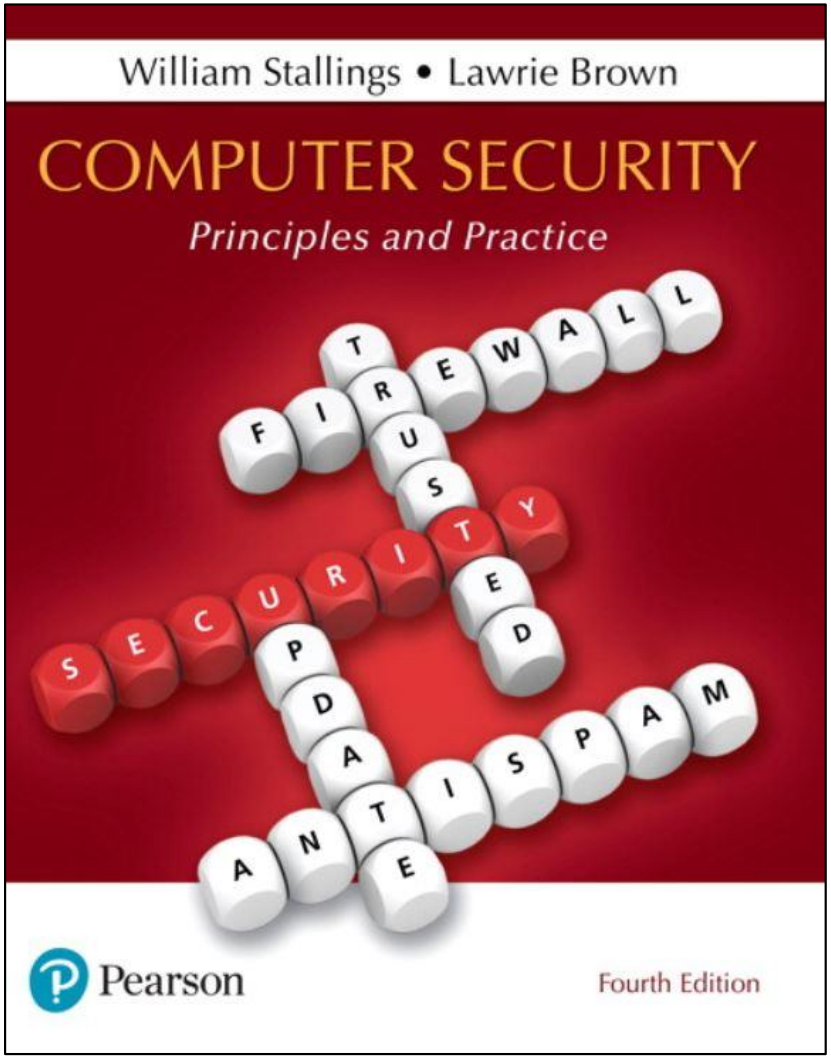
Computer Security: Principles and Practice

Fourth Edition



Chapter 3

User Authentication

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."

Table 3.1 Identification and Authentication Security Requirements (NIST SP 800-171) (1 of 2)

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.

