Computer Security: Principles and Practice

Fourth Edition

By: William Stallings and Lawrie Brown

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 (SP 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.

(Table can be found on page 65 in the textbook)

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

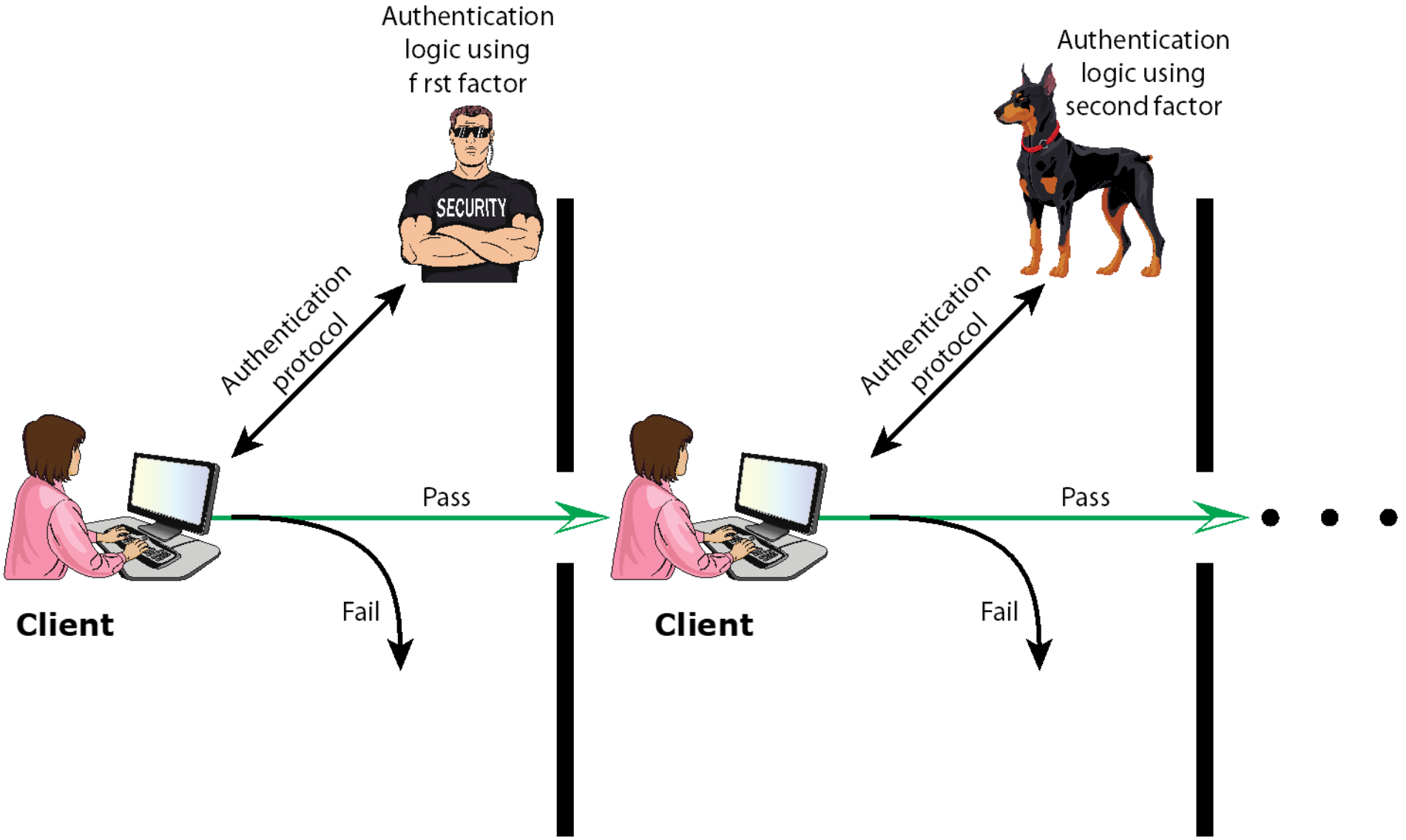
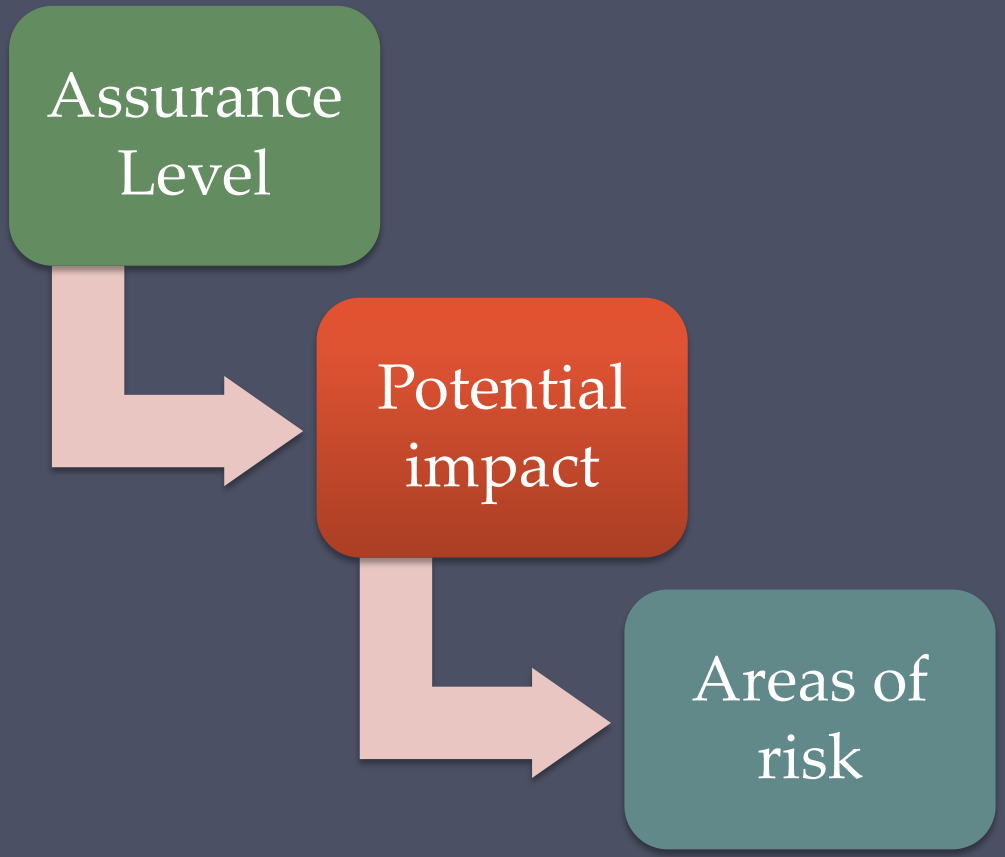


