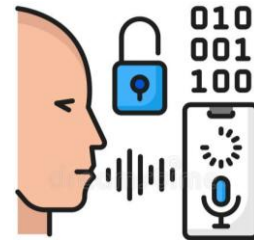
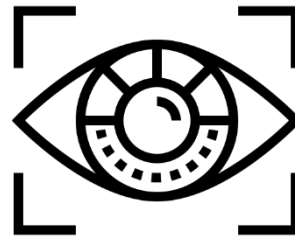
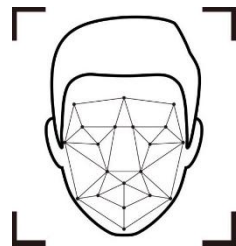
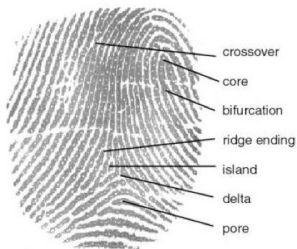


# Something You Are

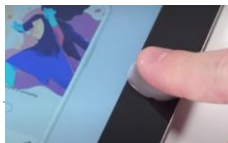
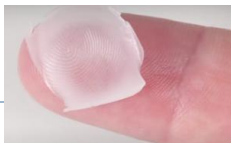
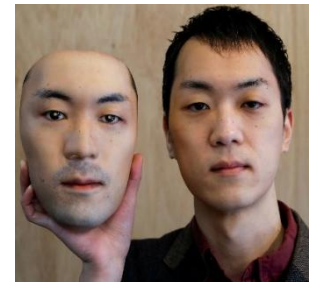
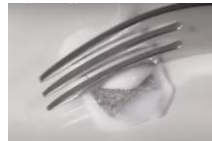
## Biometrics measure some physical characteristic

- ▶ Fingerprint, face recognition, retina scanners, voice, etc.
- ▶ Can be extremely accurate and fast



## Limitations of biometrics

- ▶ Private, but not secret. Maybe encoded on your glass, door handle
- ▶ Revocation is difficult: Sorry, your iris has been compromised, please create a new one...



# Authorization

---

## Access control

- ▶ Implement a **security policy** that specifies who or what may have access to each specific resource in a computer system, and the type of access that is permitted in each instance.
- ▶ It mediates between a user (or a process executing on behalf of a user) and system resources (e.g., applications, network sockets, firewalls).

## Three basic elements in a security policy:

- ▶ Subject: process or users
- ▶ Object: resource that is security-sensitive
- ▶ Operations: actions taken using that resource

