ĐẠI HỌC TÔN ĐỨC THẮNG
TON DUC THANG UNIVERSITY

Chapter 4
Identification and Authentication

ĐẠI HỌC TÔN ĐỨC THẮNG
TON DUC THANG UNIVERSITY

Outline

- **Overview about identification and authentication**
  - Password,
  - Bootstrapping,
  - Searching password (Dictionary, guessing, exhaustive),
  - Stealing of password
  - Preventive measure
  - Example on ATM
  - Password Reset: Security Questions
- **Biometric**
- **Multi-factor authentication**
  - Case studies: Sms vs Token

Username and Password

- The first step is called **identification**: you announce who you are.
- The second step is called **authentication**: you prove that you are who you claim to be.
- **The attacker may:**
  - intercept the password at the time a new user account is created,
  - try to guess the password,
  - get the password from the user through phishing or spoofing, or by key-loggers,
  - get the password from social engineering.

Authenticating

Stage 1: Bootstrapping

- Server and a user established a common password. The server keeps a file recording the identity (aka userid, username) and the corresponding password.

Stage 2: Authentication

- Users could be asked to come to an office and collect their password personally.
- Or the password could be transfered by mail, email, or phone, or entered by the user on a web page.

Authenticating

Authenticate a remote user when the user has not got a password yet:

- Do not give the password to the caller but call back an authorized phone number.
- Send mail by courier with personal delivery.
- Send passwords that are valid only for a single login request.
- Request confirmation on a different channel to activate the user account (e.g. send confirmation by SMS.

Authenticating

- **The procedures for resetting a password:**
  - Need an Instantly resetting
  - Have a desk staff working all the time to resolve incoming requests.
  - Security training has to be given to personnel at the hot desk.

➔Thus, password support can become a non-negligible cost factor

Guessing Passwords

- **Exhaustive search (brute force):** try all possible combinations of valid symbols, up to a certain length;

- **Intelligent search:** search through a restricted name space, e.g. try passwords that are somehow associated with a user such as name, names of friends and relatives, car brand, car registration number, phone number, etc., or try passwords that are generally popular (called dictionary attack)

Stealing the passwords

Sniffing

- ***Shoulder surfing***: This is the look-over-the-shoulder attack.
- ***Intercepting the communication***: Some systems simply send the password over the public network in clear (i.e. not encrypted)
- **Other means:**
  - ***Sniff*** the wireless keyboard.

(see http://arstechnica.com/security/2015/01/meet-keysweeper-the-10-usb-charger-that-steals-ms-keyboard-strokes/)

  - **Using sound** made by keyboard.

See http://www.cs.berkeley.edu/~tygar/papers/Keyboard_Acous6c_Emana6ons_Revisited/ccs.pdf)

Stealing the passwords

Presenting SplashData's "Worst Passwords of 2014":