Figure 3.2 Multifactor Authentication

Risk Assessment for User Authentication

- There are three separate concepts:



Assurance Level

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

More specifically, it 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 originally

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

SP 800-63-3: Four levels of assurance

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

Assurance Level Examples

SP 800-63-3: Four levels of assurance

Level 1: Little or no confidence

- Consumer registering to participate in a discussion at a company web site discussion board
- Company-issued username and password

Level 2: Some confidence

- Appropriate for a wide range of business where auth. details are verified independently beforehand
- Some sort of secure authentication is used

Level 3: High confidence

- Enable clients or employees to access restricted services of high value but not the highest value
- A patent attorney electronically submits confidential patent information to Patent/Trademark Office

Level 4: Very high confidence

- Enable employees to access restricted services of very high value
- A law enforcement official accesses a law enforcement database containing criminal records.
- Requires the use of multiple factors as well as in-person registration

Potential Impact

- FIPS 199 defines three levels of potential impact on organizations or individuals should there be a breach of security:
  - 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

Table 3.2 Maximum Potential Impacts for Each Assurance Level

Risk Areas:

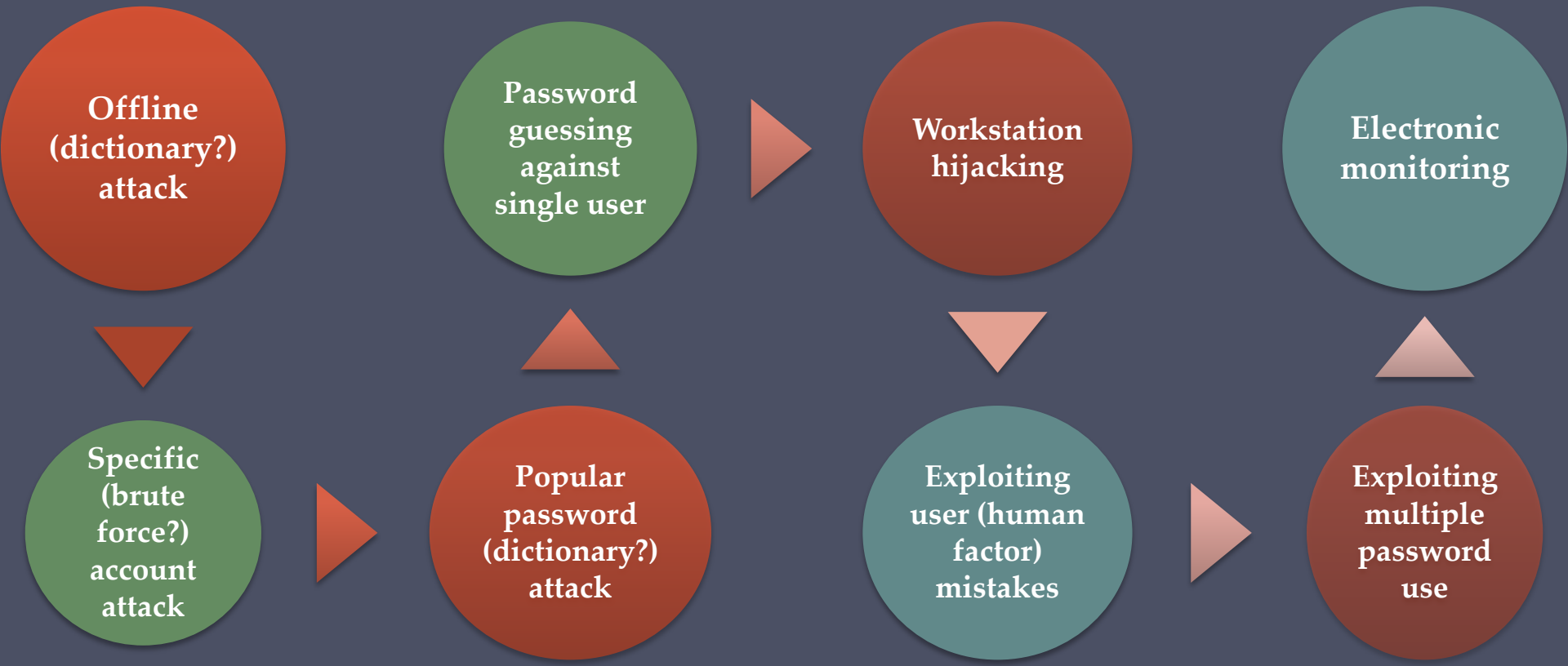
Potential Impact Categories for Authentication Errors	Assurance Level Impact Profiles			
	1	2	3	4
Inconvenience, distress, damage to standing or reputation	Low	Mod	Mod	High
Financial loss or organization liability	None	Low	Mod	High
Harm to organization programs or interests	None	Low	Mod	High
Unauthorized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

