User Authentication & Access Control

From Chapter 3 & 4

Dr Naveed Khan

n.khan@ulster.ac.uk

COM398

Introduction

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."

Authenticating user identity

The four means of authenticating user identity are based on:

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

Authenticating user identity

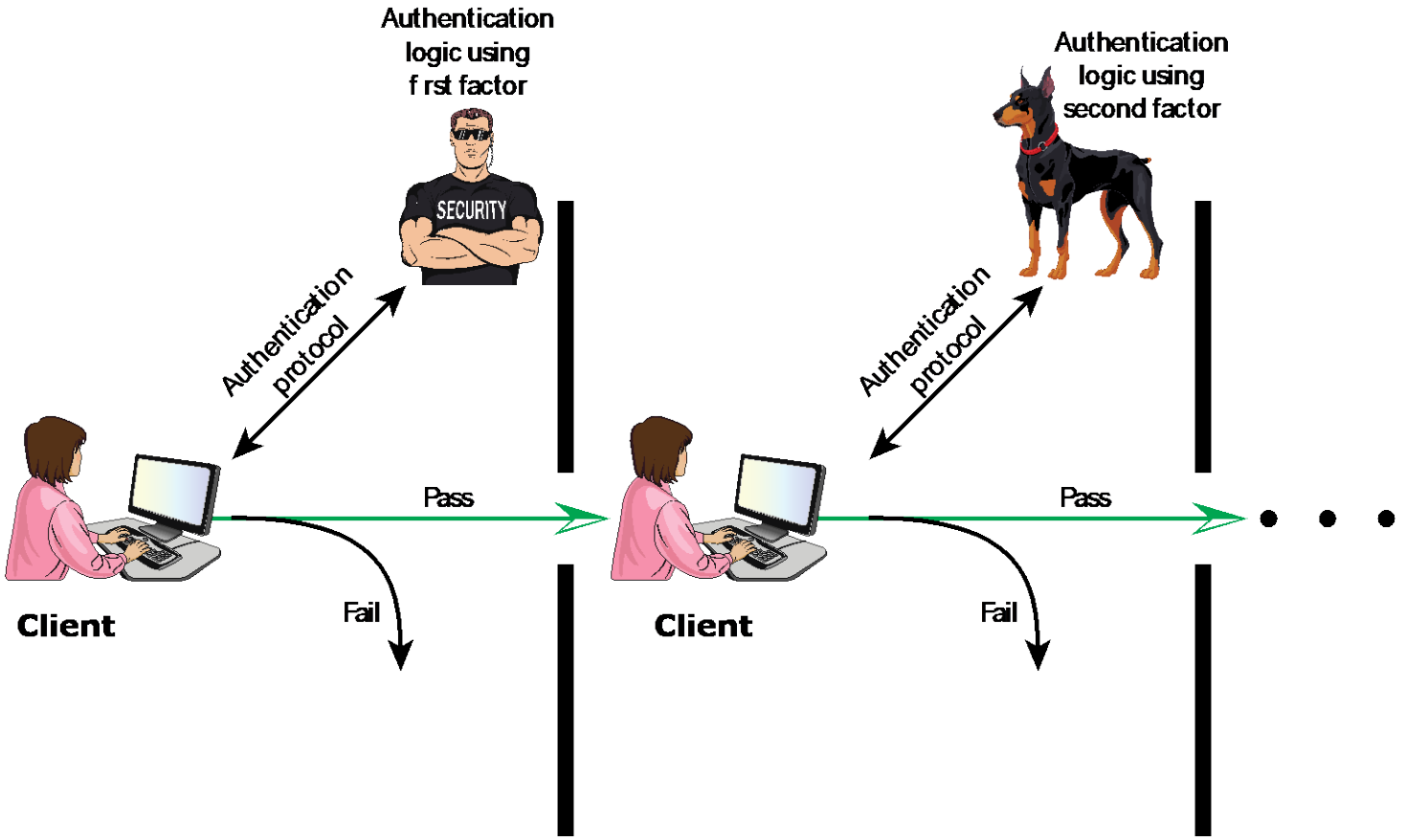


Figure 3.2 Multifactor Authentication

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-Based Authentication

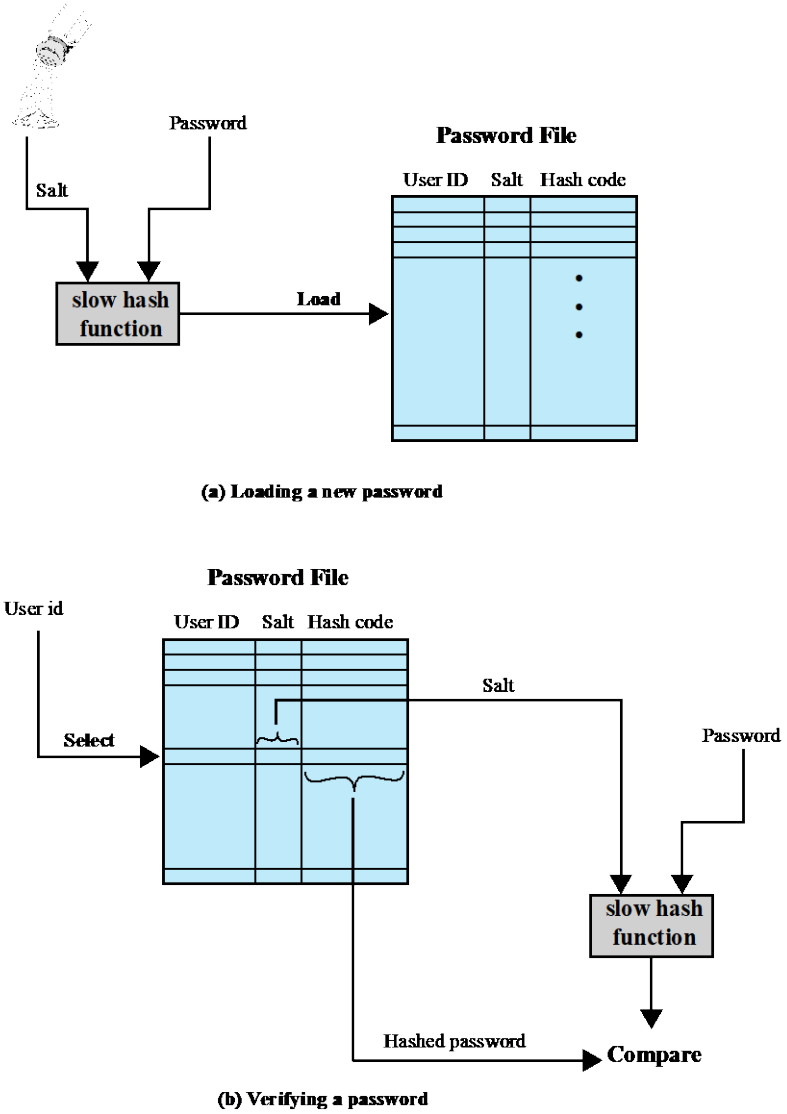
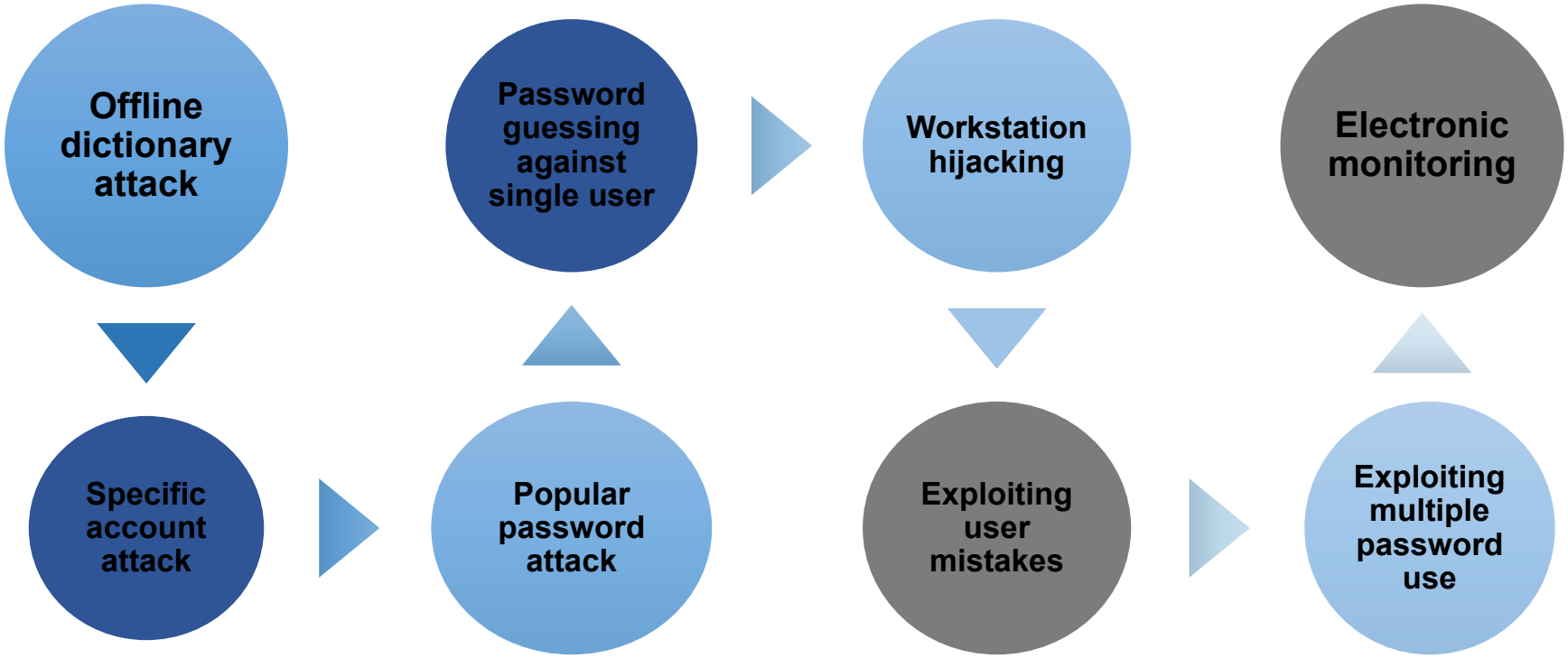


Figure 3.3 UNIX Password Scheme

