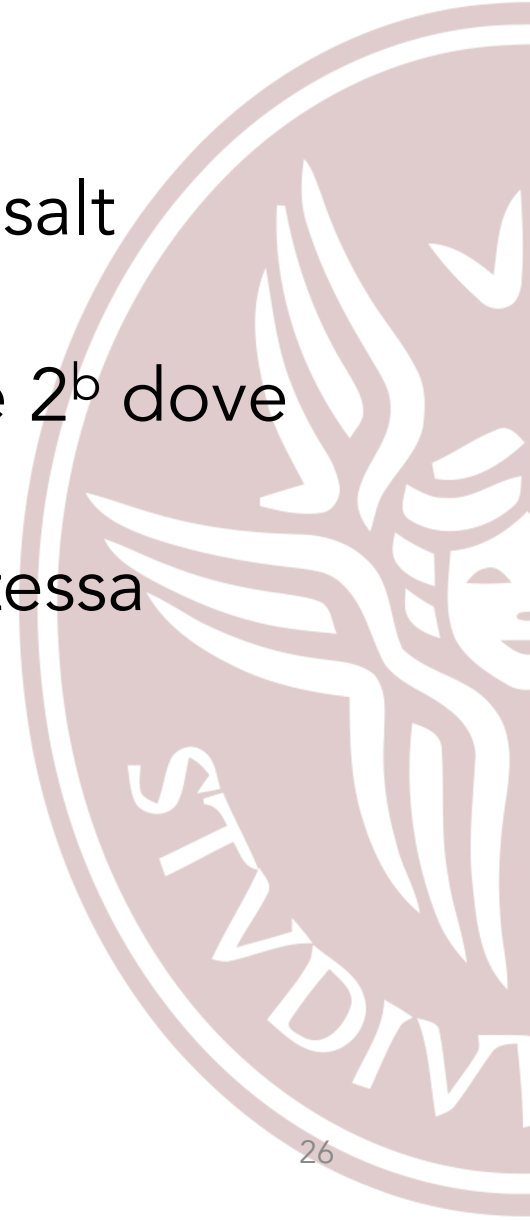



(b) Verifying a password

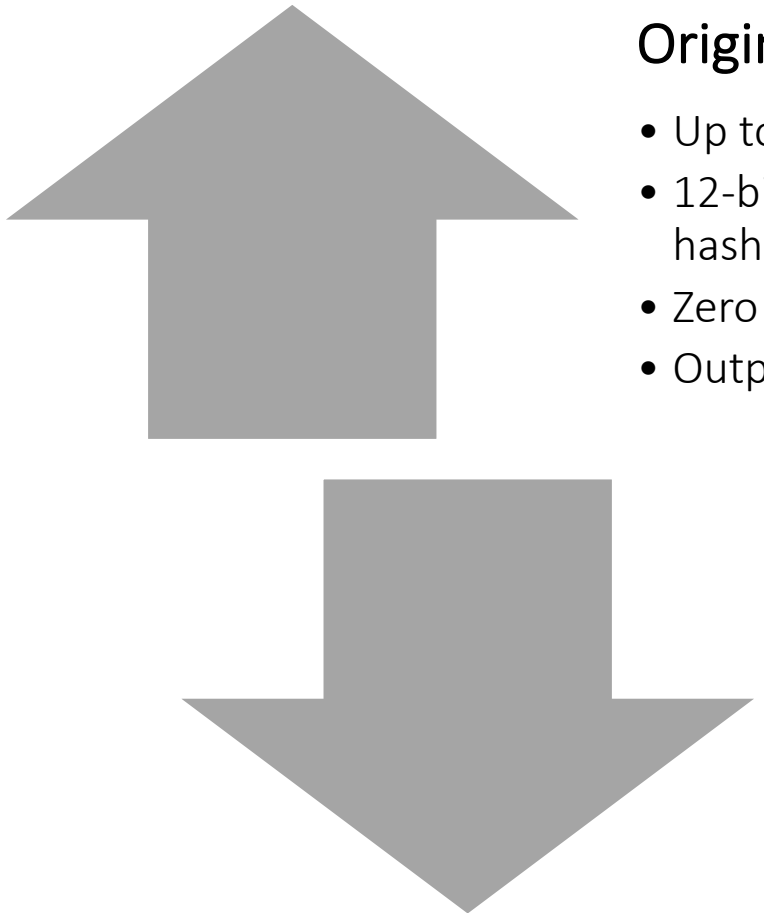
**Figure 3.3 UNIX Password Scheme**

# Vantaggi nell'uso del Salt

- Impedisce che password uguali siano visibili (avranno salt diversi e quindi hash values diversi
- Aumenta la difficolta' degli attachi offline di un fattore $2^b$ dove b e' il numero di bit del salt
- Rende impossibile scoprire se un utente ha usato la stessa password su 2 o piu' sistemi



# UNIX Implementation



## Original scheme (crypt(3))

- Up to eight printable characters in length (→56bit key)
- 12-bit salt used to modify DES encryption into a one-way hash function
- Zero value repeatedly encrypted 25 times
- Output translated to 11 character sequence

## Now regarded as inadequate

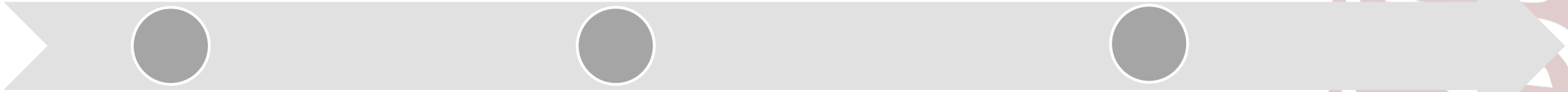
- Still often required for compatibility with existing account management software or multivendor environments

# Improved Implementations

Much stronger hash/salt schemes available for Unix

OpenBSD uses Blowfish block cipher based hash algorithm called Bcrypt

- Most secure version of Unix hash/salt scheme
- Uses 128-bit salt to create 192-bit hash value



Recommended hash function is based on MD5

- Salt of up to 48-bits
- Password length is unlimited
- Produces 128-bit hash
- Uses an inner loop with 1000 iterations to achieve slowdown

# Password Cracking

## Dictionary attacks

- Develop a large dictionary of possible passwords and try each against the password file
- Each password must be hashed using each salt value and then compared to stored hash values

## Rainbow table attacks

- Pre-compute tables of hash values for all salts
- A mammoth table of hash values
- Can be countered by using a sufficiently large salt value and a sufficiently large hash length

## Password crackers exploit the fact that people choose easily guessable passwords

- Shorter password lengths are also easier to crack (avg 6-8 chars 2012/70K)

## John the Ripper

- Open-source password cracker first developed in in 1996
- Uses a combination of brute-force and dictionary techniques