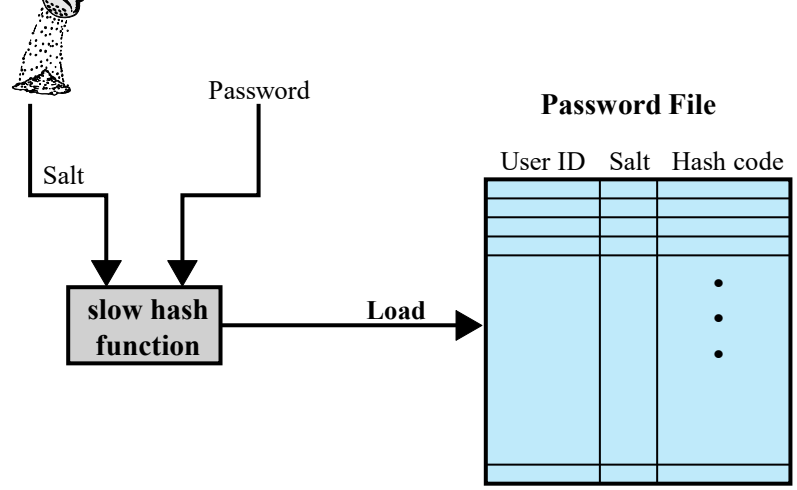
For example, consider the potential for financial loss if there is an authentication error that results in unauthorized access to a database

Password-Based Authentication

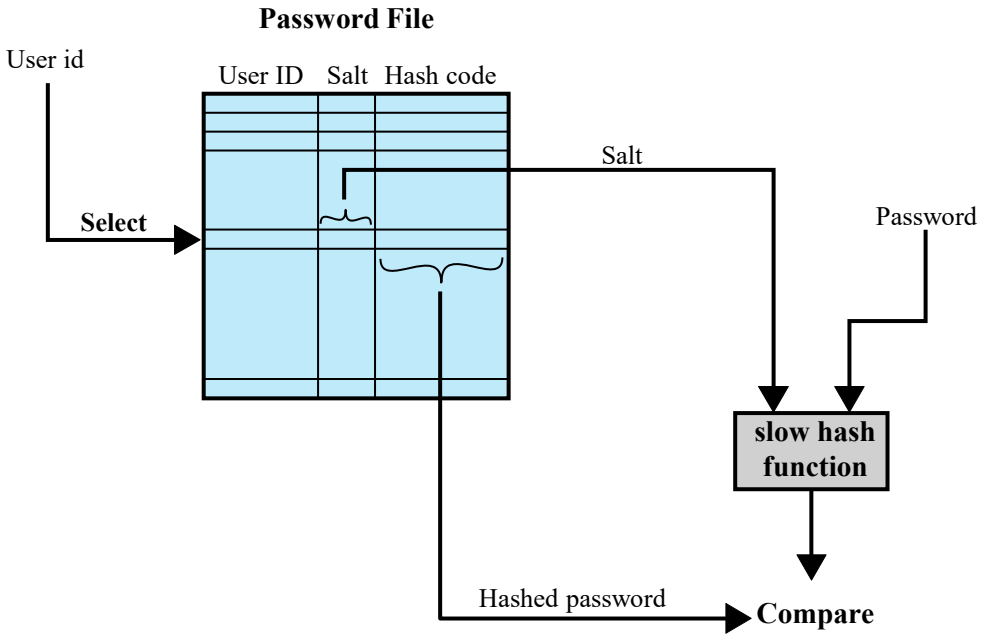
- Widely-used line of defense against intruders
  - User provides name/login and password
  - System compares password with the one stored for that specified login
- The user ID (name/login):
  - Determines that the user is registered to access the system
  - Determines the user's privileges
  - Is used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