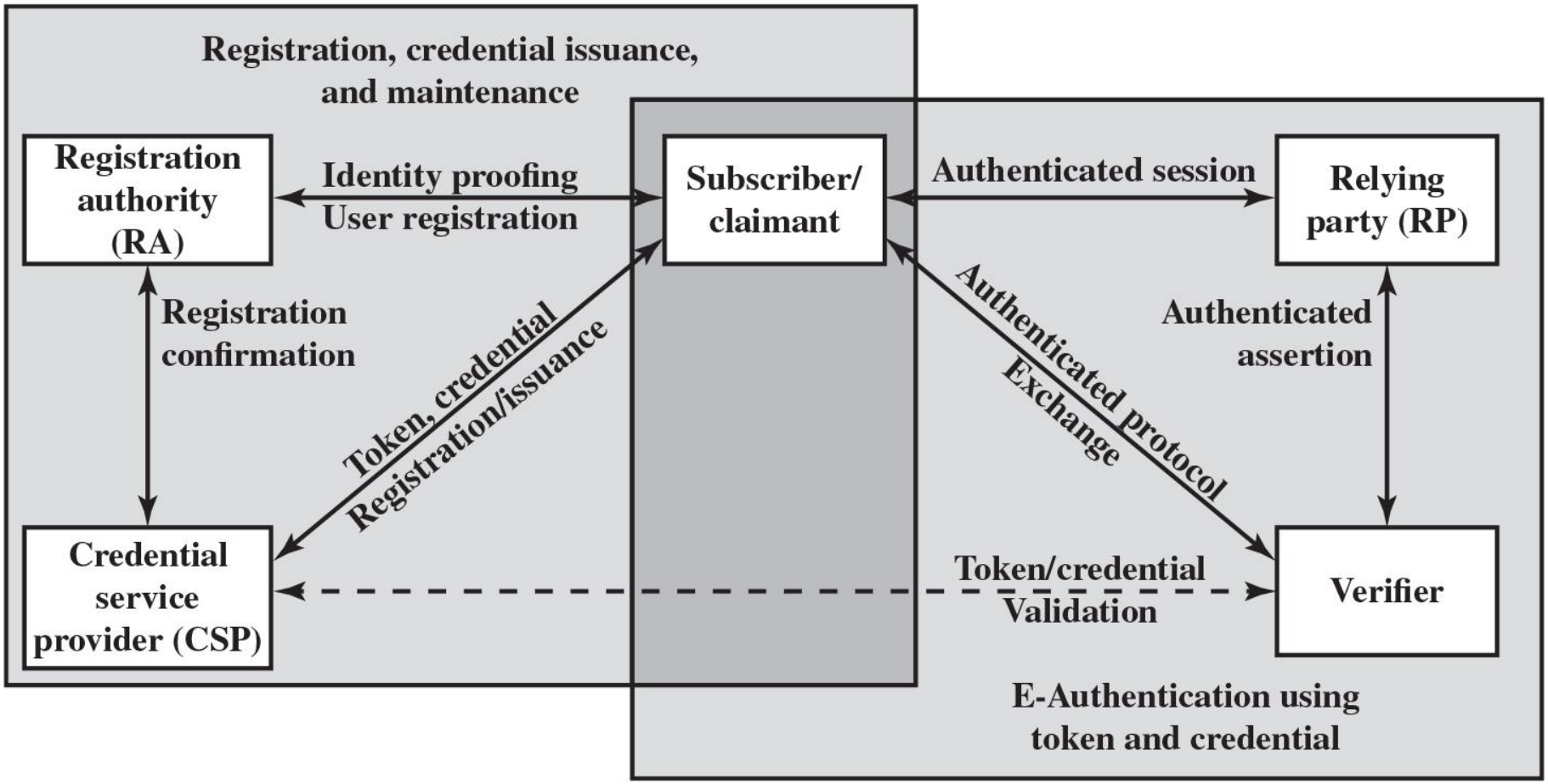
Derived Security Requirements:

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.

Table 3.1 Identification and Authentication Security Requirements (NIST SP 800-171) (2 of 2)