Password Vulnerabilities



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

Guessing / Password crackers exploit the fact that people choose easily guessable passwords

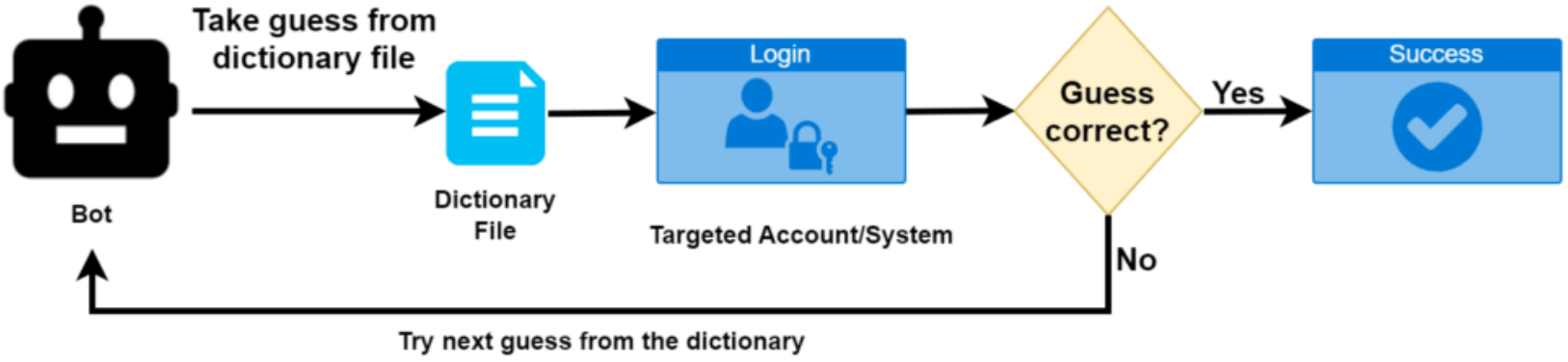
- Shorter password lengths are also easier to crack

John the Ripper

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

Dictionary Attacks

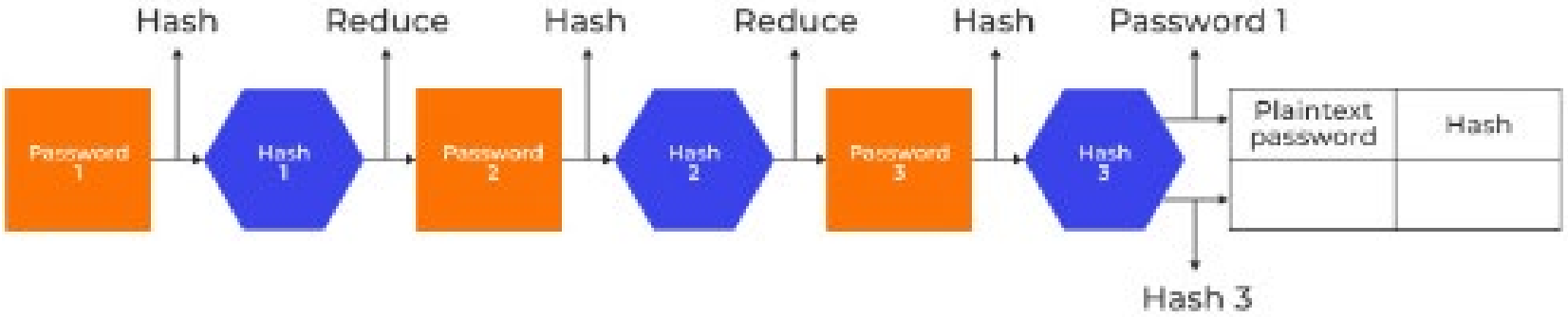
- use a preselected library of words and phrases to guess possible passwords.
- operates under the assumption that users tend to pull from a basic list of passwords, such as "password," "123abc" and "123456.“