# Modern Approaches

- Complex password policy
  - Forcing users to pick stronger passwords
- However password-cracking techniques have also improved
  - The processing capacity available for password cracking has increased dramatically
  - The use of sophisticated algorithms to generate potential passwords
    - Probability of characters in natural language + Markov model
  - Studying examples and structures of actual passwords in use
    - Based on large datasets of leaked password
    - probabilistic context-free gramma

with a complex password policy

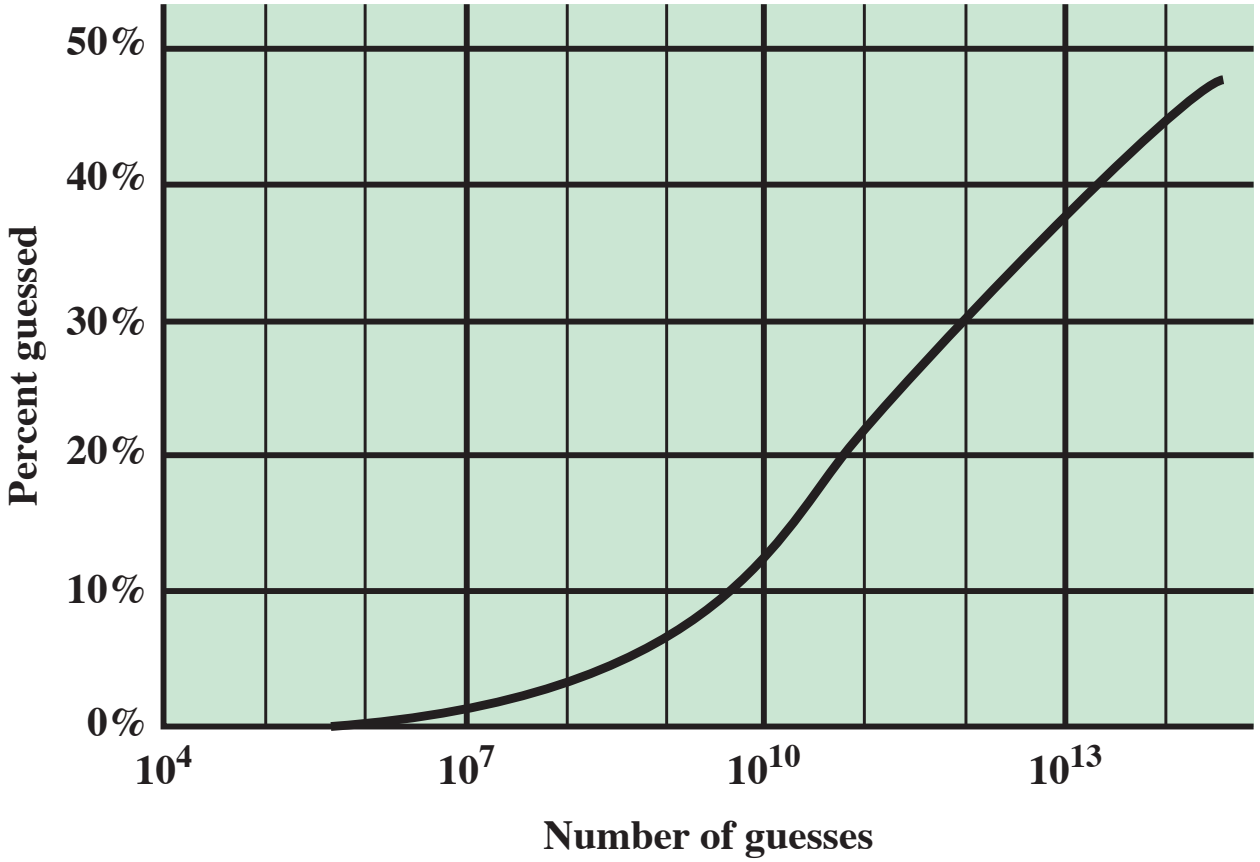



**Figure 3.4 The Percentage of Passwords Guessed After a Given Number of Guesses**

# Password File Access Control

**Can block offline guessing attacks by denying access to encrypted passwords**

- **Make available only to privileged users**
- **Shadow password file**

**Vulnerabilities**

- **Weakness in the OS that allows access to the file**
- **Accident with permissions making it readable**
- **Users with same password on other systems**
- **Access from backup media**
- **Sniff passwords in network traffic**

# Password Selection Strategies

## User education

Users can be told the importance of using hard to guess passwords and can be provided with guidelines for selecting strong passwords

## Computer generated passwords

Users have trouble remembering them

## Reactive password checking

System periodically runs its own password cracker to find guessable passwords

## Complex password policy

User is allowed to select their own password, however the system checks to see if the password is allowable, and if not, rejects it

Goal is to eliminate guessable passwords while allowing the user to select a password that is memorable

# Proactive Password Checking

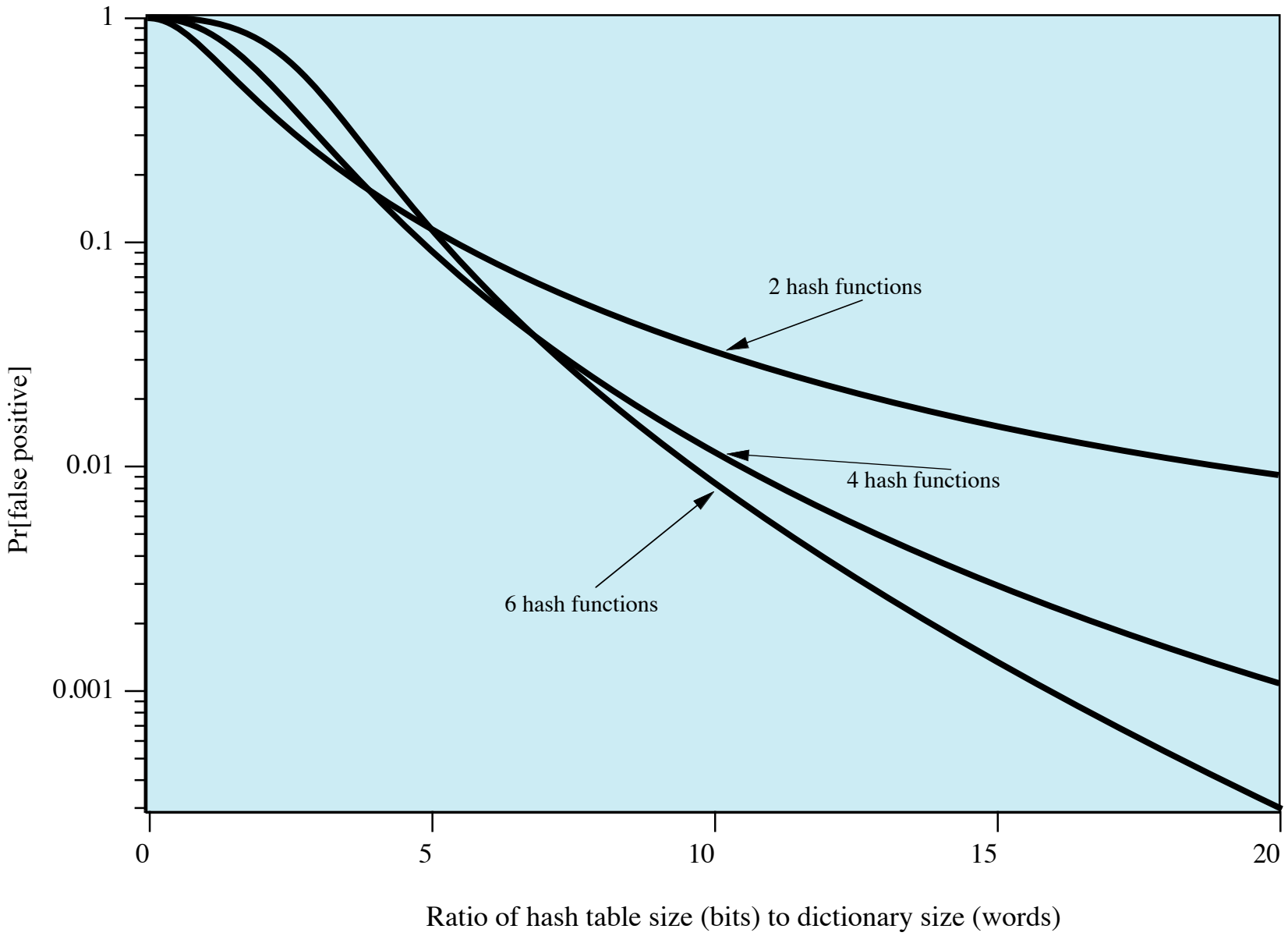
| | |
|---|---|
| Rule enforcement | • Specific rules that passwords must adhere to |
| Password checker | • Compile a large dictionary of passwords not to use |
| Bloom filter | • Used to build a table based on hash values<br>• Check desired password against this table |