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.

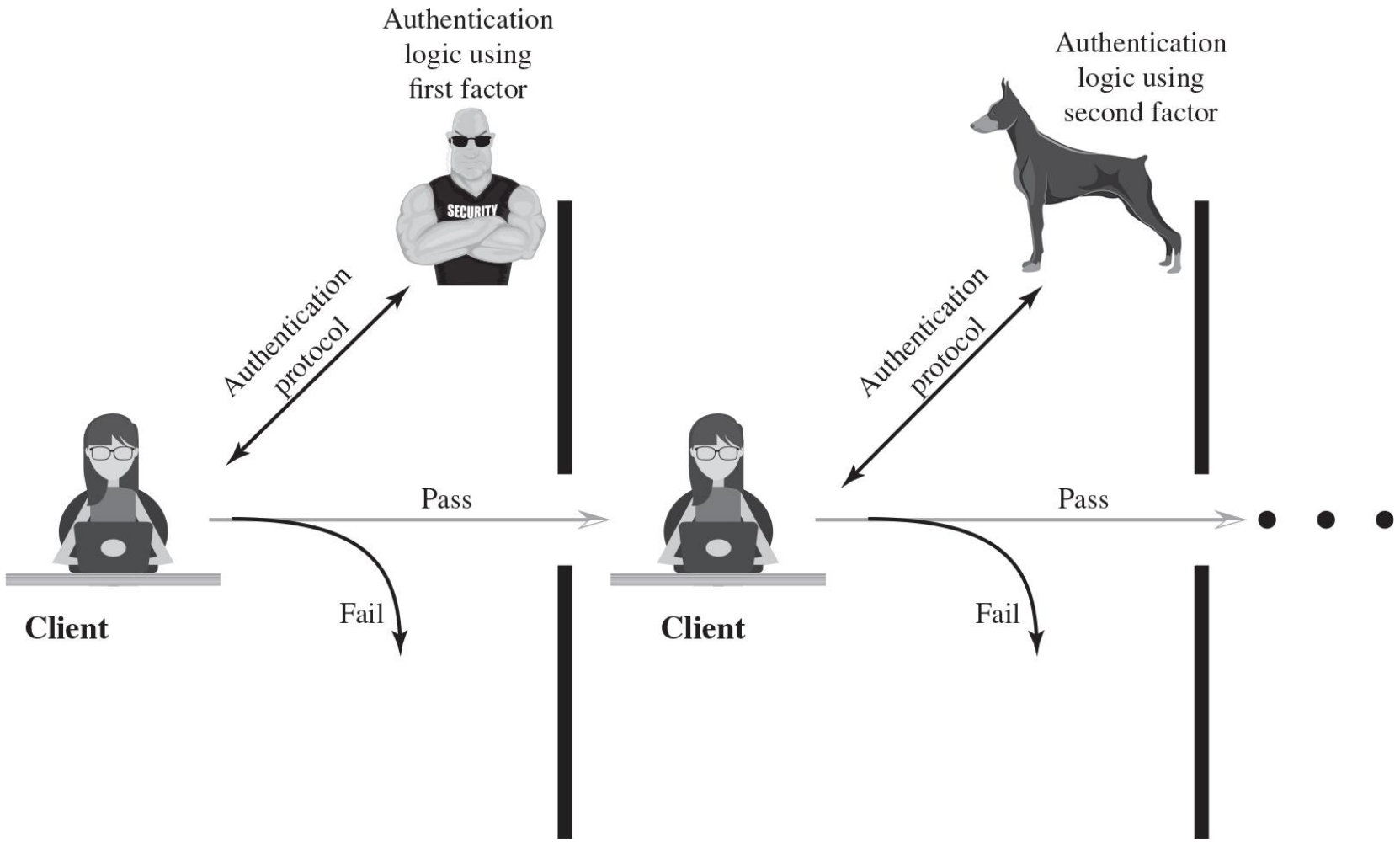
Figure 3.1 The NIST SP 800-63-3 E-Authentication Architectural Model



