Something You Have

Different types of possessions for authentication

- Tokens
- Smartcards: a physical card + a smart card reader

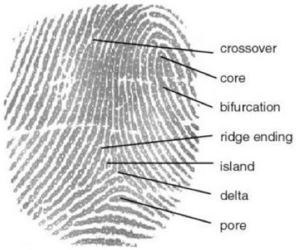
Limitations of physical belongings

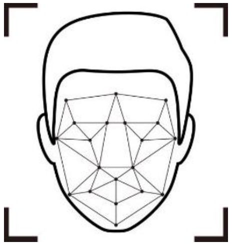
- Easy to get lost. Therefore, it is safer to combine users' knowledge with physical belongings. This is referred to as **two-factor authentication**
- High cost (e.g., $15-$25, banks with million customers).
- Possible to get damaged (e.g., card in the washing machine, battery death)
- Non-standard algorithms.

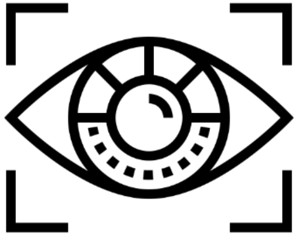
Something You Are

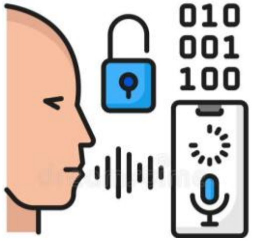
Biometrics measure some physical characteristic

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



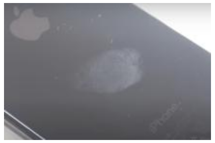


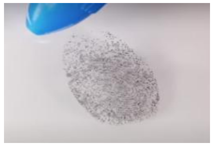


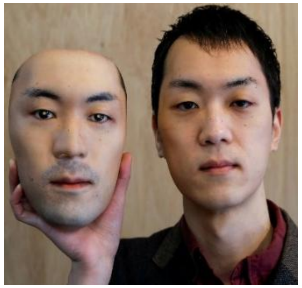


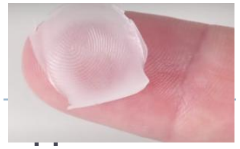
Limitations of biometrics

- 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...









https://www.youtube.com/watch?v=VYI9XNO4XzU

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

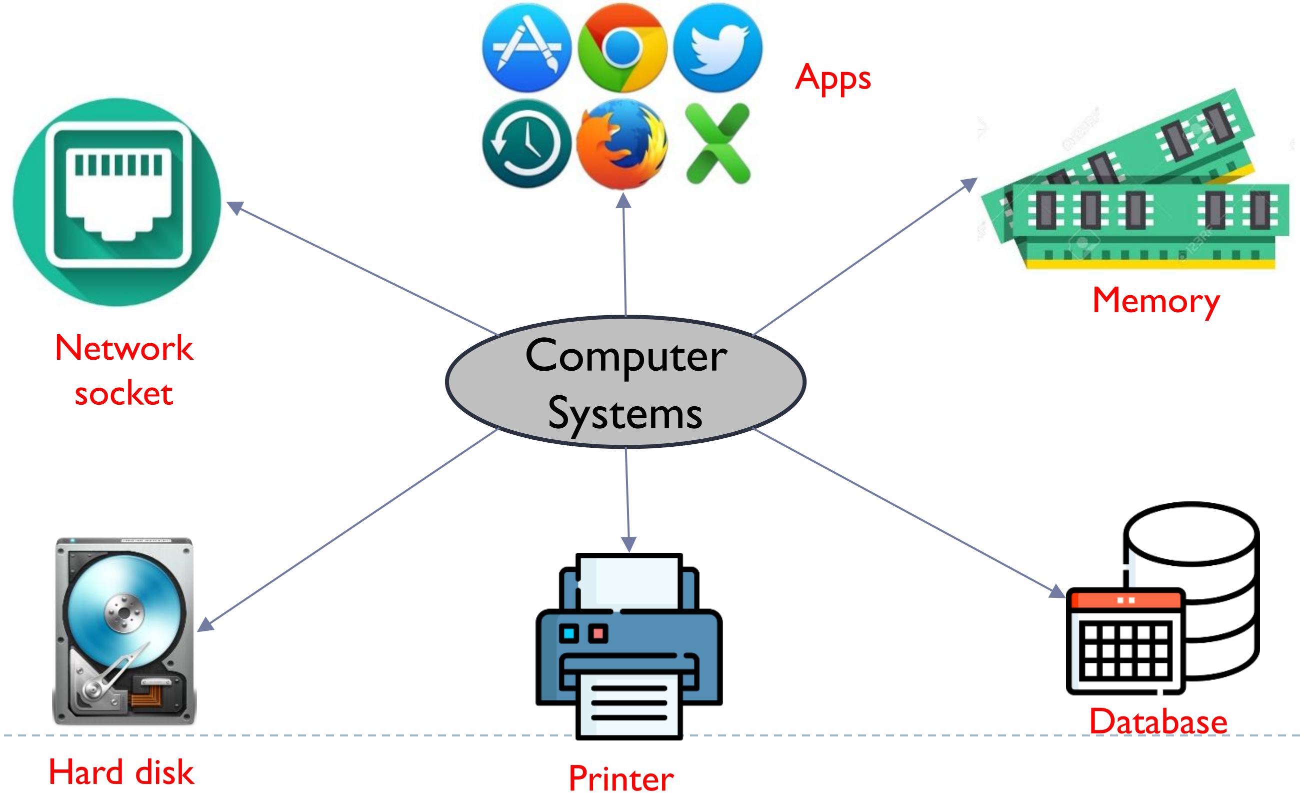
A subject is typically held accountable for the actions they have initiated. There can be three types of subjects.

- **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 quiiting the group will loss 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.


Computer Systems
Apps
Network socket
Memory
Hard disk
Printer
Database