Dictionary attack mechanism

Rainbow table Attacks

- uses a special table consisting of precomputed strings or commonly used passwords and corresponding hashes.
- works on passwords that are hashed — protected by using the hashing method



A rainbow table chain

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
  - In 2009- an SQL injection attack against online games service RockYou.com exposed 32 million plaintext passwords

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 / Proactive Password checker

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

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

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

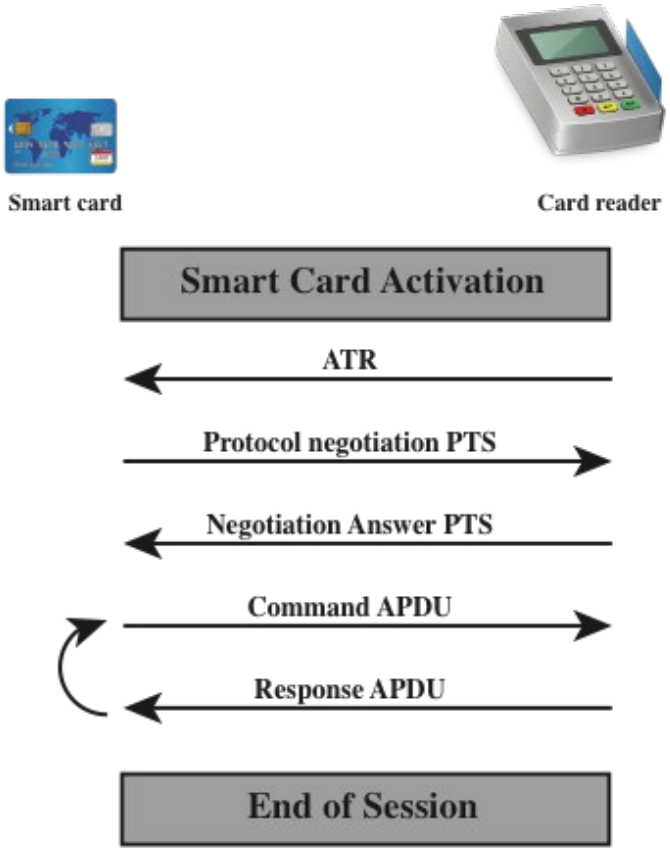
Smart Tokens

- **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
  - Memory
- **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

Smart Cards



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

Figure 3.6 Smart Card/Reader Exchange

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 include:
  - Facial characteristics
  - Fingerprints
  - Hand geometry
  - Retinal pattern
  - Iris
  - Signature
  - Voice

Biometric Authentication

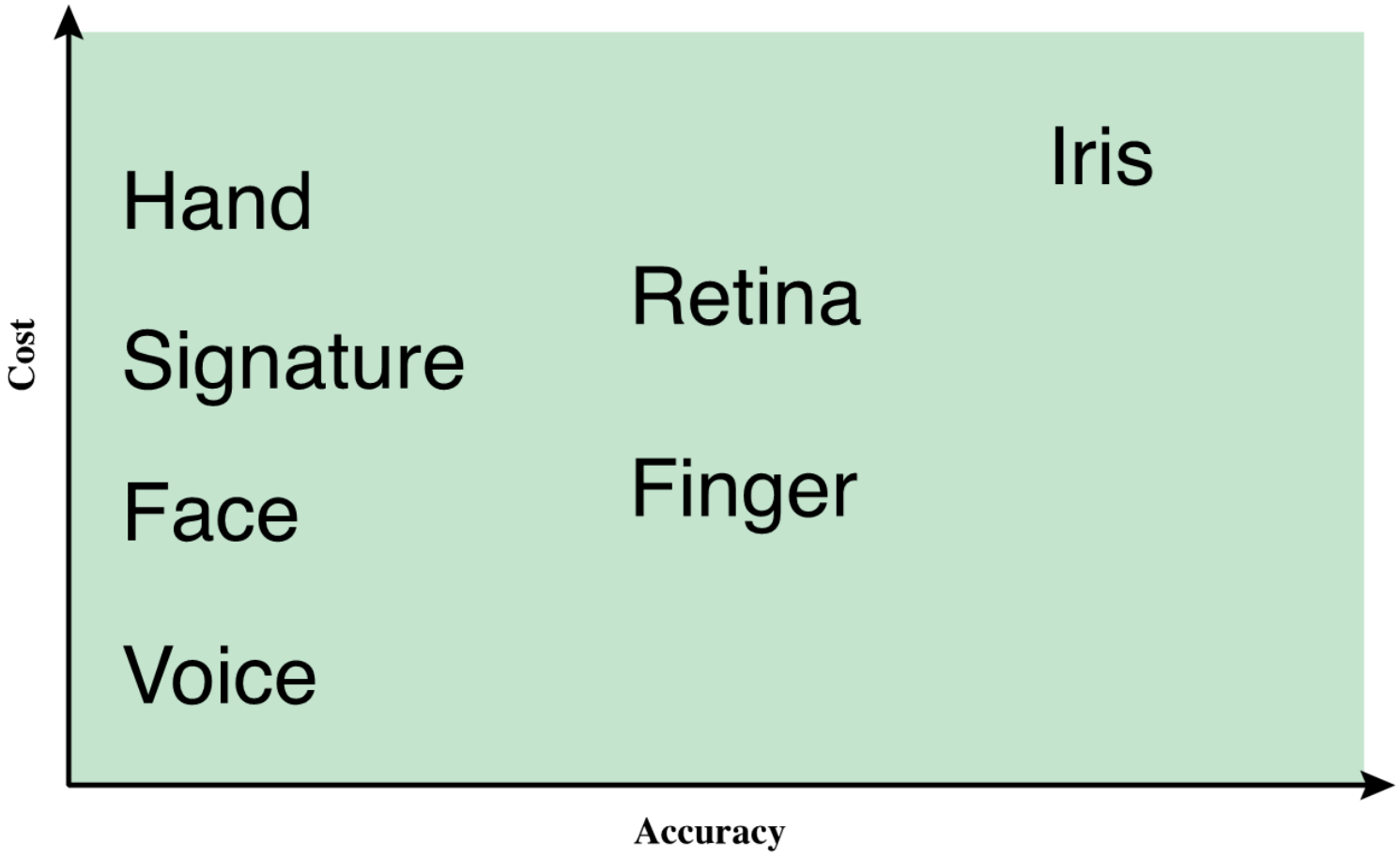


Figure 3.8 Cost Versus Accuracy of Various Biometric Characteristics in User Authentication Schemes.