The Four Means of Authenticating User Identity Are Based On:

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

Figure 3.2 Multifactor Authentication



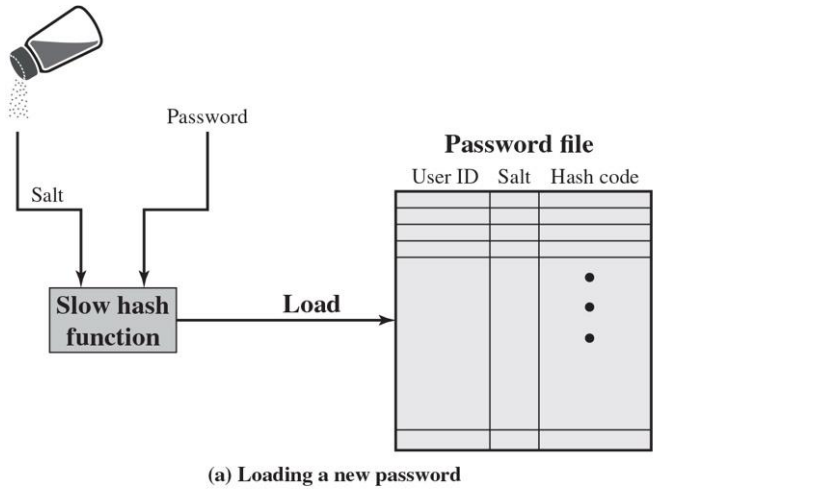
Password-Based Authentication

- 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

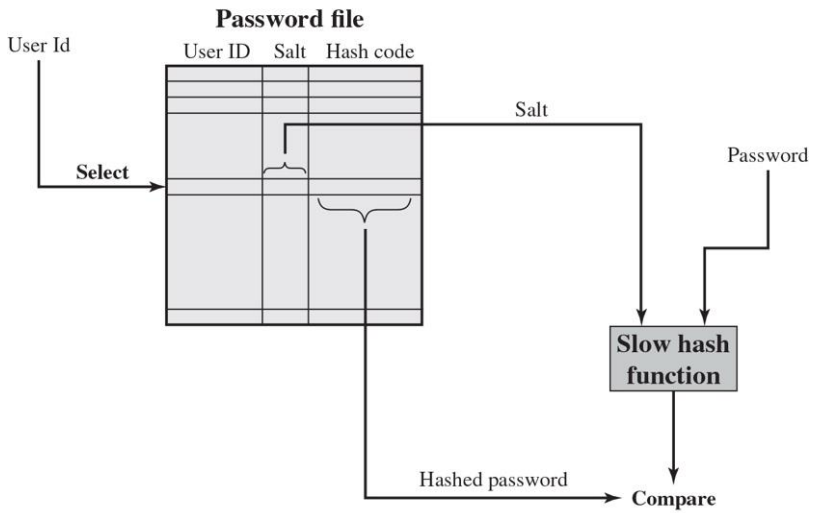
Password Vulnerabilities

- 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

Figure 3.3 UNIX Password Scheme



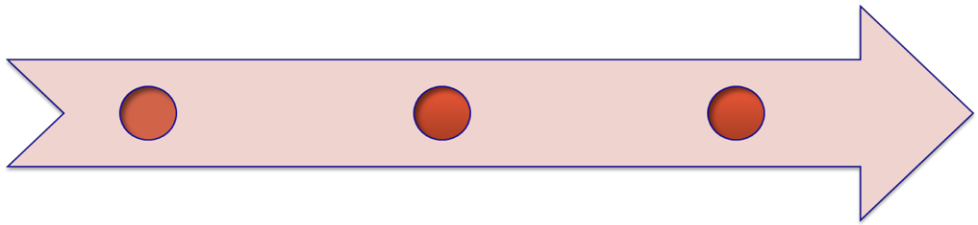
(a) Loading a new password



(b) Verifying a password

Improved Implementations

- Much stronger hash/salt schemes available for Unix
- 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
- 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



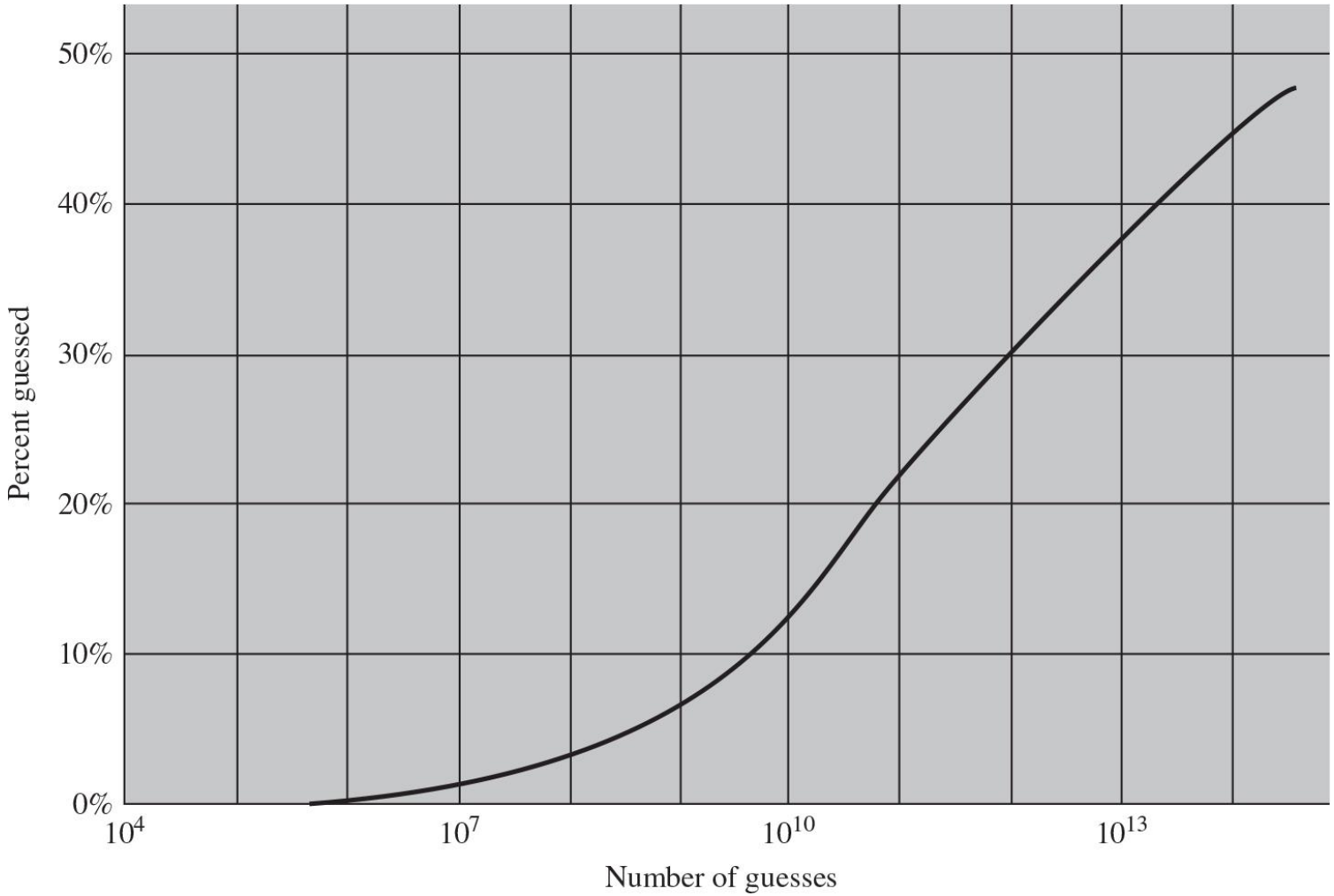
Password Cracking

- 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
- 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
  - Studying examples and structures of actual passwords in use