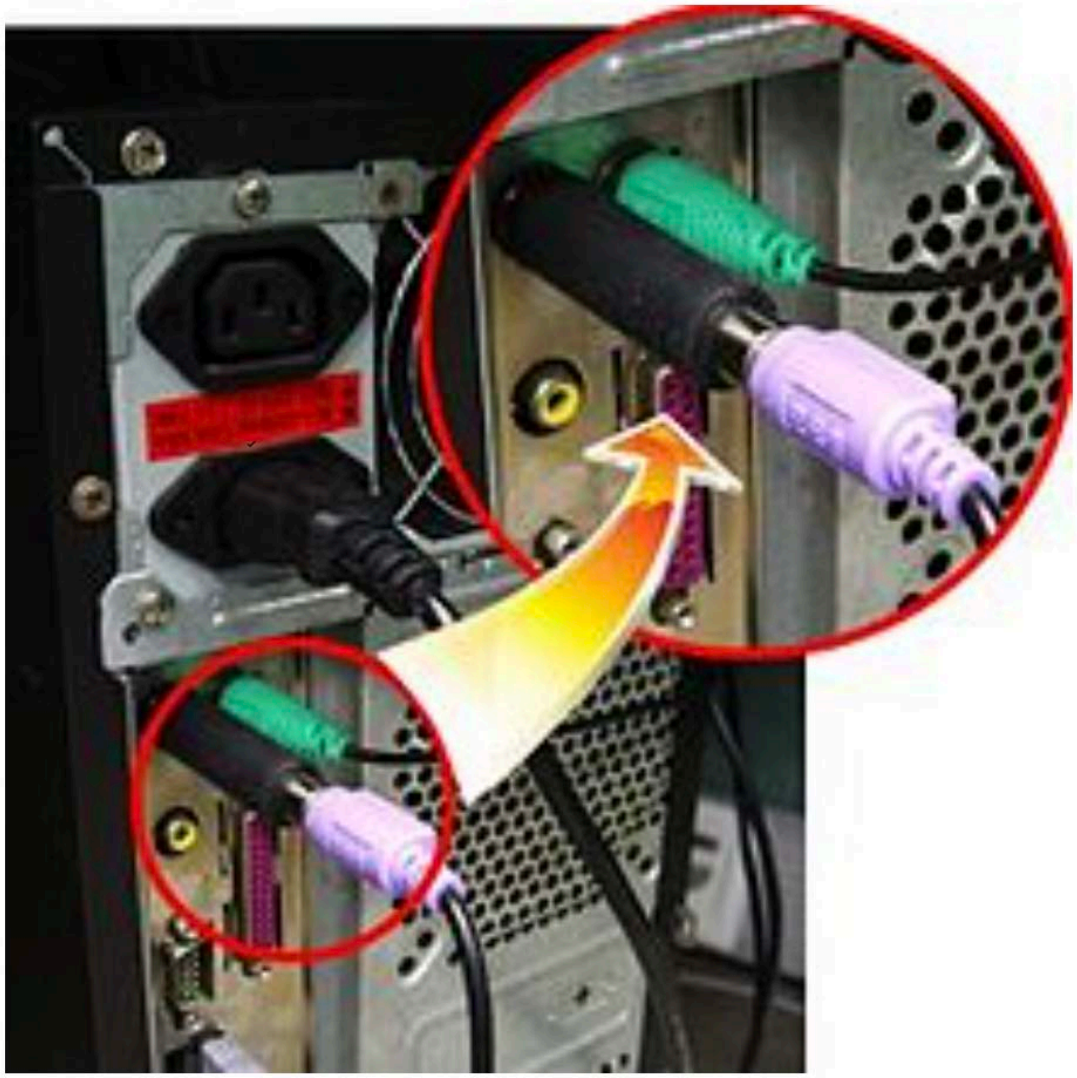
1 123456 (Unchanged from 2013)
2 password (Unchanged)
3 12345 (Up 17)
4 12345678 (Down 1)
5 qwerty (Down 1)
6 1234567890 (Unchanged)
7 1234 (Up 9)
8 baseball (New)
9 dragon (New)
10 football (New)
11 1234567 (Down 4)
12 monkey (Up 5)
13 letmein (Up 1)
14 abc123 (Down 9)
15 111111 (Down 8)
16 mustang (New)
17 access (New)
18 shadow (Unchanged)
19 master (New)
20 michael (New)
21 superman (New)
22 696969 (New)
23 123123 (Down 12)
24 batman (New)
25 trustno1 (Down 1)

Stealing the passwords

Viruses, Key-logger

- Some computer viruses are designed as a ***key-logger***.
- *Hardware key-logger:* the image in the next slide is self- explanatory.
- **read** "Hardware-based key-loggers" in http://en.wikipedia.org/wiki/Keystroke_logging