# Subject

---

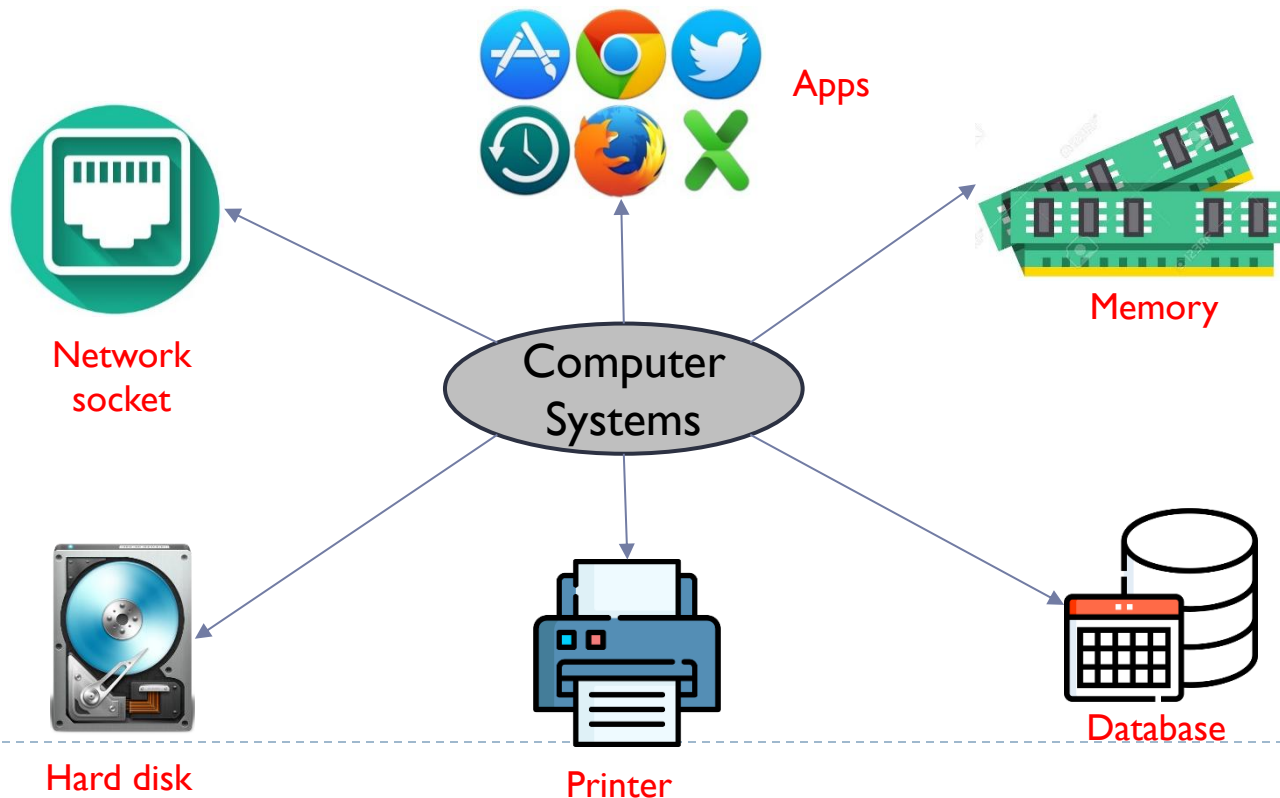
A **subject** is typically held accountable for the actions they have initiated. There can be three types of subjects.

- ▶ **Owner**: this may be the creator of a resource. For system resources, ownership may belong to a system administrator.
- ▶ **Group**: in addition to individual users, privileges can also be assigned to a group of users. A user joining the group will automatically have the corresponding privileges, while a user quitting the group will lose the corresponding permissions. A user may belong to multiple groups. The concept of groups makes it easier to manage and update the permissions.
- ▶ **Other**: the **least amount of access** is granted to users who are able to access the system but are not included in the categories of owner and group for this resource.

# Object

An **object** is a resource to which access is controlled.

- ▶ An entity used to contain and/or receive information.
- ▶ Examples: records, blocks, pages, segments, files, portions of files, directories, directory trees, mailboxes, messages, and programs.



# Operation

## Describes the way in which a subject may access an object

- ▶ **Read:** user may **view** information in a system resource (e.g., a file, selected records in a file, selected fields within a record, or some combination).  
Read access includes **the ability to copy or print**.
- ▶ **Write:** user may **modify** data in the system resource (e.g., files, records, programs).
- ▶ **Execute:** user may **execute** specified programs.
- ▶ **Delete:** user may **delete** certain system resources, such as files or records.
- ▶ **Create:** user may **create** new files, records, or fields.
- ▶ **Search:** user may **list** the files in a directory or otherwise **search** the directory.

# Access Control Matrix

## A popular implementation of access control policy.

- ▶ One dimension consists of identified subjects that may attempt 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

		Objects			
Subjects		File 1	File 2	File 3	File 4
	User A	Read Write Execute		Read Write Execute	
	User B	Read	Read Write Execute	Write	Read
	User C	Read Write	Read		Read Write Execute

# Update Access Control Matrix

## Possible changes over Access Control Matrix

- ▶ Create subject  $s$ : add a new row  $s$ . This is typically done by the system administrator.
- ▶ Create object  $o$ : create a new column  $o$ . This is typically done by the system administrator.
- ▶ Grant permission  $r$  for subject  $s$  over object  $o$ : enter  $r$  to entry  $M_{s,o}$ . This is typically done by the resource owner or system administrator.
- ▶ Revoke permission  $r$  for subject  $s$  over object  $o$ : delete  $r$  from entry  $M_{s,o}$ . This is typically done by the resource owner or system administrator.
- ▶ Destroy subject  $s$ : delete the row  $s$ . This is typically done by the system administrator.
- ▶ Destroy object  $o$ : deletes the column  $o$ . This is typically done by the system administrator.