# Bloom filter

- Dizionario passwordd di dimensione D (parole), X parola
- K funzioni hash Hi che producono una output intero [0,N-1]
- Ad ogni parola X in D vengono applicate le K funzioni hash
- In una tabella di dim N bit, il bit Hi(X), viene settato ad 1

- Quando l'utente inserisce una password, vengono calcolate le K funzioni hash e se tutti i bit della tabella sono a 1 la password e' rifiutata

- Prob Falsi Positivi si riduce incrementando N e K, N>>D
- Tempo calcolo hash indipendente da D, confronto tempo costante.


1
0.1
0.01
0.001
Pr[false positive]
2 hash functions
4 hash functions
6 hash functions
0
5
10
15
20
Ratio of hash table size (bits) to dictionary size (words)

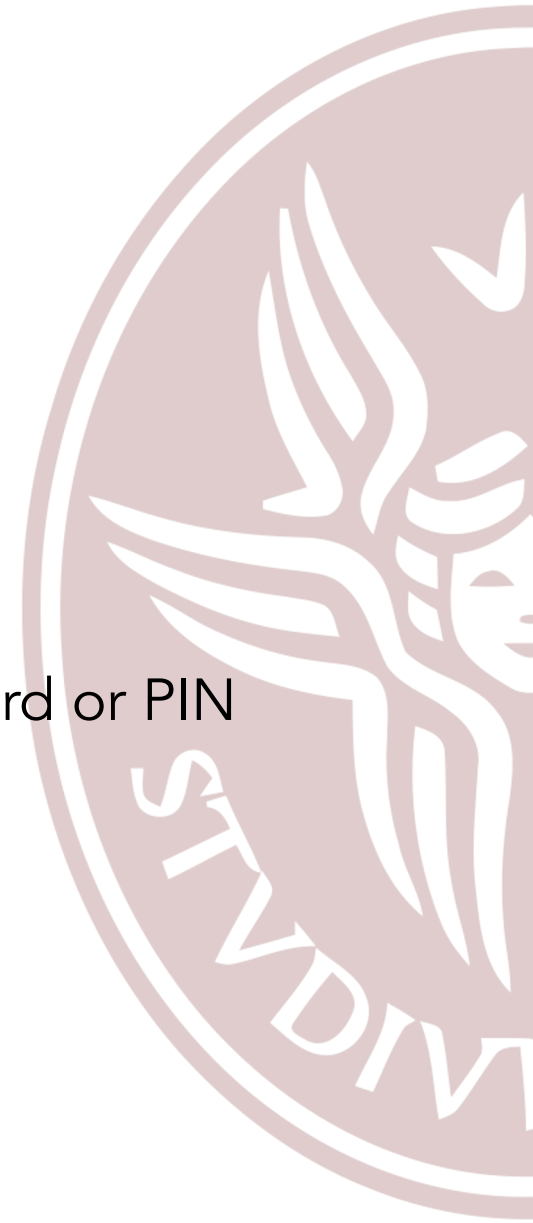
# Autenticazione basata su token

| Card Type | Defining Feature | Example |
|---|---|---|
| Embossed | Raised characters only, on front | Old credit card |
| Magnetic stripe | Magnetic bar on back, characters on front | Bank card |
| Memory | Electronic memory inside | Prepaid phone card |
| Smart<br>Contact<br>Contactless | Electronic memory and processor inside<br>Electrical contacts exposed on surface<br>Radio antenna embedded inside | Biometric ID card |

Types of Cards Used as Tokens

# Memory Cards

- Can store but do not process data
- The most common is the magnetic stripe card
- Can include an internal electronic memory
- Can be used alone for physical access
  - Hotel room
  - ATM
- Provides significantly greater security when combined with a password or PIN
- Drawbacks of memory cards include:
  - Requires a special reader
  - Loss of token
  - User dissatisfaction