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
  - Check desired password against this table

Table 3.3 Types of Cards Used as Tokens

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 Contact Contactless	Electronic memory and processor inside Electrical contacts exposed on surface Radio antenna embedded inside	Biometric ID card

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 (1 of 2)

- 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

Smart Cards (2 of 2)

- 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

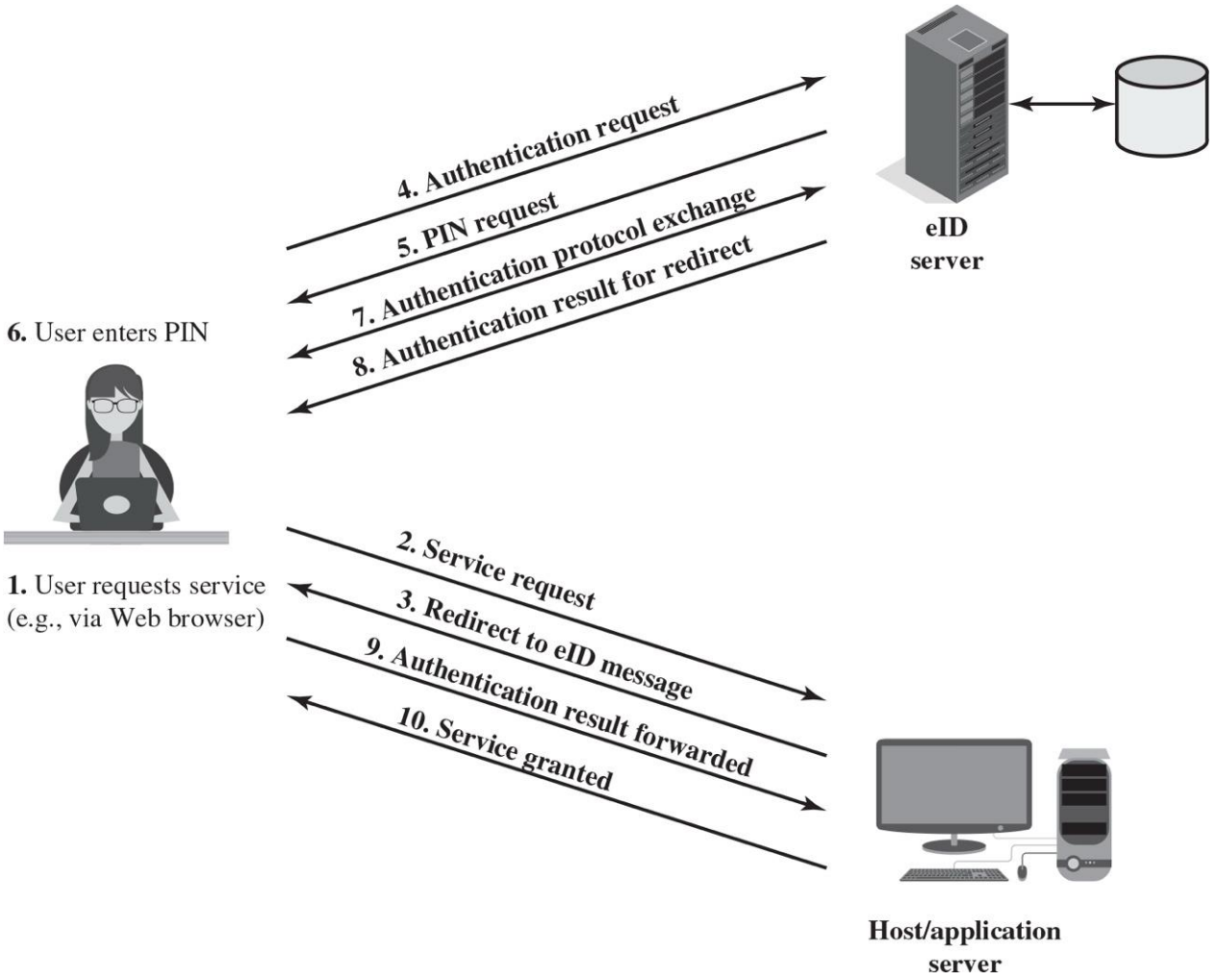
Electronic Identity Cards (eID) (1 of 2)

- 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

Electronic Identity Cards (eID) (2 of 2)

- 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)