Password Vulnerabilities and attack strategies





(a) Loading a new password



(b) Verifying a password

Figure 3.3 UNIX Password Scheme (see
https://www.youtube.com/watch?v=--tnZMuoK3E

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 by brute force

John the Ripper

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

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

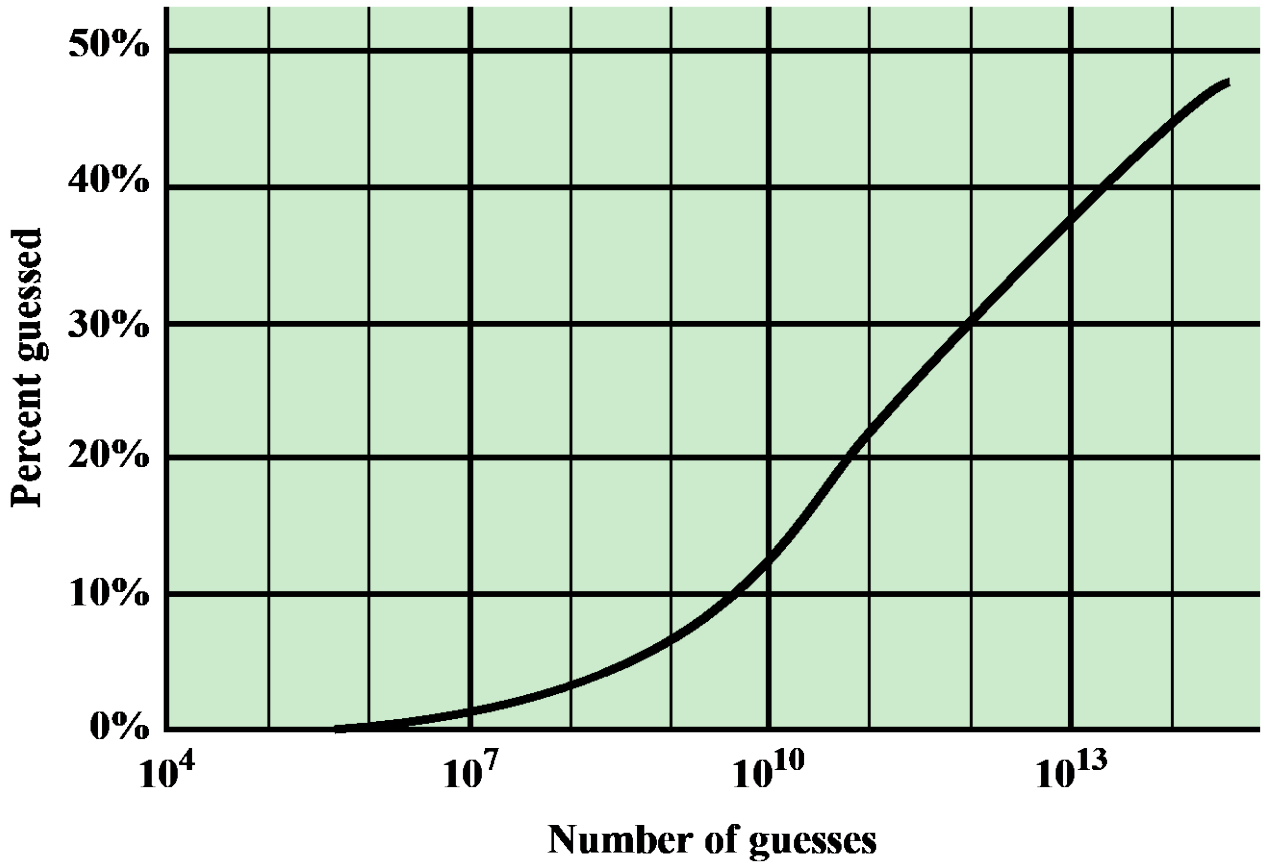


Figure 3.4 The Percentage of Passwords Guessed After a Given Number of Guesses

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
- Dictionary 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
  - Almost like a mini rainbow table principle

Table 3.3

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

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 (SmartCard)
- 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

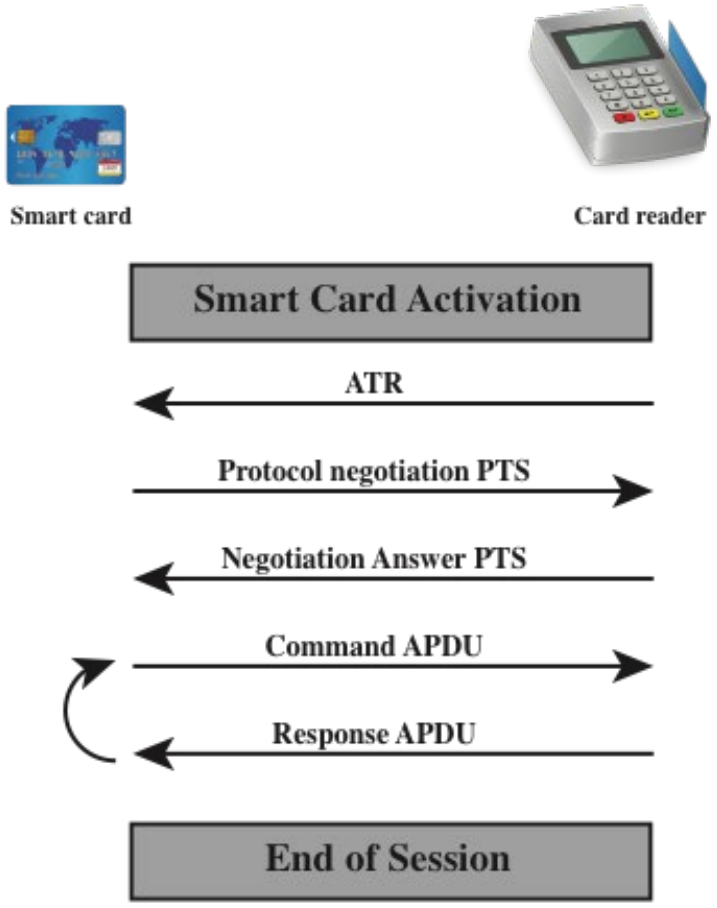
Smart Tokens

- 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

Verified by national governments as valid and authentic means

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)