Stealing the passwords



Stealing the passwords

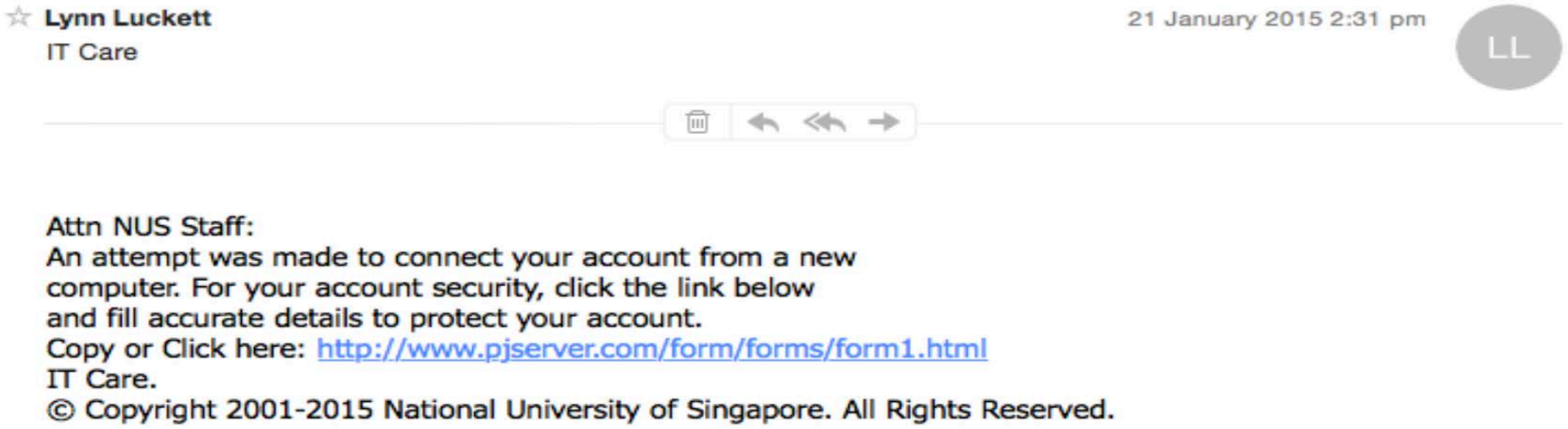
Login spoofing

- Attacker displays a “spoofed” login screen.
- Prevention: Some systems have a ***secure attention key*** or ***secure attention sequence***. When they are pressed, the system starts the trusted login processing (e.g. Ctrl+Alt+Del for Windows)

Stealing the passwords

Phishing

- Same as login spoofing, here, the user is tricked to voluntarily sends the password to the attacker.
- Phishing attacks for password under some false pretense. For example:



Stealing the passwords

- Phishing attack is a ***social engineering*** attack.
- Phishing of passwords is typically done through emails, over phone calls.
- Wiki definition of social engineering:

"Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information."

See http://en.wikipedia.org/wiki/Social_engineering_%28security%29

Stealing the passwords

Cache

- When using a shared workstation (for e.g. a browser in airport), information keyed in could be cached. The next user may able to see the cache.

Insider attack

- The malicious system administrator steals the password file.
- The system administrator's account is compromised (e.g. password stolen via phishing), leading to lost of password file.

Preventive measure

❑ What are your defences?

- ✓ Change default passwords
- ✓ Using Strong Password
- ✓ Password Policy
- ✓ Additional protection to password files

Using Strong Password

- **Random:** A password is chosen randomly among all possible keys using an automated password generator. High "entropy" but difficult to remember.

  e.g., *3n5dcvUD9cfm* (12 characters)

- **User selection:**
  - Combining and Altering Word: *B@nkC@mera*
  - Mnemonic Method: *Pbmbval!*

Password Policy

Password Policy: Rules set by the organiza6on to ensure that users use strong passwords, and to minimize lost of passwords.

- *Password checkers:* prevent users from choosing 'weak' passwords. e.g. using the password dictionary
- *Password generation*: Users have to adopt a password proposed by the system.
- *Password ageing:* Forcing users to change passwords at regular intervals.
- *Limit login attempts:* monitors unsuccessful login attempts.