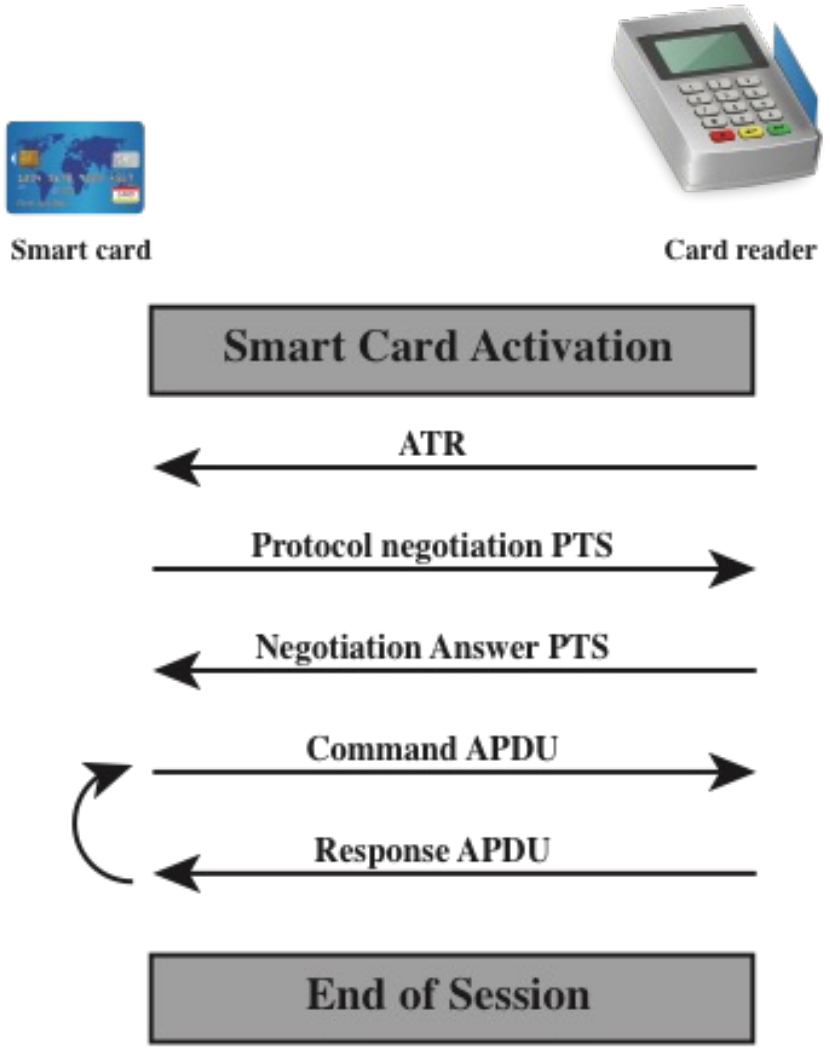


# Smart Tokens

- Physical characteristics:
  - Include an embedded microprocessor
  - A smart token that looks like a bank card
  - Can look like calculators, keys, small portable objects
- User interface:
  - Manual interfaces include a keypad and display for human/token interaction
- Electronic interface
  - A smart card or other token requires an electronic interface to communicate with a compatible reader/writer
  - Contact and contactless interfaces
- Authentication protocol:
  - Classified into three categories:
    - Static
    - Dynamic password generator
    - Challenge-response

# Smart Cards

- Most important category of smart token
  - Has the appearance of a credit card
  - Has an electronic interface
  - May use any of the smart token protocols
- Contain:
  - An entire microprocessor
    - Processor
    - Memory
    - I/O ports
- Typically include three types of memory:
  - Read-only memory (ROM)
    - Stores data that does not change during the card's life
  - Electrically erasable programmable ROM (EEPROM)
    - Holds application data and programs
  - Random access memory (RAM)
    - Holds temporary data generated when applications are executed




APDU = application protocol data unit
ATR = Answer to reset
PTS = Protocol type selection

**Figure 3.6 Smart Card/Reader Exchange**

# Electronic Identity Cards (eID)

**Use of a smart card as a national identity card for citizens**

- Can serve the same purposes as other national ID cards, and similar cards such as a driver's license, for access to government and commercial services
- Can provide stronger proof of identity and can be used in a wider variety of applications
- In effect, is a smart card that has been verified by the national government as valid and authentic

**Most advanced deployment is the German card *neuer Personalausweis***

- Has human-readable data printed on its surface
  - Personal data
  - Document number
  - Card access number (CAN)
  - Machine readable zone (MRZ)

# Table 3.4

## Electronic Functions and Data for eID Cards

| Function | Purpose | PACE Password | Data | Uses |
|---|---|---|---|---|
| ePass (mandatory) | Authorized offline inspection systems read the data | CAN or MRZ | Face image; two fingerprint images (optional), MRZ data | Offline biometric identity verification reserved for government access |
| eID (activation optional | Online applications read the data or acess functions as authorized | eID PIN | Family and given names; artistic name and doctoral degree: date and place of birth; address and community ID; expiration date | Identification; age verification; community ID verification; restricted identification (pseudonym); revocation query |
| | Offline inspection systems read the data and update the address and community ID | CAN or MRZ | | |
| eSign (certificate optional | A certification authority installs the signature certificate online | eID PIN | Signature key; X.509 certificate | Electronic signature creation |
| | Citizens make electronic signature with eSign PIN | CAN | | |

CAN = card access number
MRZ = machine readable zone
PACE = password authenticated connection establishment
PIN = personal identification number

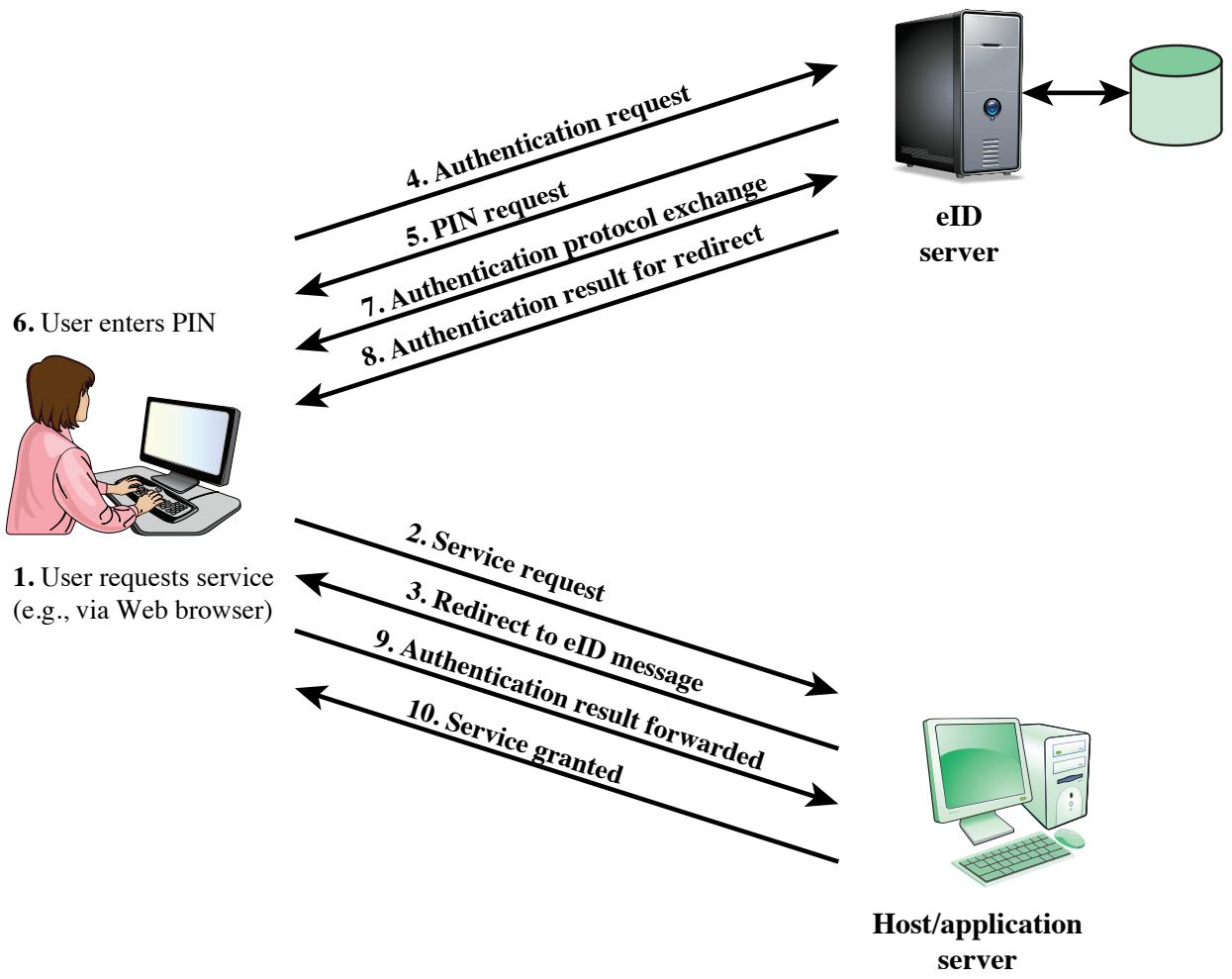



**Figure 3.7 User Authentication with eID**

# Password Authenticated Connection Establishment (PACE)

Ensures that the contactless RF chip in the eID card cannot be read without explicit access control