Biometric Authentication

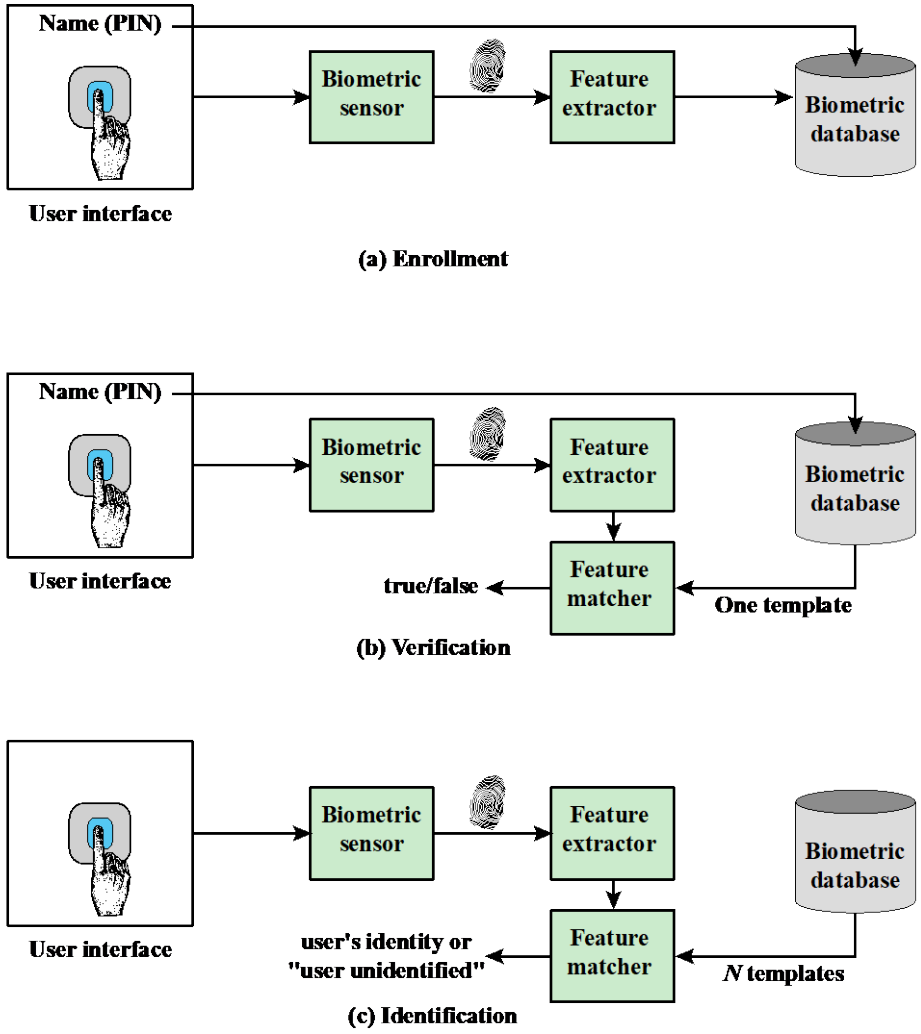
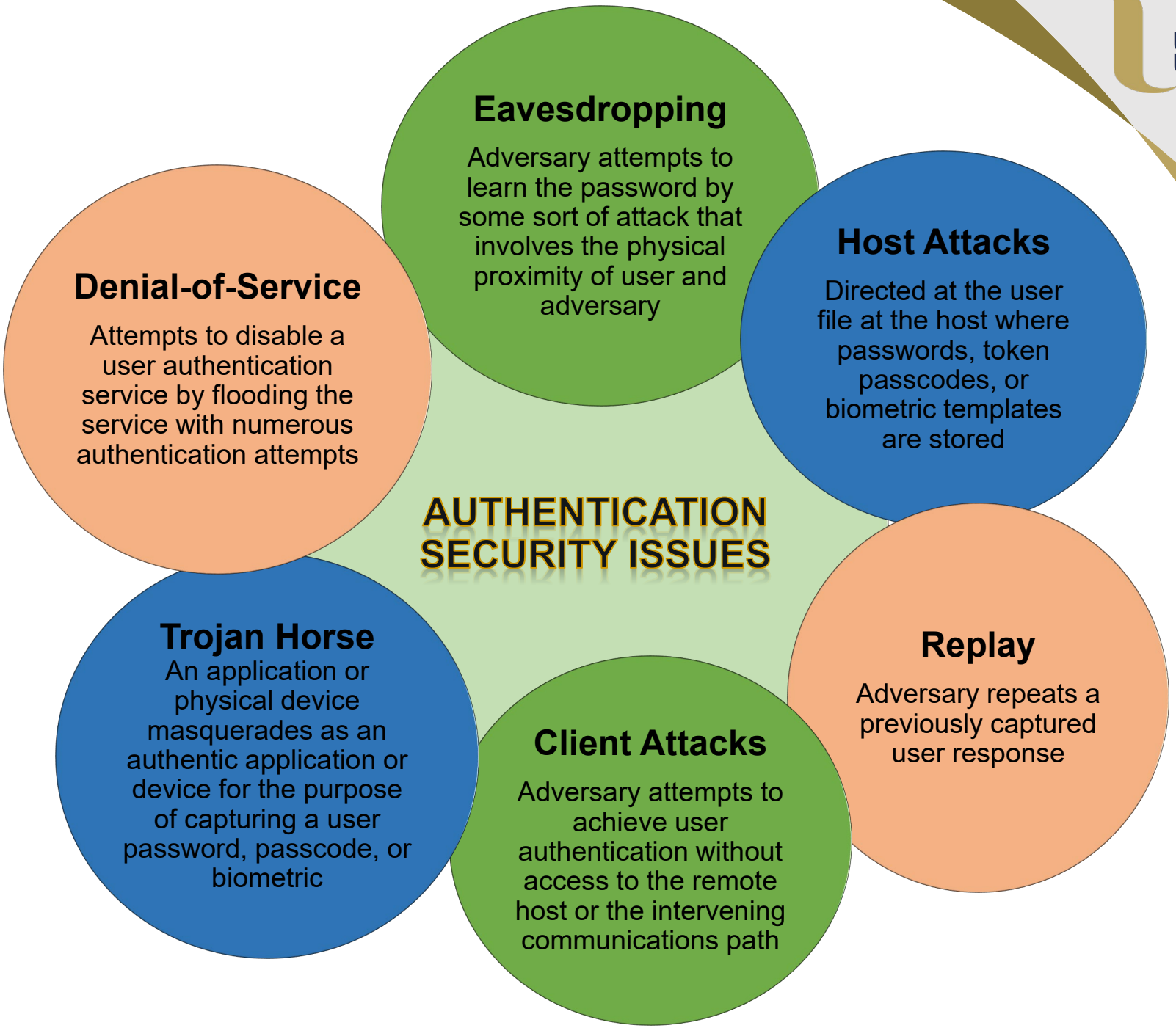