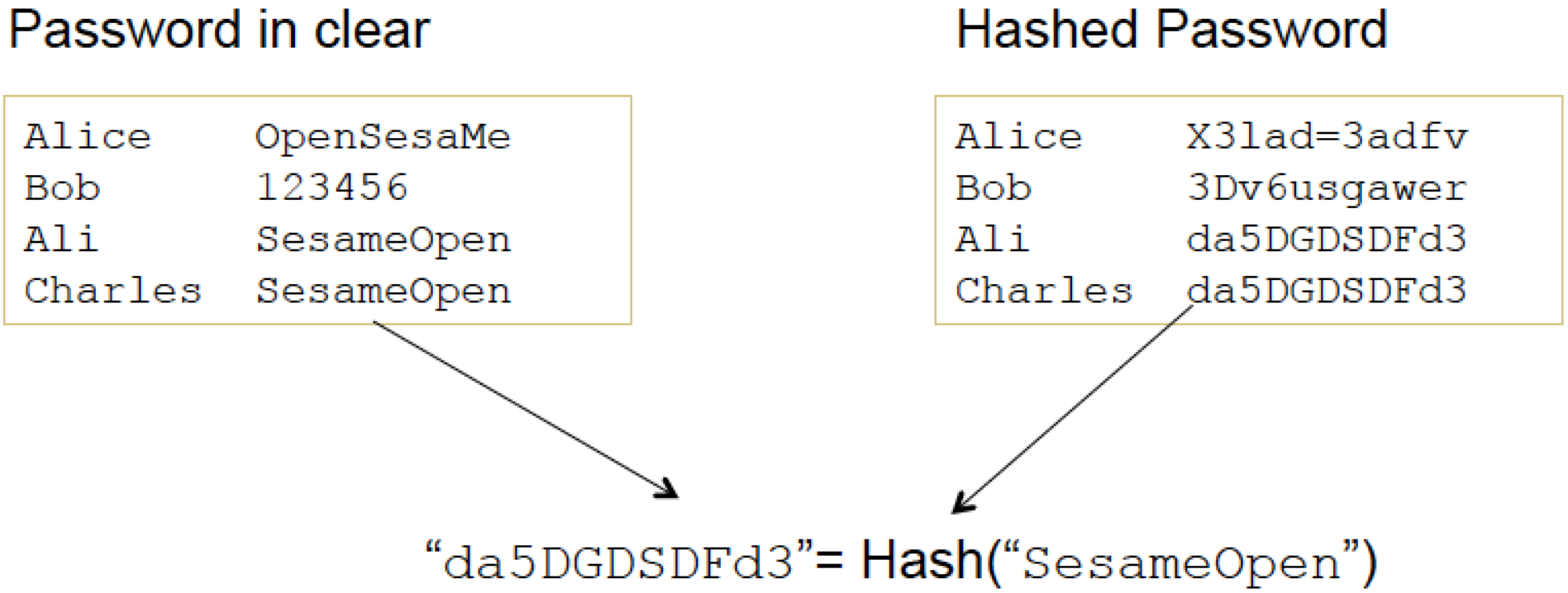
Additional protection to password files

- The password file could be leaked, due to insider attack, accidental leakage, system being hacked, etc.
- The password file store the *userid+password*.
- Hence, it is desired to add an additional layer of protection to the password file.
- There are many well-known incidents where unprotected or weakly protected password files are leaked, leading to a large number of passwords being compromised.

  (https://en.wikipedia.org/wiki/2012_LinkedIn_hack)