For online applications, access is established by the user entering the 6-digit PIN (which should only be known to the holder of the card)

For offline applications, either the MRZ printed on the back of the card or the six-digit card access number (CAN) printed on the front is used

# Biometric Authentication

- Attempts to authenticate an individual based on unique physical characteristics
- Based on pattern recognition
- Is technically complex and expensive when compared to passwords and tokens
- Physical characteristics used include:
  - Facial characteristics
  - Fingerprints
  - Hand geometry
  - Retinal pattern
  - Iris
  - Signature
  - Voice

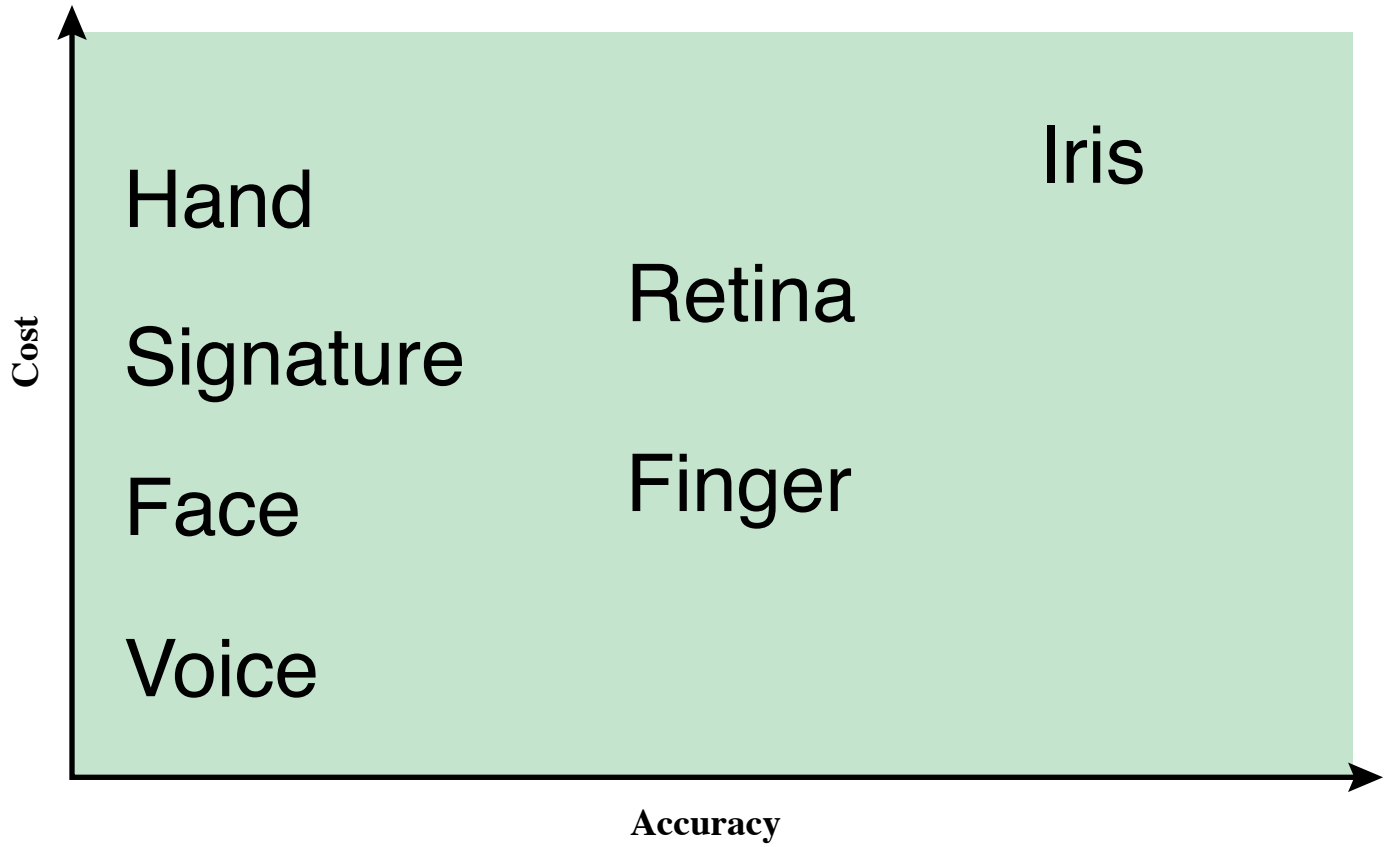



