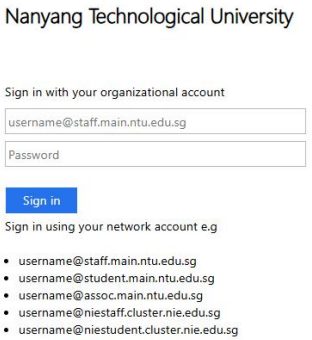
Something You Know: Password

Password is the most common way to prove who you are

- Adopted by various networking websites and applications
- The security of the password-based authentication mechanism depends on the strength of the selected password, i.e., the chance attacker can guess the password.
- The trade-off between the password security and convenience:
  - Weak password is easy to memorize, but also easy to be guessed.
  - Complex password is strong but results in frustrated users



Weak Password

A weak password is a character combination that is easy for friends, bad actors or password-hacking software to guess

- Short passwords: a single word (e.g., password) or numerical phrase (e.g., 12345).
- Recognizable keystroke patterns: take a look at your keyboard and find QWERTY
- Personal information in passwords: e.g., date of birth, address, name
- Repeated letters or numbers: e.g., 55555, aaaa

Password Popularity – Top 20

Rank	Password	Number of Users with Password (absolute)
1	123456	290731
2	12345	79078
3	123456789	76790
4	Password	61958
5	iloveyou	51622
6	princess	35231
7	rockyou	22588
8	1234567	21726
9	12345678	20553
10	abc123	17542

Rank	Password	Number of Users with Password (absolute)
11	Nicole	17168
12	Daniel	16409
13	babygirl	16094
14	monkey	15294
15	Jessica	15162
16	Lovely	14950
17	michael	14898
18	Ashley	14329
19	654321	13984
20	Qwerty	13856

Strong Password

A strong password is a long combination of unique characters that is difficult for other people to guess or technology to crack

- Lengthy combinations: long passwords with various character types, such as numbers, letters and symbols, e.g., N0r+Hc^R0|in^99
- Mnemonic: create passwords inspired by events only notable to you, e.g., a string of first letters of a meaningful sentence
- Non-dictionary words: dictionary words — formal or slang — are publicly known combinations of characters stored in a database that cybercriminals access using software to input thousands of passwords per second

A strong authentication system requires users to change their password periodically (e.g., every six months), and the new passwords must be different from the used ones.

Something You Have

Different types of possessions for authentication

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

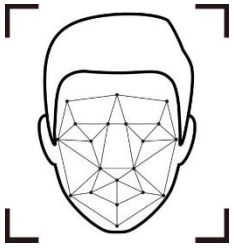
Limitations of physical belongings

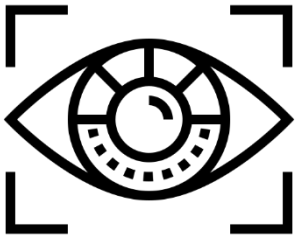
- Easy to get lost. Therefore, it is safer to combine users' knowledge with physical belongings. This is referred to as **two-factor authentication**
- High cost (e.g., $15-$25, banks with million customers).
- Possible to get damaged (e.g., card in the washing machine, battery death)
- Non-standard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

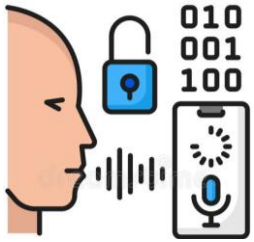
Something You Are

Biometrics measure some physical characteristic

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

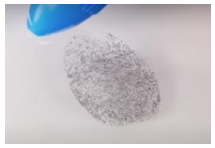


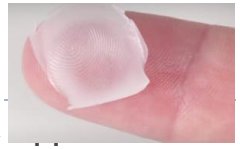


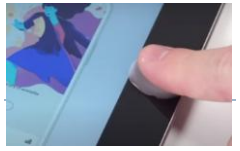


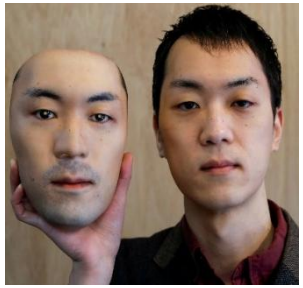
Limitations of biometrics

- 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.