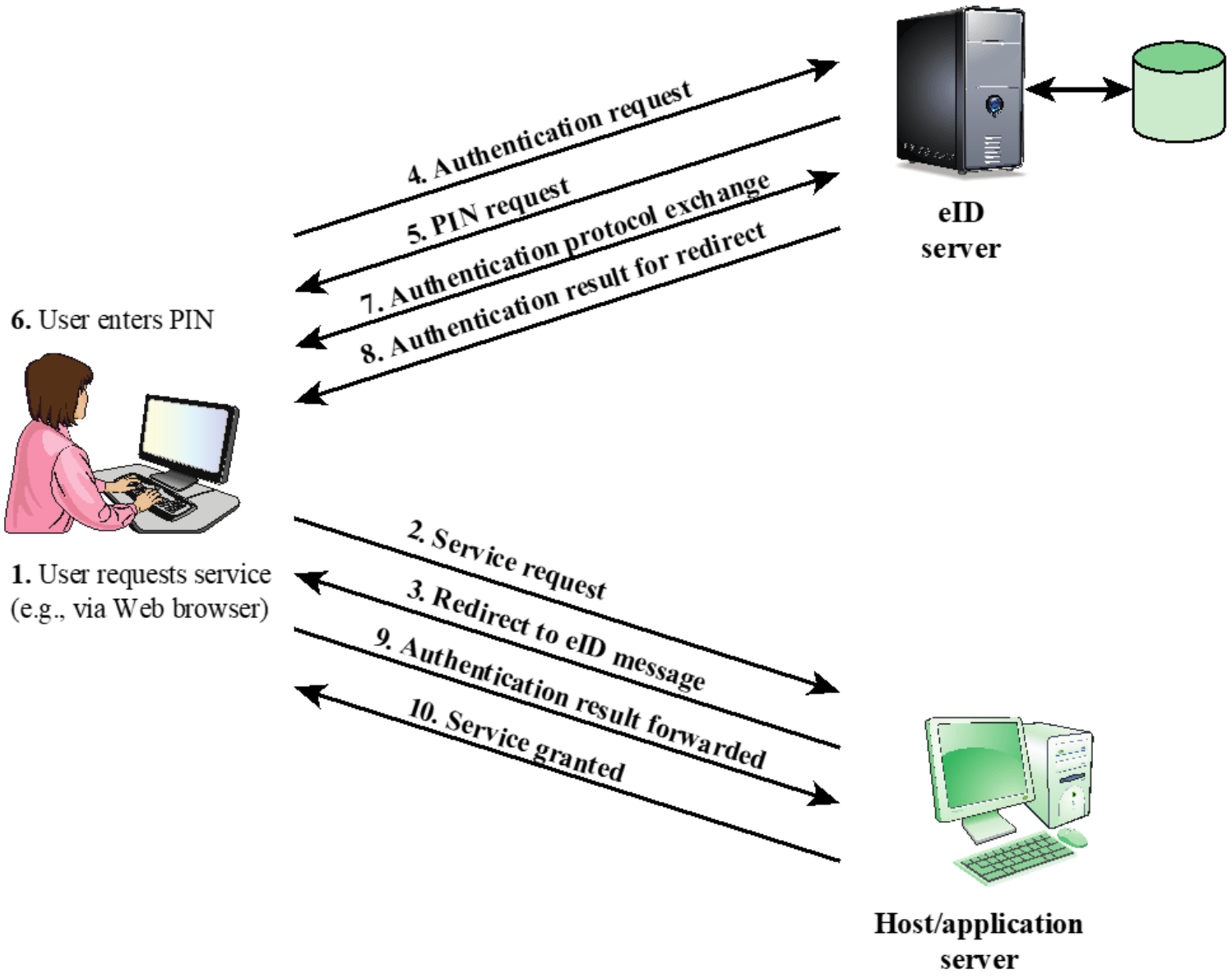


Figure 3.7 User Authentication with eID

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