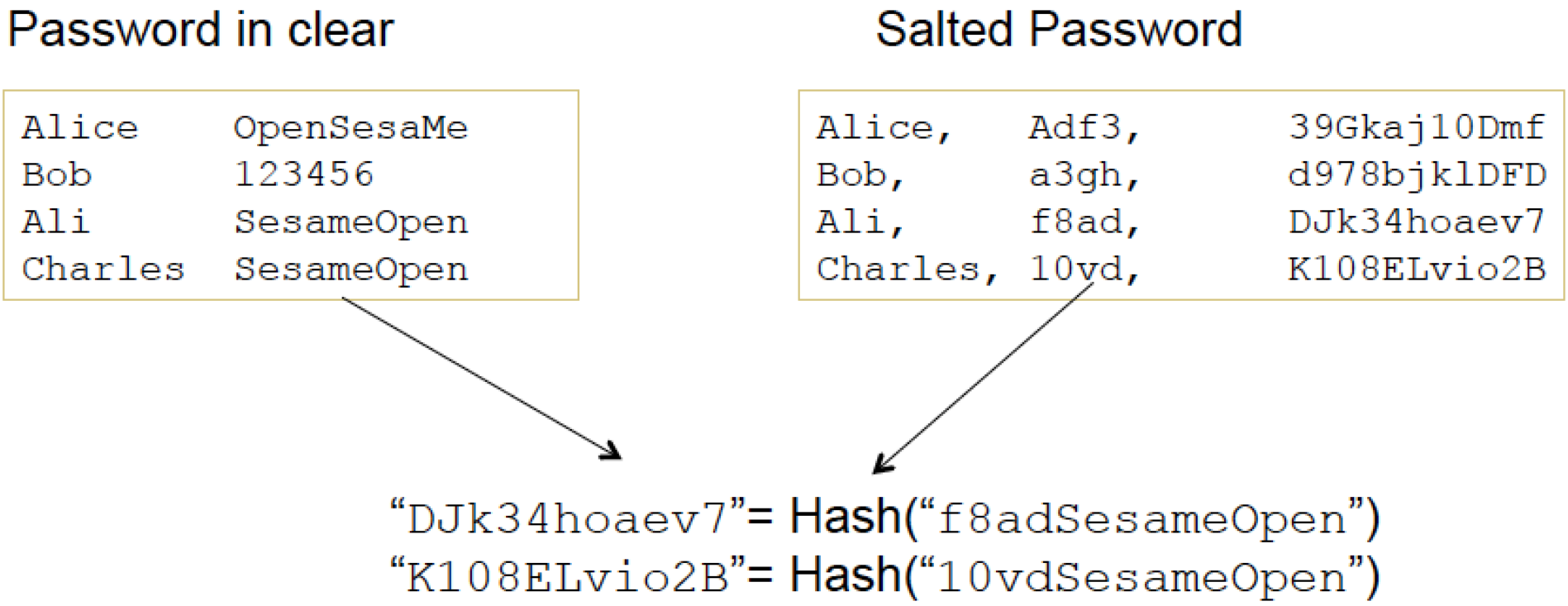
Additional protection to password files

- Passwords should be “hashed” and stored in the password files.
- During authentication, the password entered by the entity is being hashed, and compared with the the value



Additional protection to password files

- The same password would be hashed to two different values for two different user id. Why? (tutorial)
- This can be achieved using salt.



Security Questions

- Security Questions can be viewed as a mechanism for fallback authentication, or a self-services password reset.
- Enhancing “usability”: a user can still login even if password is lost.
- Reducing cost: reduces operating cost of helpdesk.
- Students read: https://www.owasp.org/index.php/Choosing_and_Using_Security_Questions_Cheat_Sheet

Choices of Security Questions

- **Memorable**: If users can't remember their answers to their security questions, you have achieved nothing.
- **Consistent**: The user's answers **should not** change over time.
- **Safe**: The answers to security questions **should not** be something that is easily guessed, or research.

(https://www.owasp.org/index.php/Choosing_and_Using_Security_Ques6ons_Cheat_Sheet)

Question: Give example of "bad" security questions?

Example on ATM

ATM Card

- To get authenticated, the user has to present a card, and the PIN. Note that the PIN plays the role of password.
- The card contains a magnetic strip, which stores the user account id. Essentially, the magnetic strip simplifies the input of account id into the ATM system: instead of keying it in, just inserting the card. Data are encoded into the magnetic strip using well-known standards. Given a valid card, an attacker can “copy” the card by reading the info from the card, and write it to the spoofed card.

Example on ATM

ATM skimmer

An ATM skimmer steals the victim's account id (username) and PIN (password).

The skimmer consists of:

- 1) a card-reader attached on top of existing ATM reader;
- 2) a camera overlooking the keypad, or a spoofed key-pad on top of existing keypad;
- 3) some means to record and transmit the information back to the attacker.

With the information obtained from (1), the attacker can spoof the victim's ATM card. With (2), the attacker obtain the PIN.

Example on ATM

- Well known incidents in Singapore: DBS in 2012.