**Figure 3.8 Cost Versus Accuracy of Various Biometric Characteristics in User Authentication Schemes.**

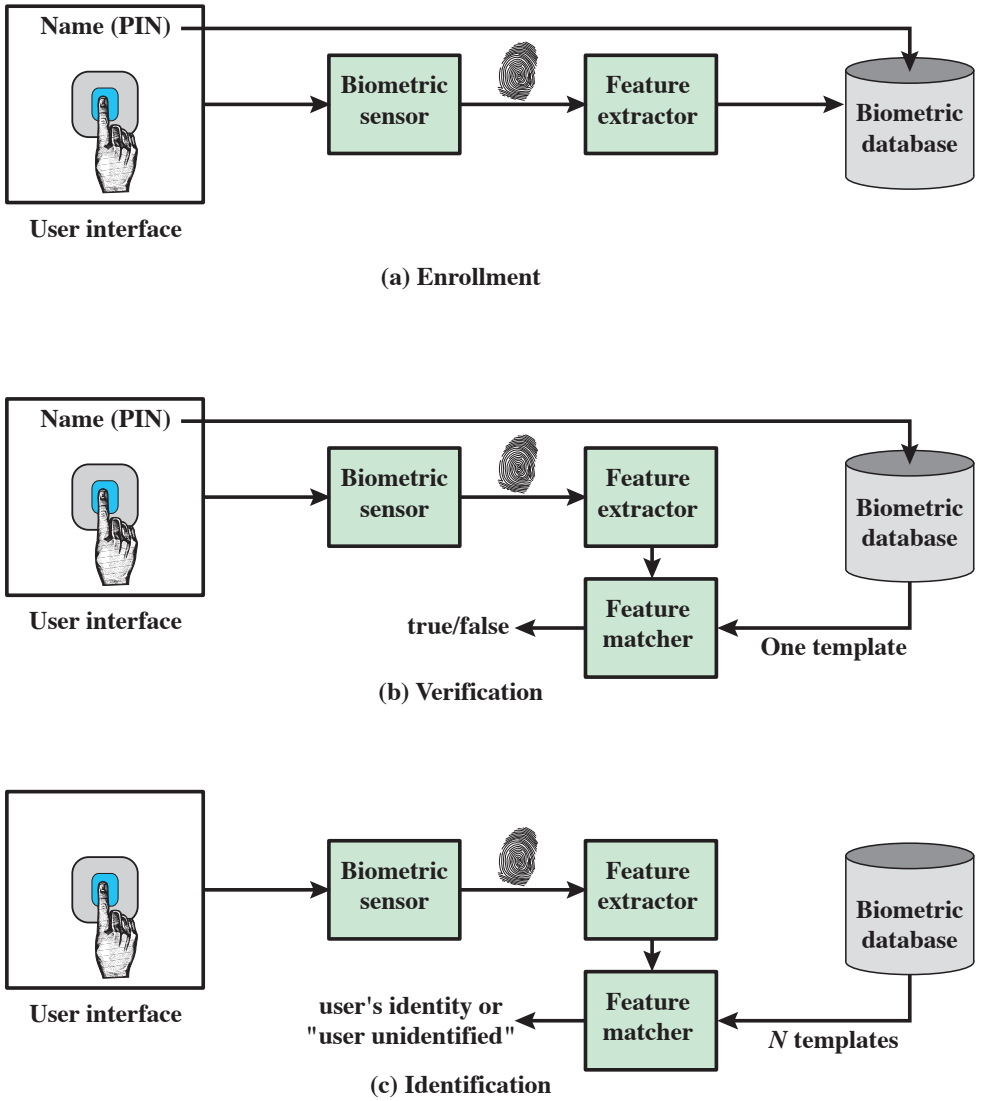



Figure 3.9 A Generic Biometric System. Enrollment creates an association between a user and the user's biometric characteristics. Depending on the application, user authentication either involves verifying that a claimed user is the actual user or identifying an unknown user.

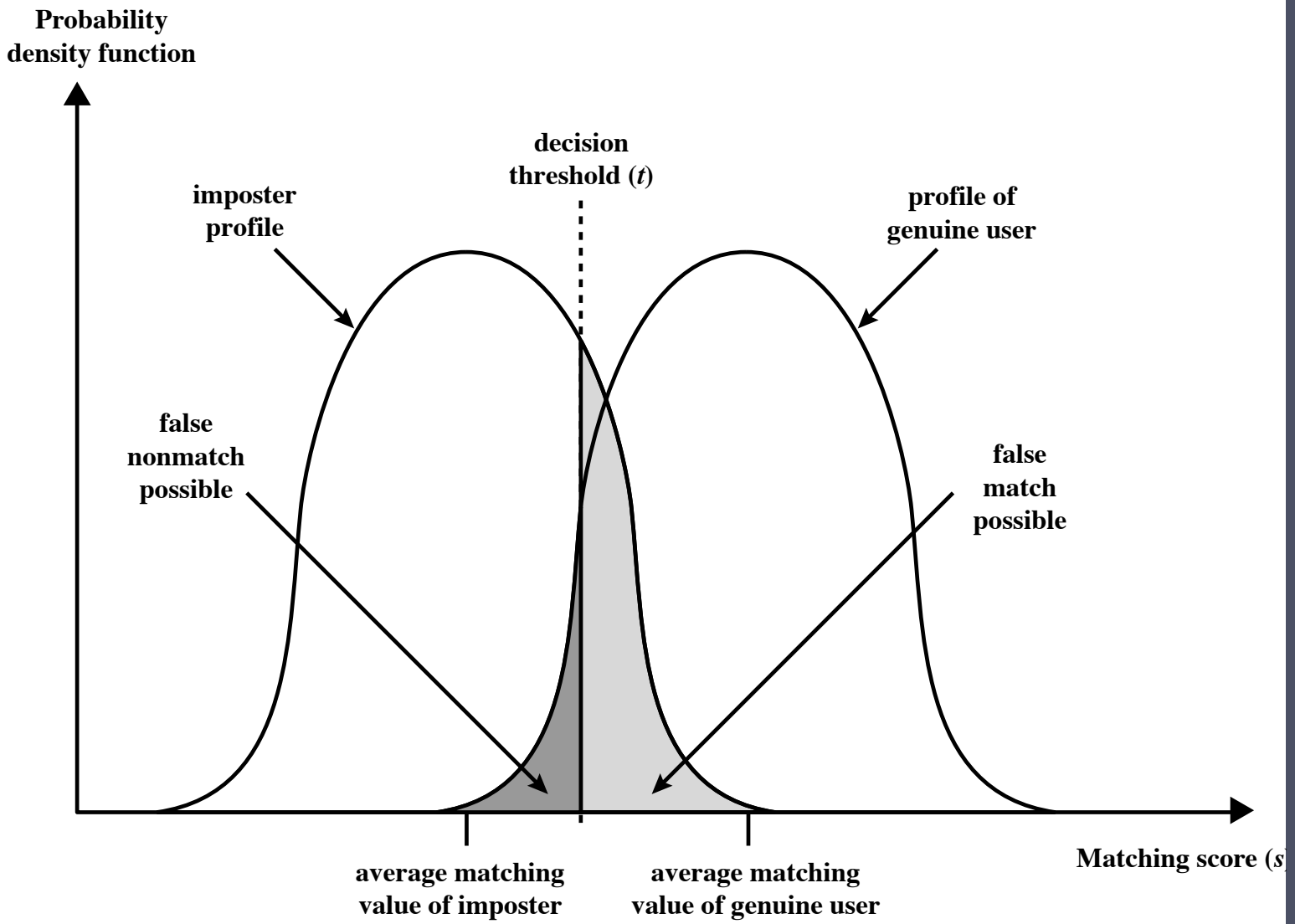



Figure 3.10 Profiles of a Biometric Characteristic of an Imposter and an Authorized Users In this depiction, the comparison between presented feature and a reference feature is reduced to a single numeric value. If the input value ($s$) is greater than a preassigned threshold ($t$), a match is declared.