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

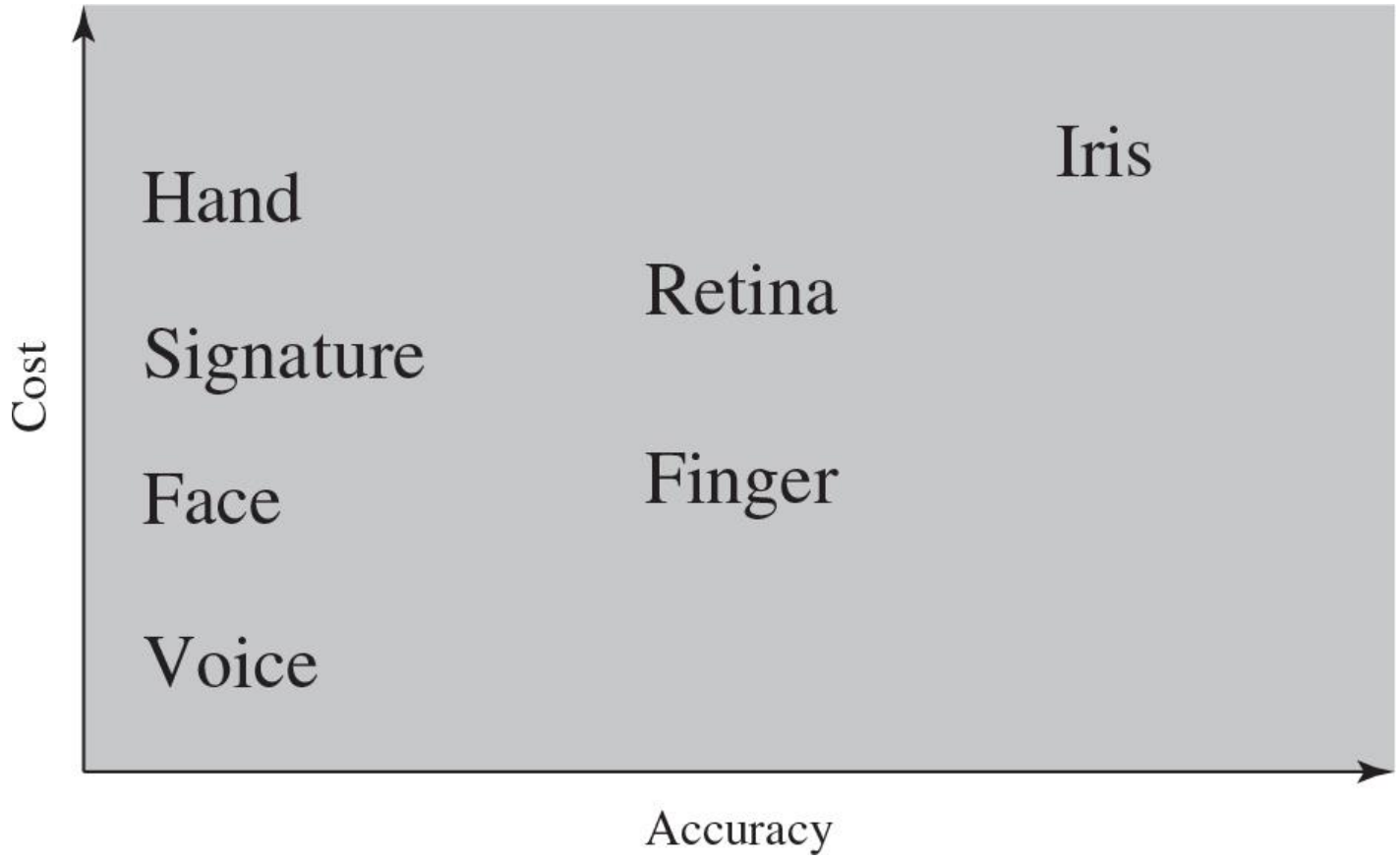
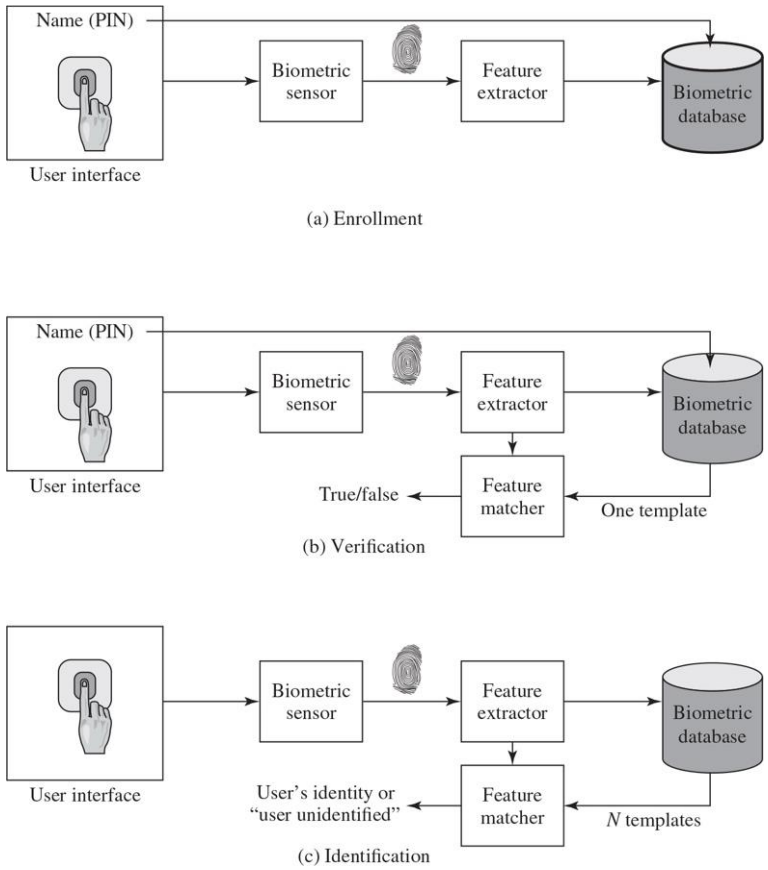