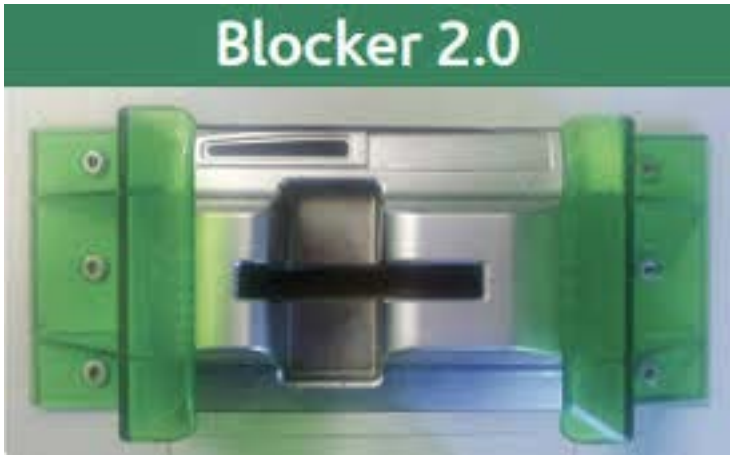
"$1 million stolen from the bank accounts of 700 DBS and POSB customers."

- See http://news.asiaone.com/News/Latest+News/Singapore/Story/A1Story20120223-329820.html

ATM SKIMMING

MEASURES

- ***Anti-Skimmer device:*** A device that prevents external card reader to be attached onto the ATM.
- Shielding the keypad.
- Awareness among users.