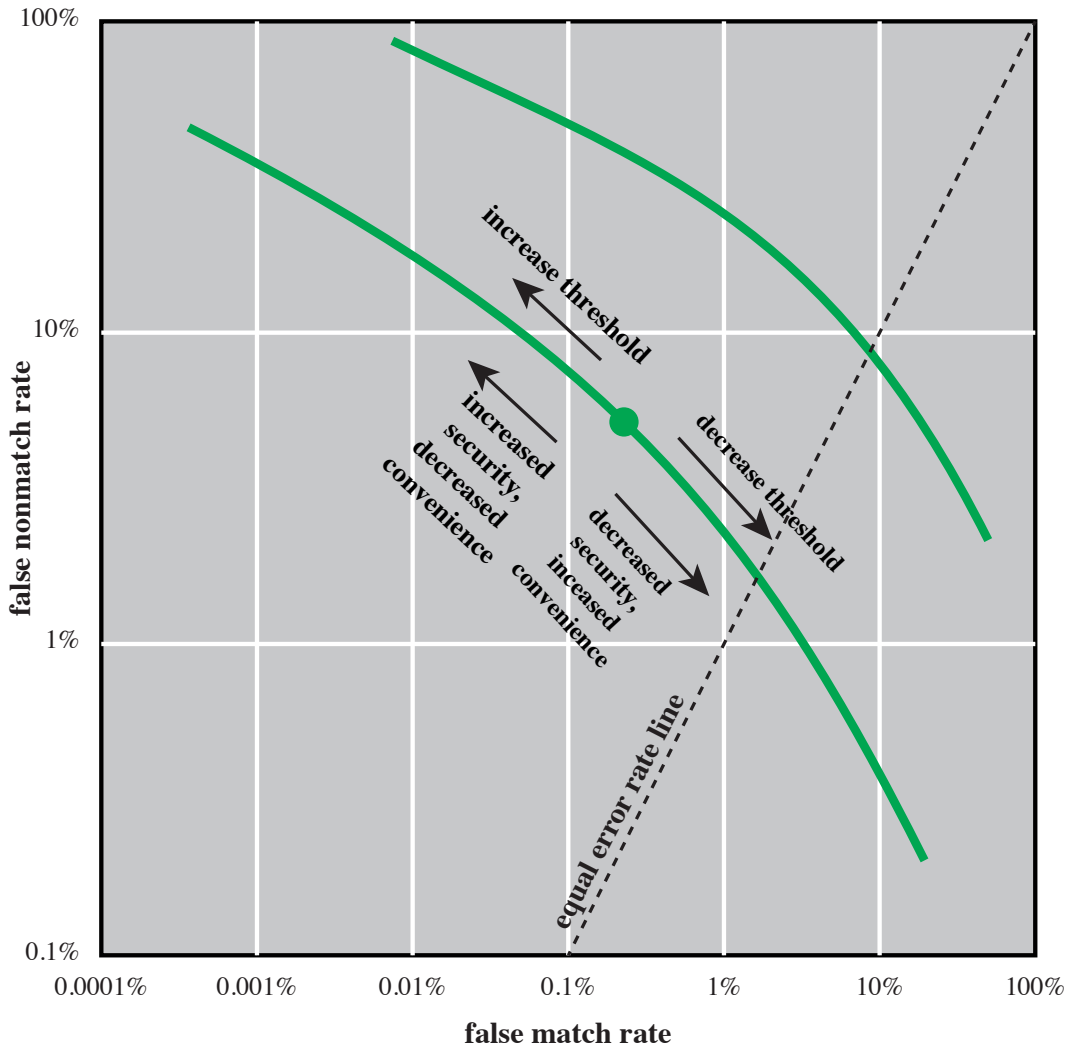



**Figure 3.11 Idealized Biometric Measurement Operating Characteristic Curves (log-log scale)**

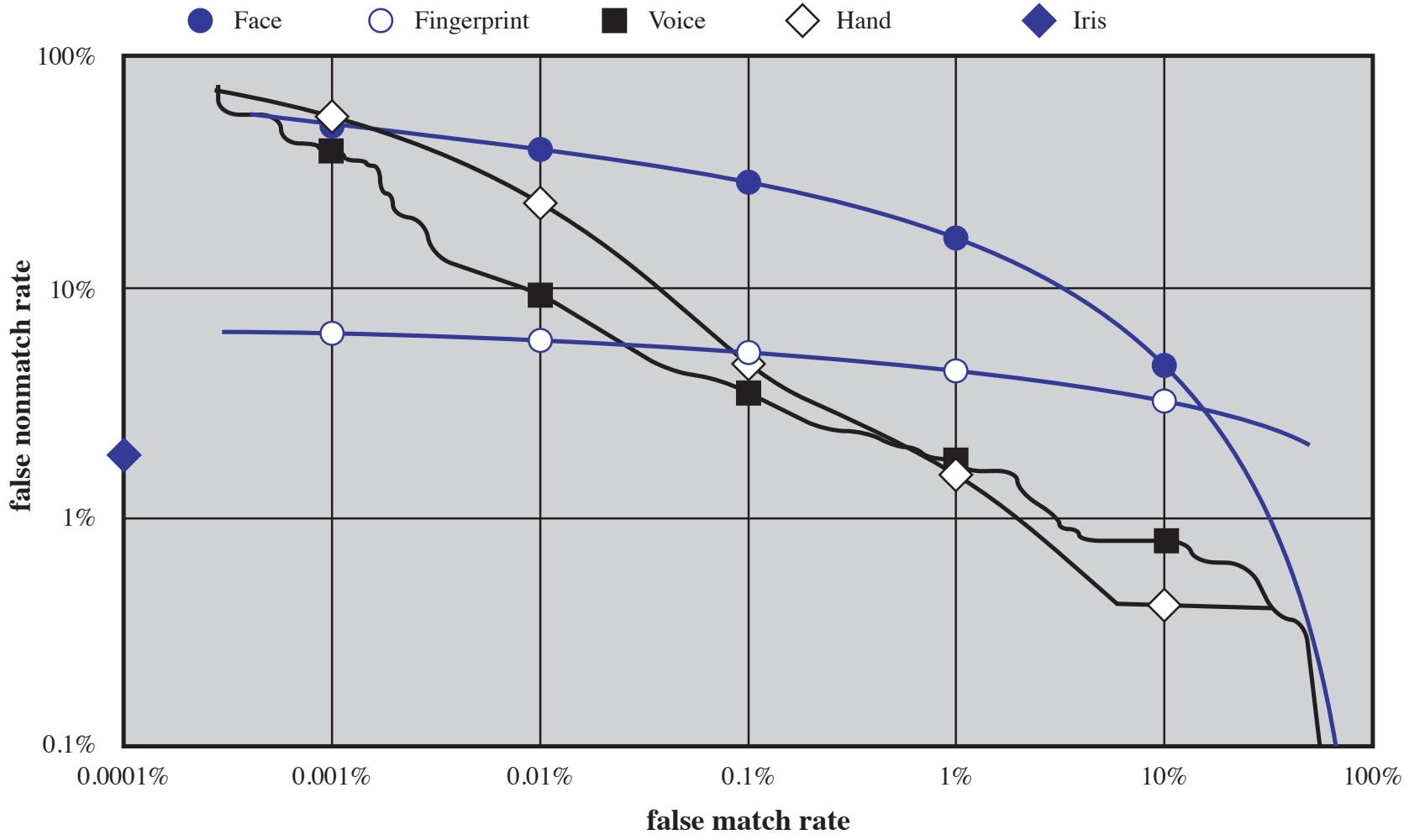



Figure 3.12 Actual Biometric Measurement Operating Characteristic Curves, reported in [MANS01]. To clarify differences among systems, a log-log scale is used.