Figure 3.9 A Generic Biometric System

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.



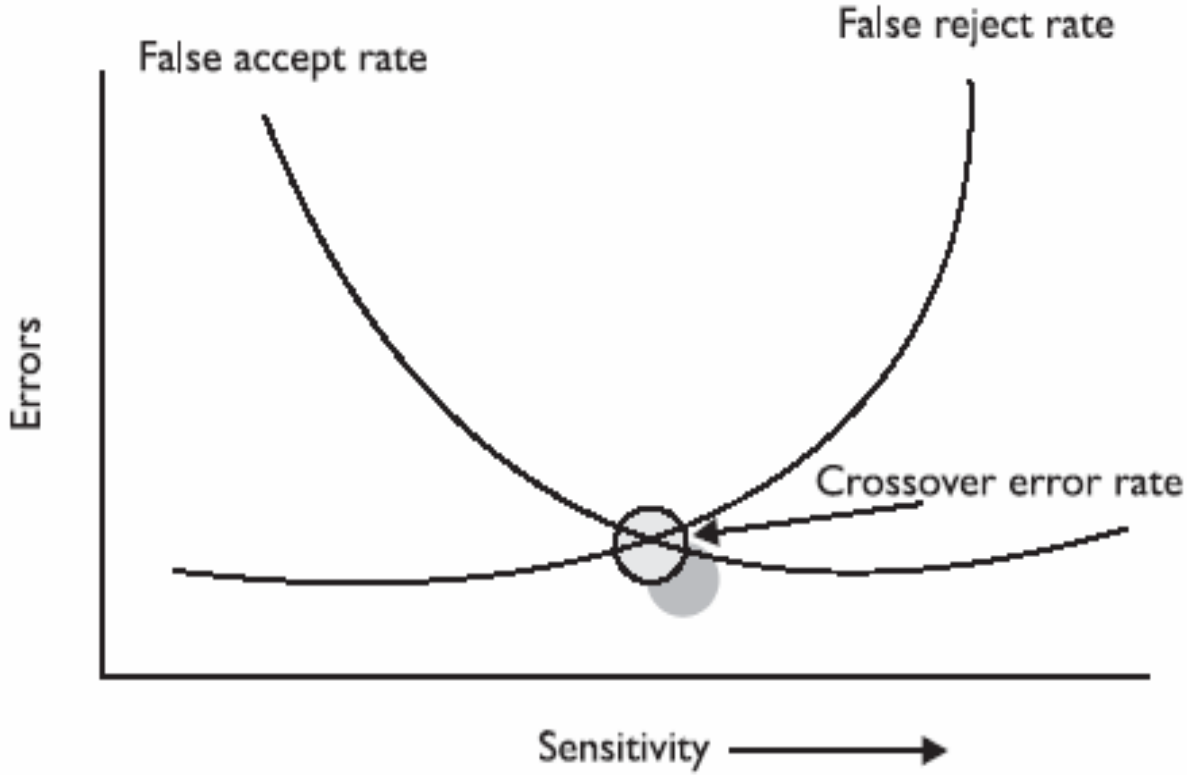
Biometric System Errors

- Type I Error (False Rejection Rate): When a biometric system rejects an authorized individual
- Type II Error (False Acceptance Rate): When the system accepts impostors who should be rejected
- Type II errors are the most dangerous and thus the most important to avoid

- The **goal** is to obtain low numbers for each type of error

- Crossover Error Rate (CER): a Percentage and represents the point at which the false rejection rate equals the false acceptance rate

Biometric System Errors



CER represents when Type I errors equal Type II errors.

NOTE Crossover error rate (CER) is also called equal error rate (EER).