Figure 3.9 A Generic Biometric System. Enrollment creates an association between a user and the user's biometric characteristics. Depending on the application, user authentication either involves verifying that a claimed user is the actual user or identifying an unknown user.


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

Cyber attacks

Clients Attacks

- Client attacks target the client-side components of a system, aiming to exploit vulnerabilities in software or hardware that the end-users interact with.
- For example - Phishing is a common client attack. In a phishing attack, an attacker sends deceptive emails or messages to users, attempting to trick them into revealing sensitive information like login credentials.

Replay Attacks

- Replay attacks involve capturing and retransmitting data exchanged between two parties, often to gain unauthorized access or perform malicious actions.
- For example - In a replay attack against a secure access control system, an attacker intercepts an encrypted access request from a legitimate user. The attacker then replays this request to gain unauthorized entry to a secure facility.

Cyber attacks

Host Attacks

- Host attacks target vulnerabilities in a specific host or computer system. These vulnerabilities can be exploited to gain unauthorized access or compromise the host's integrity.
- For example - An example of a host attack is a "Remote Code Execution" attack. Attackers exploit a vulnerability in a host's software, allowing them to execute malicious code remotely on the compromised host, potentially gaining control of the system.

Eavesdropping Attacks

- Eavesdropping attacks involve intercepting and monitoring communications between two or more parties without their knowledge, potentially gaining access to sensitive information.
- For example - Sniffing unencrypted network traffic is a common eavesdropping attack. An attacker listens to data packets on an unsecured network, capturing and analyzing sensitive information such as login as credentials or personal messages.

Cyber attacks

DoS (Denial of Service) Attacks

- DoS attacks disrupt the normal operation of a system or network by overwhelming it with excessive traffic or requests, rendering it inaccessible to legitimate users.
- For example - An example of a DoS attack is a "Ping Flood." In a Ping Flood attack, an attacker sends a large number of ping requests to a target server or network. The server becomes overwhelmed by processing these requests and can't respond to legitimate requests.

Trojan Horse Attacks

- Trojan Horse attacks involve disguising malicious software as legitimate or benign software. Once installed, this software can perform malicious actions without the user's knowledge.
- For example – An attacker may create a fake antivirus software package and distribute it online. Users who download and install this software unknowingly infect their systems with malware, giving the attacker unauthorized access to their computer.

Access Control Definitions 1/2

Ulster University

NISTIR 7298 defines access control as:

"the process of granting or denying specific requests to: (1) obtain and use the information and related information processing services, and (2) enter specific physical facilities"

Access Control Definitions 2/2

RFC 4949 defines access control as:

"a process by which use of system resources is regulated according to a security policy and is permitted only by authorized entities (users, programs, processes, or other systems) according to that policy"

Access Control Principles

In a broad sense, all of computer security is concerned with access control

RFC 4949 defines computer security as:

"measures that implement and assure security services in a computer system, particularly those that assure access control service"