| Attacks | Authenticators | Examples | Typical defenses |
|---|---|---|---|
| **Client attack** | Password | Guessing, exhaustive search | Large entropy; limited attempts |
| | Token | Exhaustive search | Large entropy; limited attempts, theft of object requires presence |
| | Biometric | False match | Large entropy; limited attempts |
| **Host attack** | Password | Plaintext theft, dictionary/exhaustive search | Hashing; large entropy; protection of password database |
| | Token | Passcode theft | Same as password; 1-time passcode |
| | Biometric | Template theft | Capture device authentication; challenge response |
| **Eavesdropping, theft, and copying** | Password | "Shoulder surfing" | User diligence to keep secret; administrator diligence to quickly revoke compromised passwords; multifactor authentication |
| | Token | Theft, counterfeiting hardware | Multifactor authentication; tamper resistant/evident token |
| | Biometric | Copying (spoofing) biometric | Copy detection at capture device and capture device authentication |
| | Password | Replay stolen password response | Challenge-response protocol |

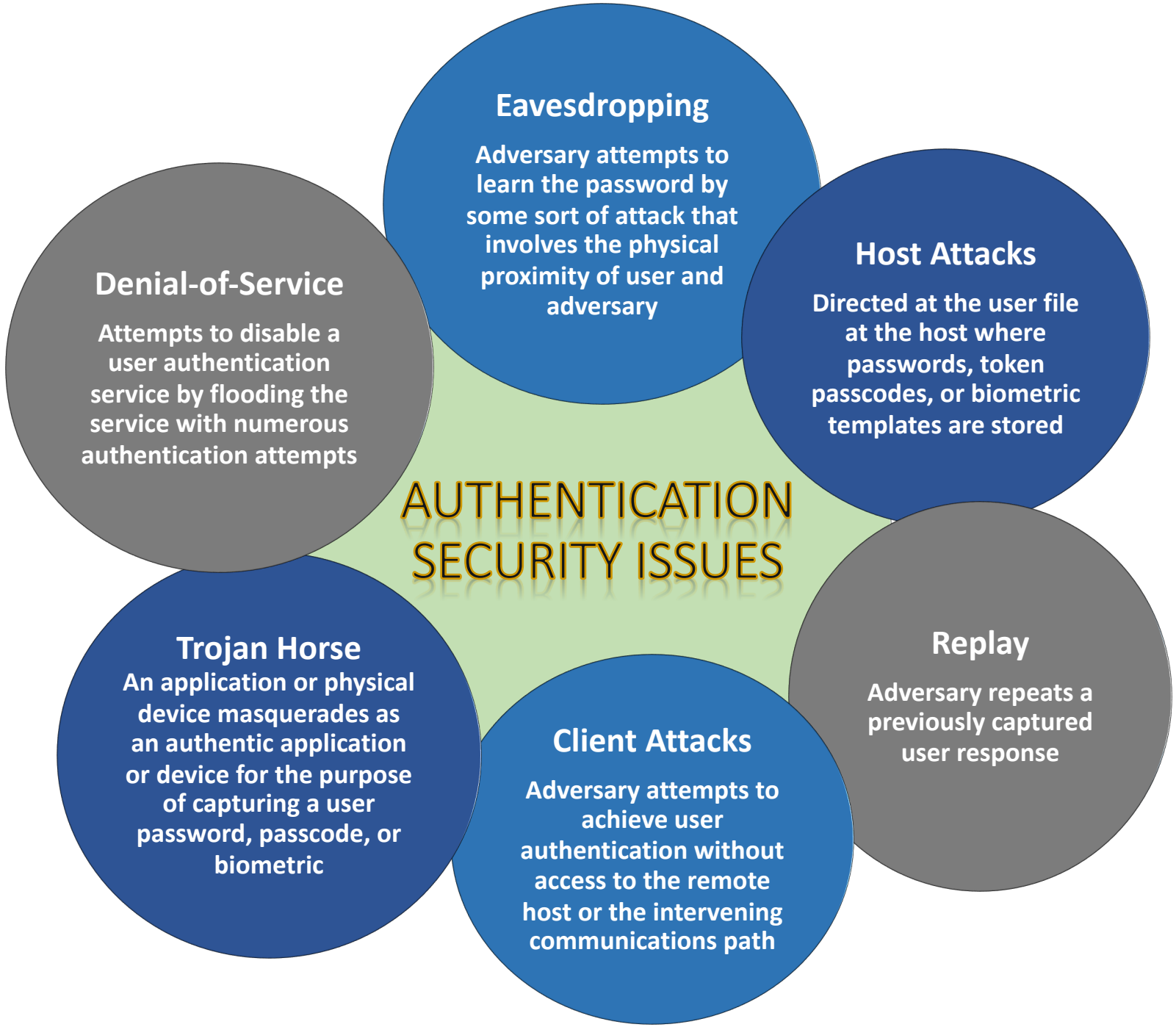
# Some Potential Attacks, Susceptible Authenticators, and Typical Defenses

(Table is on page 96 in the textbook)

| | | | |
|---|---|---|---|
| **Eavesdropping, theft, and copying** | Password | Shoulder surfing | User diligence to keep secret; administrator diligence to quickly revoke compromised passwords; multifactor authentication |
| | Token | Theft, counterfeiting hardware | Multifactor authentication; tamper resistant/evident token |
| | Biometric | Copying (spoofing) biometric | Copy detection at capture device and capture device authentication |
| **Replay** | Password | Replay stolen password response | Challenge-response protocol |
| | Token | Replay stolen passcode response | Challenge-response protocol; 1-time passcode |
| | Biometric | Replay stolen biometric template response | Copy detection at capture device and capture device authentication via challenge-response protocol |
| **Trojan horse** | Password, token, biometric | Installation of rogue client or capture device | Authentication of client or capture device within trusted security perimeter |
| **Denial of service** | Password, token, biometric | Lockout by multiple failed authentications | Multifactor with token |

# Some Potential Attacks, Susceptible Authenticators, and Typical Defenses

(Table is on page 96 in the textbook)


AUTHENTICATION SECURITY ISSUES
Eavesdropping
Adversary attempts to learn the password by some sort of attack that involves the physical proximity of user and adversary
Host Attacks
Directed at the user file at the host where passwords, token passcodes, or biometric templates are stored
Denial-of-Service
Attempts to disable a user authentication service by flooding the service with numerous authentication attempts
Replay
Adversary repeats a previously captured user response
Trojan Horse
An application or physical device masquerades as an authentic application or device for the purpose of capturing a user password, passcode, or biometric
Client Attacks
Adversary attempts to achieve user authentication without access to the remote host or the intervening communications path

# Summary

- Digital user authentication principles
  - A model for digital user authentication
  - Means of authentication
  - Risk assessment for user authentication
- Password-based authentication
  - The vulnerability of passwords
  - The use of hashed passwords
  - Password cracking of user-chosen passwords
  - Password file access control
  - Password selection strategies
- Token-based authentication
  - Memory cards
  - Smart cards
  - Electronic identity cards
- Biometric authentication
  - Physical characteristics used in biometric applications
  - Operation of a biometric authentication system
  - Biometric accuracy
- Security issues for user authentication