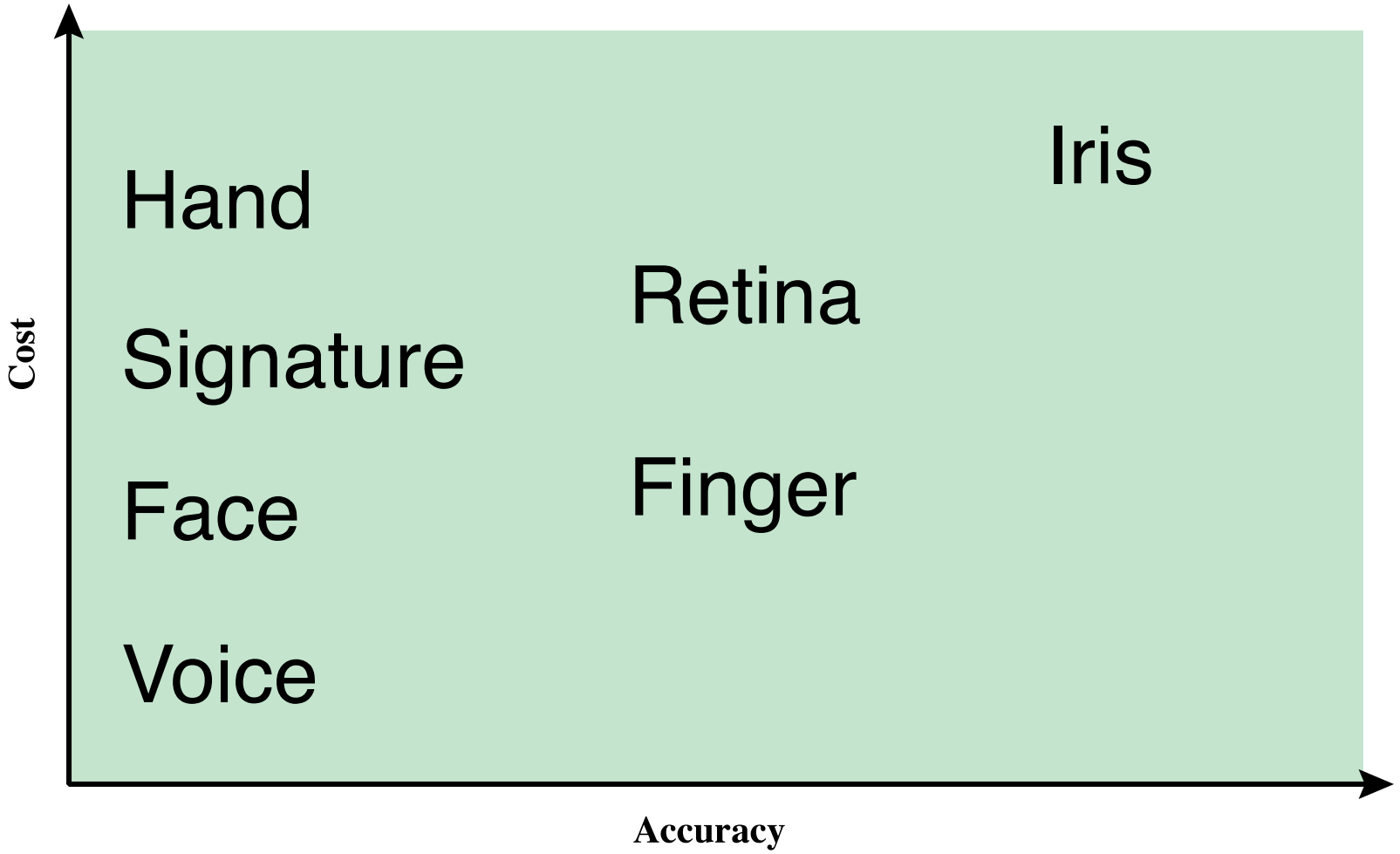
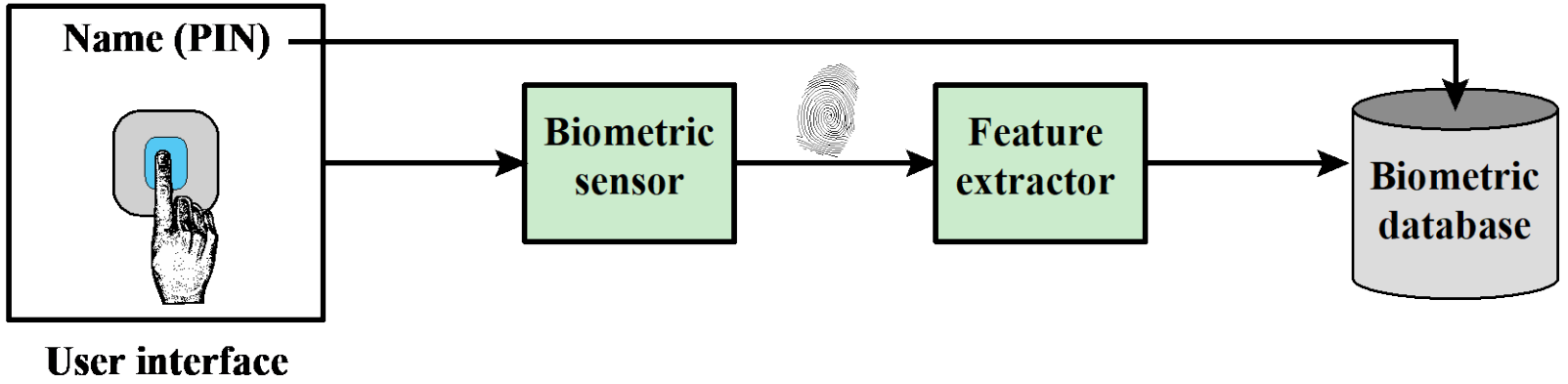
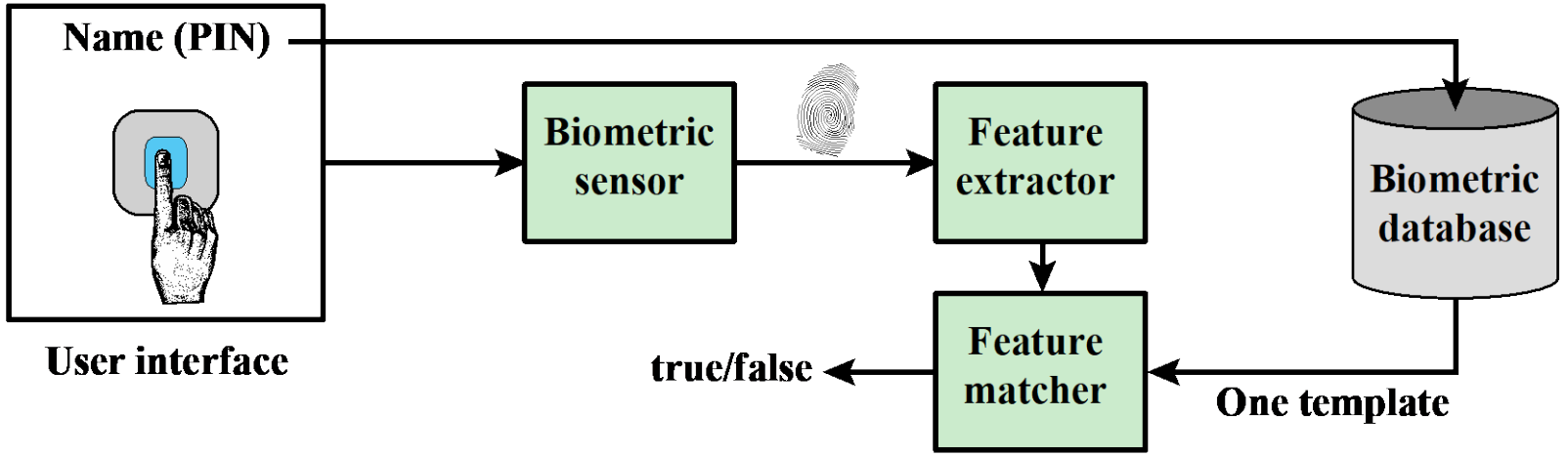