Access Control Principles

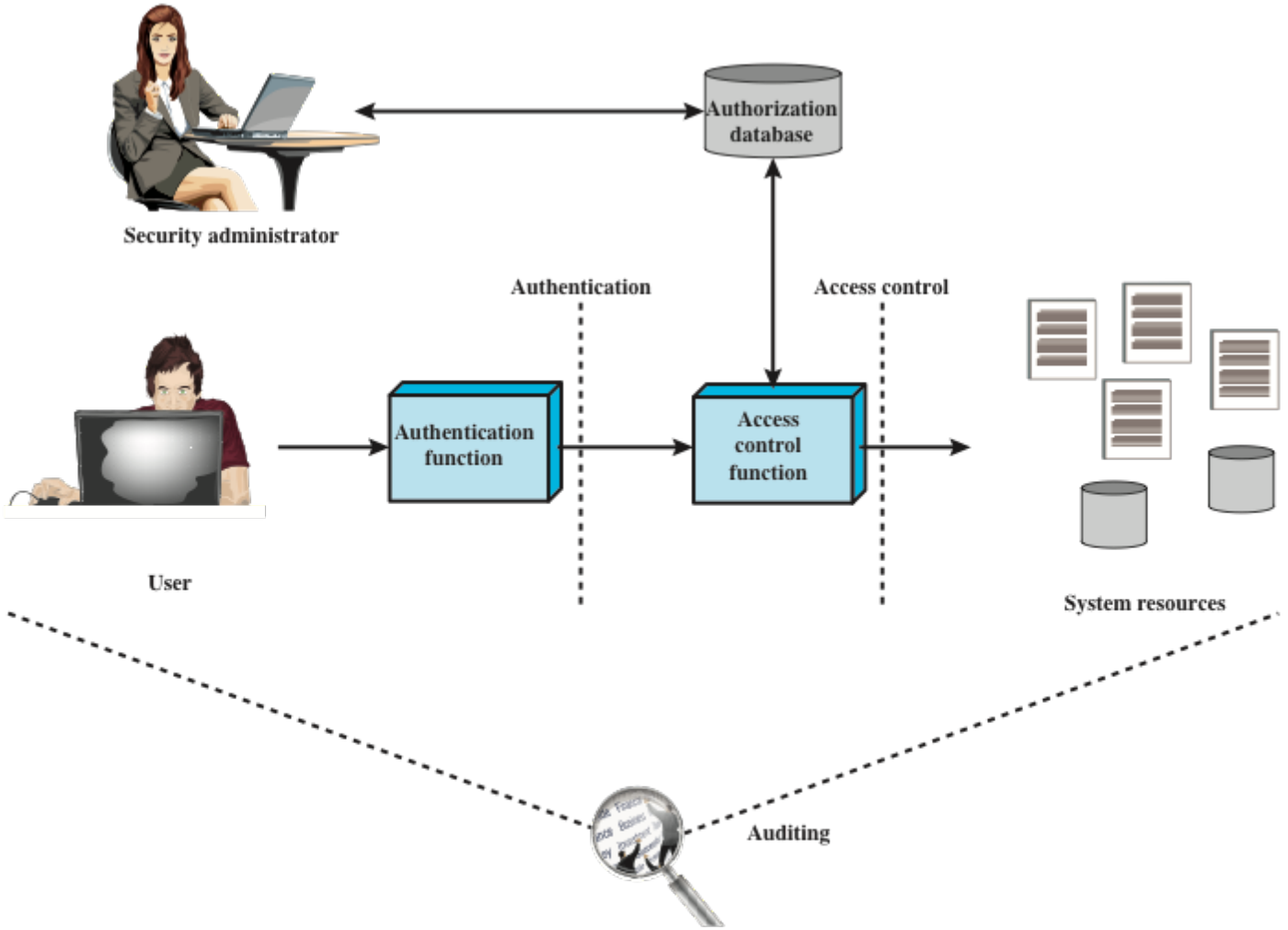
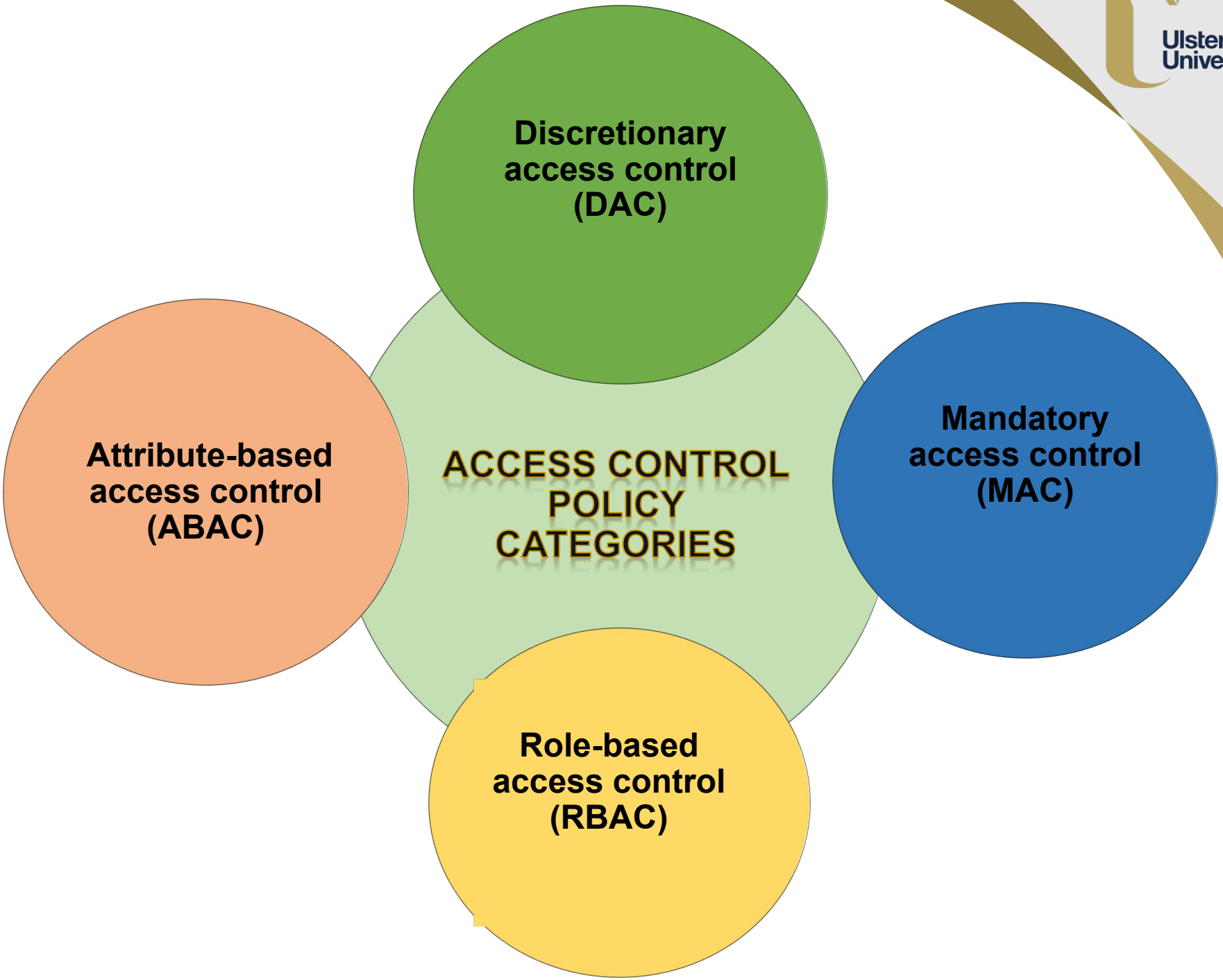
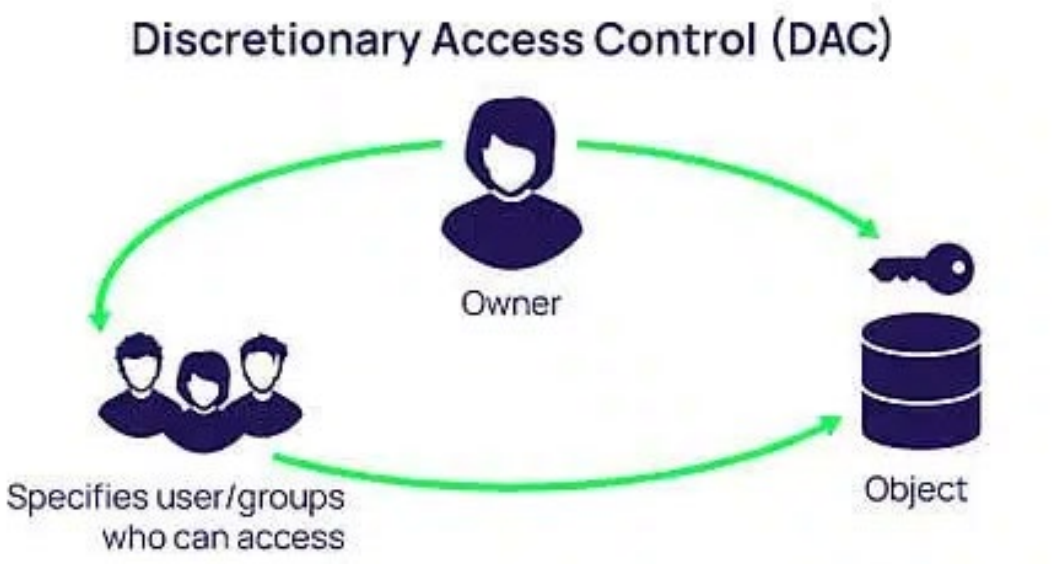