CER is used to compare biometric products from different vendors

Remote User Authentication

- Authentication over a network, the Internet, or a communications link is more complex
- Additional security threats such as:
  - Eavesdropping, capturing a password, replaying an authentication sequence that has been observed
- Generally rely on some form of a challenge-response protocol to counter threats

Figure 3.13 Basic Challenge-Response Protocols for Remote User Authentication

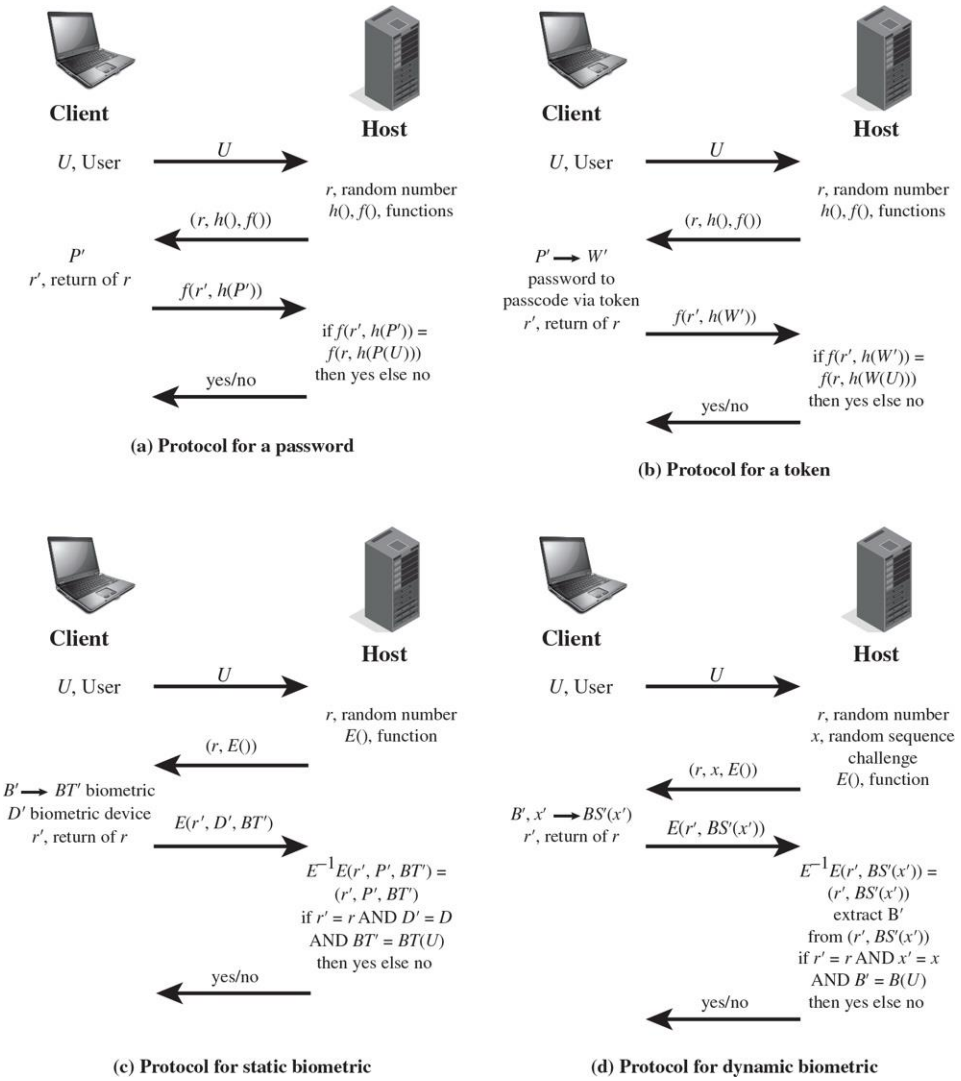


Table 3.5 Some Potential Attacks, Susceptible Authenticators, and Typical Defenses (1 of 2)

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
Eavesdroppin, 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

Table 3.5 Some Potential Attacks, Susceptible Authenticators, and Typical Defenses (2 of 2)

Attacks	Authenticators	Examples	Typical Defenses
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

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
- Replay: Adversary repeats a previously captured user response
- Client Attacks: Adversary attempts to achieve user authentication without access to the remote host or the intervening communications path
- 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
- Denial-of-Service: Attempts to disable a user authentication service by flooding the service with numerous authentication attempts

Summary (1 of 2)

- 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

Summary (2 of 2)

- Biometric authentication
  - Physical characteristics used in biometric applications
  - Operation of a biometric authentication system
  - Biometric accuracy
- Remote user authentication
  - Password protocol
  - Token protocol
  - Static biometric protocol
  - Dynamic biometric protocol
- Security issues for user authentication

Copyright