Figure 3.8 Cost Versus Accuracy of Various Biometric Characteristics in User Authentication Schemes.



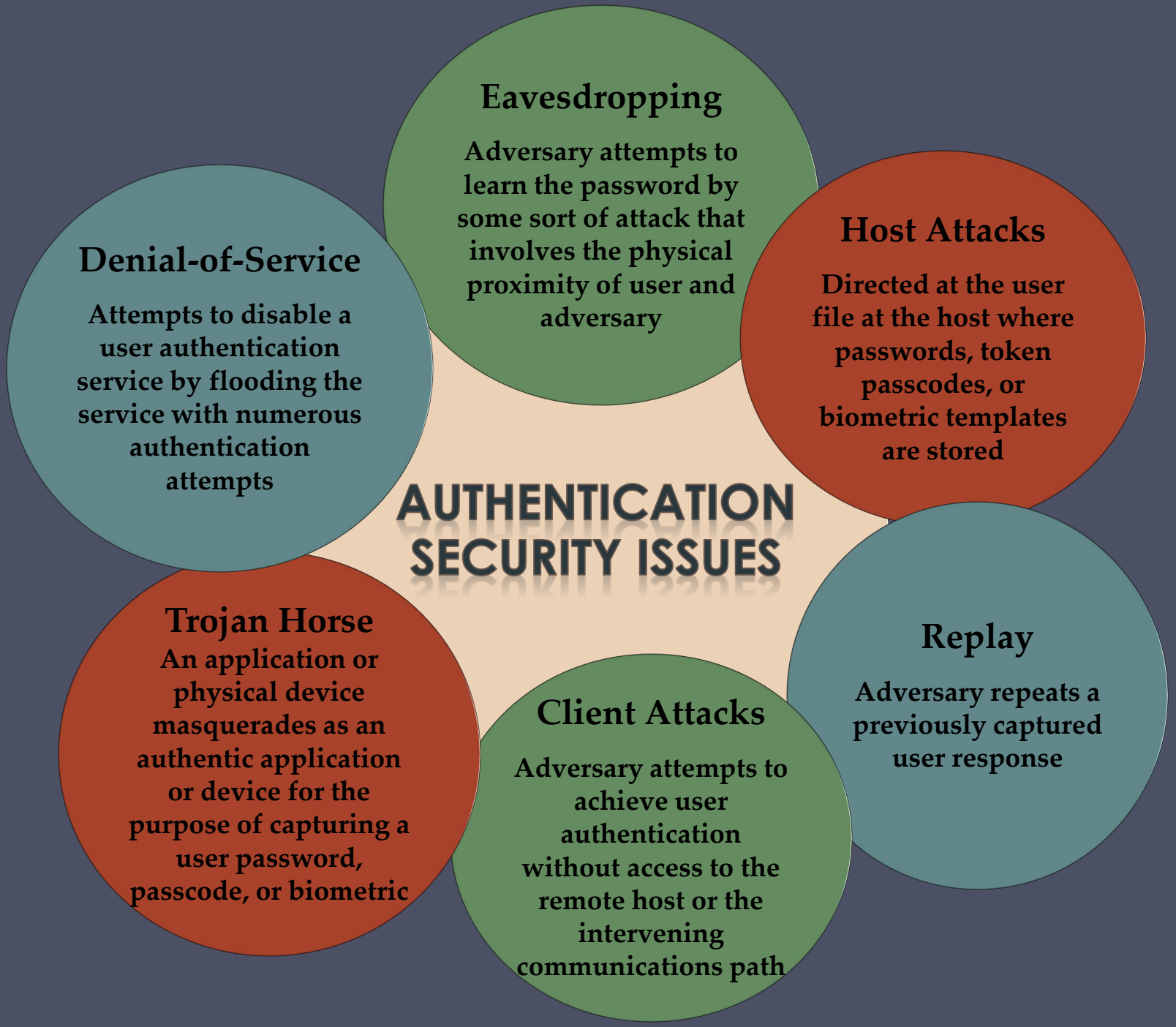
(a) Enrollment



(b) Verification

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


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

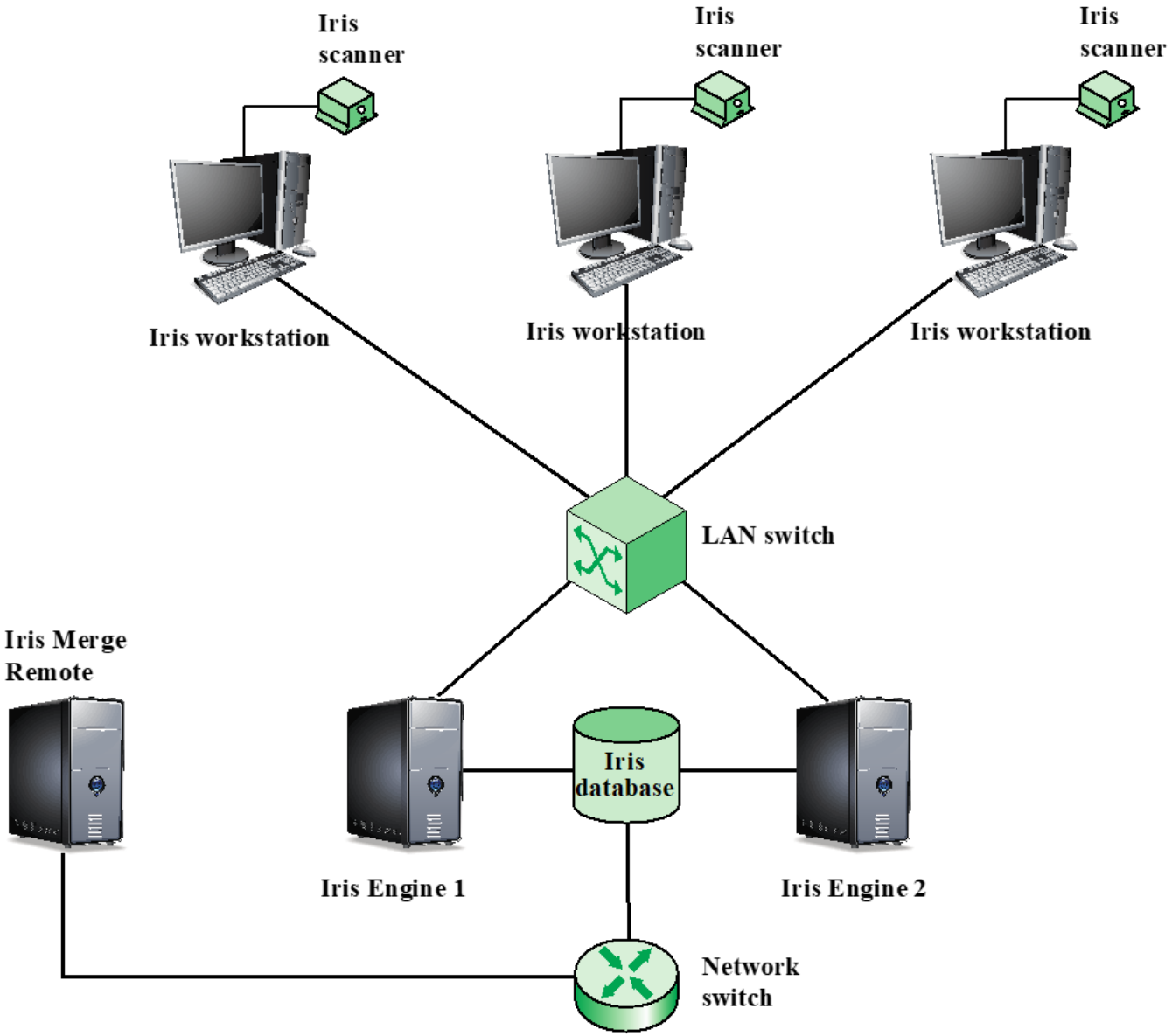


Figure 3.14 General Iris Scan Site Architecture for UAE System

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
- Remote user authentication
  - Password protocol
  - Token protocol
  - Static biometric protocol
  - Dynamic biometric protocol
- Security issues for user authentication

Practical 2

- Choose any identification & authentication scheme or implementation NOT mentioned in this Chapter 3
- Write up a 1-page document and submit in PDF using the following template: (Total: 10 marks)
- Your name, surname and student number
- Name of the scheme/implementation
- What is used for identification? (1)
- What is used for authorization? (1)
- Brief description of the scheme, how it works, and perhaps showing a picture/diagram etc. (4)
- How can it be attacked? (2)
- What countermeasure(s) could be put in place? (2)
- Please provide at least one reference (-1 if no ref.)

Practical 2

- Deadline for submission: Tuesday 20 August 2024, 09:00 sharp
- No late submissions will be accepted! Claiming that the connection was slow or you got disconnected or whatever other reason will not be accepted – upload well in time!
- No email submissions will be accepted.
- Only two upload opportunities are allowed. No resubmissions after that is allowed.
- Work alone! We will detect plagiarism/academic dishonesty with software.
- You will be penalized if you submit more than 1 page.
- If you use a scheme already mentioned in Chapter 3, you will not score any marks. Read through CH3!