Figure 4.1 Relationship Among Access Control and Other Security Functions


Discretionary access control (DAC)
Attribute-based access control (ABAC)
ACCESS CONTROL POLICY CATEGORIES
Mandatory access control (MAC)
Role-based access control (RBAC)

Access Control Policies

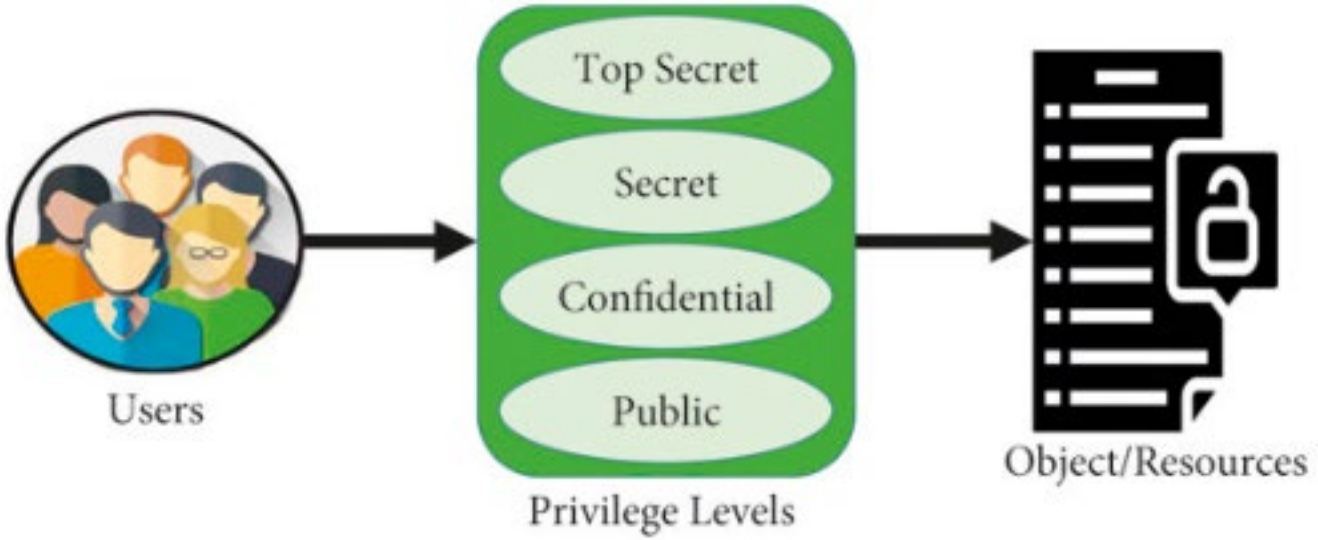
- **Discretionary access control (DAC)**
  - Controls access based on the identity of the requestor and on access rules (authorizations) stating what requestors are (or are not) allowed to do



https://spectralops.io/blog/examples-of-discretionary-access-control/

Access Control Policies

- **Mandatory access control (MAC)**
  - Controls access based on comparing security labels with security clearances

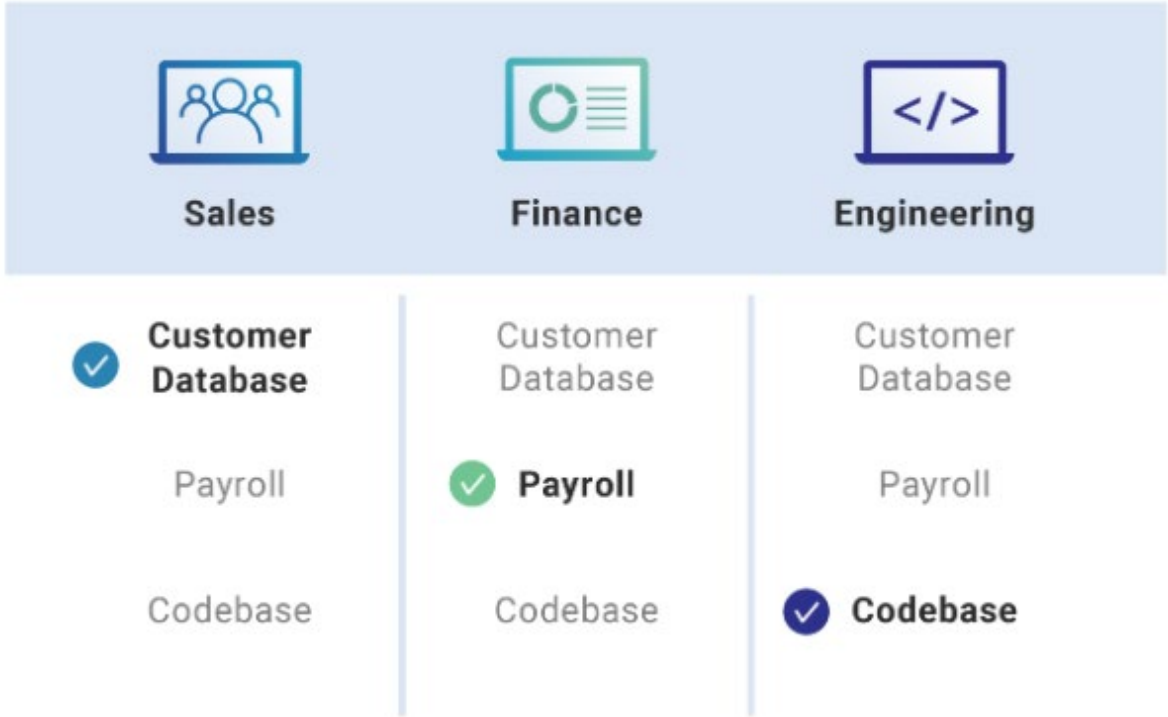


Mandatory Access Control (MAC)

https://www.researchgate.net/figure/view-of-mandatory-access-control-MAC_fig4_358430862

Access Control Policies

- **Role-based access control (RBAC)**
  - Controls access based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles

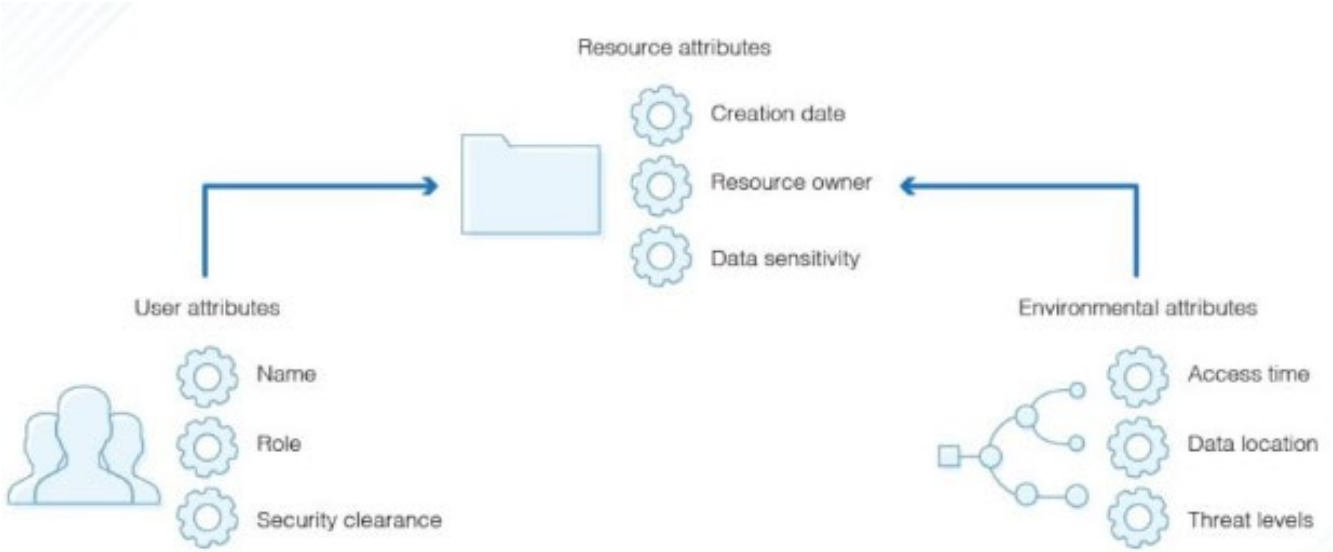


Role Based Access Control (RBAC)

https://www.cloudflare.com/en-gb/learning/access-management/role-based-access-control-rbac/

Access Control Policies

- **Attribute-based access control (ABAC)**
  - Controls access based on attributes of the user, the resource to be accessed, and current environmental conditions



Attribute Based Access Control (ABAC)

https://www.dnsstuff.com/rbac-vs-abac-access-control

Subjects, Objects, and Access Rights

Ulster University

Subject

- An entity capable of accessing objects
- Three classes
  - Subject
  - Owner
  - Group

Object

- A resource to which access is controlled
- Entity used to contain and/or receive information

Access right

- Describes the way in which a subject may access an object
- Could include:
  - Read
  - Write
  - Execute
  - Delete
  - Create
  - Search

Discretionary Access Control (DAC)

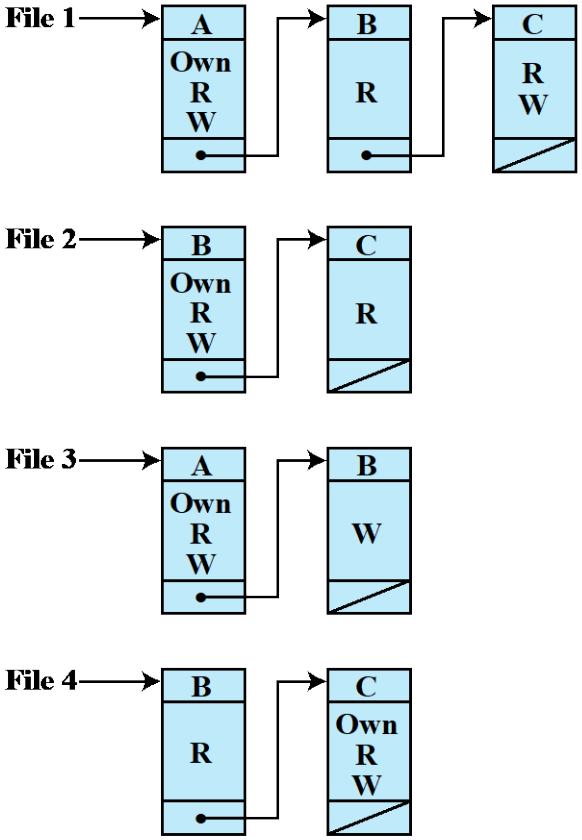
- Scheme in which an entity may be granted access rights that permit the entity, by its own violation, to enable another entity to access some resource
- Often provided using an access matrix
- One dimension consists of identified subjects that may attempt data access to the resources
- The other dimension lists the objects that may be accessed
- Each entry in the matrix indicates the access rights of a particular subject for a particular object

Access control structure

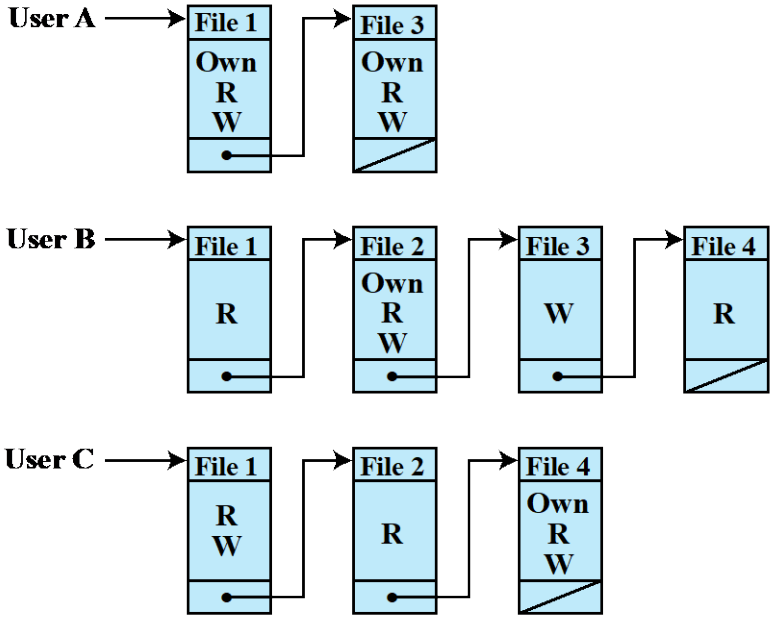
		OBJECTS			
		File 1	File 2	File 3	File 4
SUBJECTS	User A	Own Read Write		Own Read Write	
	User B	Read	Own Read Write	Write	Read
	User C	Read Write	Read		Own Read Write

(a) Access matrix

Access control structure



(b) Access control lists for files of part (a)



(c) Capability lists for files of part (a)

Figure 4.2 Example of Access Control Structures

Ulster University

Thanks!