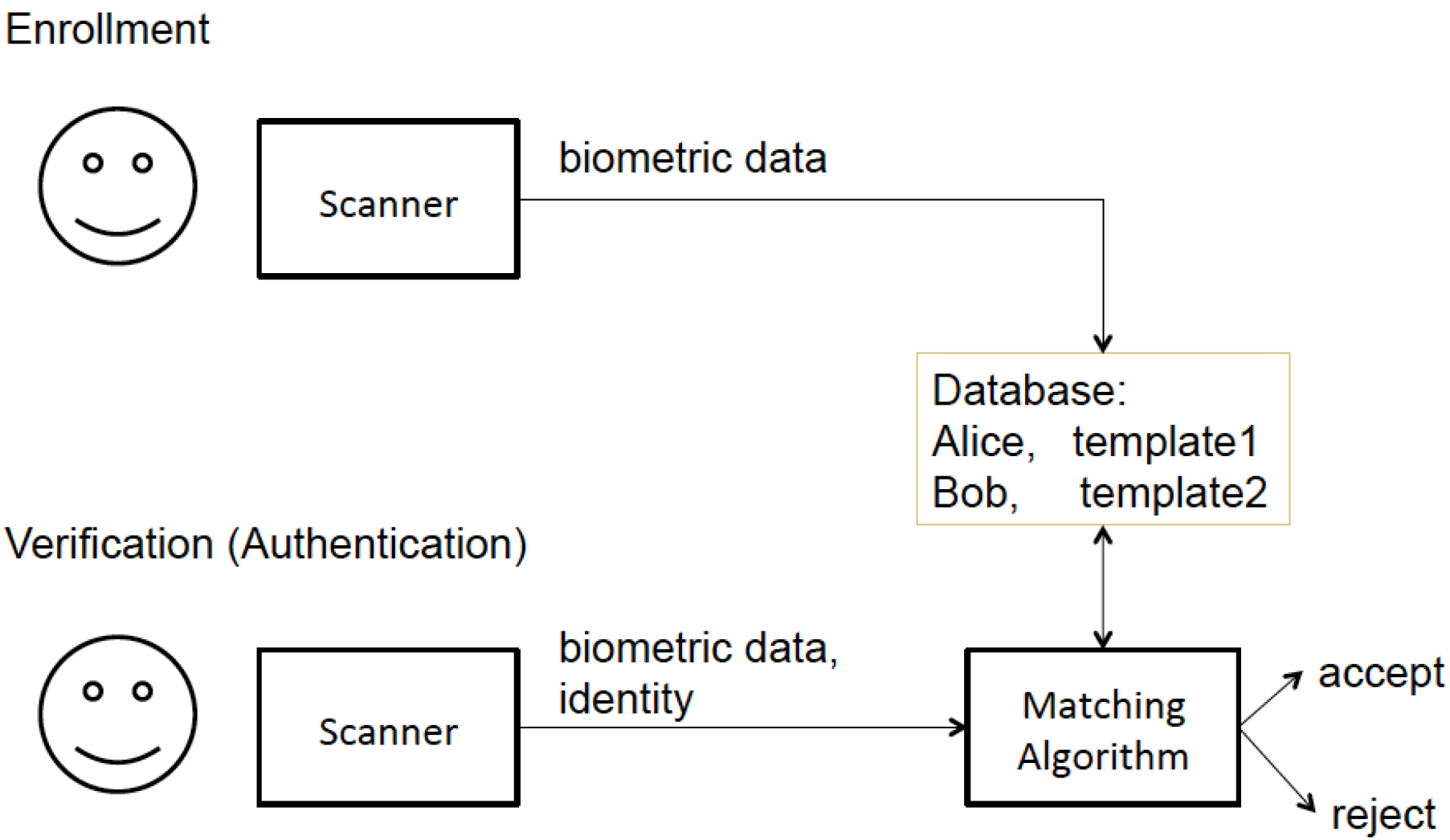


Biometric

- Biometric use unique physical characteristics of a person for authentication.
- During enrollment, a template of an user's biometric data is captured and stored.
- During verification, biometric data of the person-in-question is captured and compared with the template using a matching algorithm. The algorithm decides whether to accept or reject.

(see http://i-talents.vn/Sinh-trac-van-tay-p40/Dich-vu-p3/Sinh-Trac-Hoc-Dau-Van-Tay-La-Gi-p12)

Biometric


Enrollment
Scanner
biometric data
Database:
Alice, template1
Bob, template2
Verification (Authentication)
Scanner
biometric data,
identity
Matching
Algorithm
accept
reject

Biometric

- Unlike password, there are inevitable noise in capturing the biometric data, leading to error in making the matching decision:
  - FMR (False match rate)
  - FNMR (false non-match rate) .

Biometric

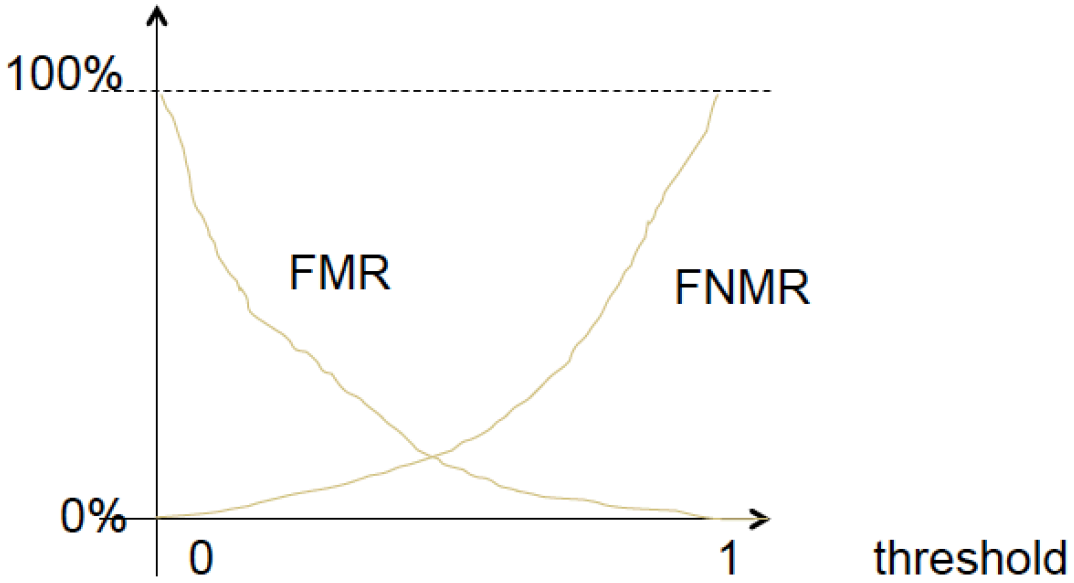
$$FMR = \frac{\text{number of successful false matches (B)}}{\text{number of attempted false matches (B+D)}}$$

$$FNMR = \frac{\text{number of rejected genuine matches (C)}}{\text{number of attempted genuine matches (A+C)}}$$

	accept	reject
genuine attempt	A	C
false attempt	B	D

Biometric

- The matching algorithm typically makes decision based on some adjustable threshold. By adjusting the threshold, the FMR and FNMR can be adjusted.
- (lower threshold => more relax in accepting, higher threshold => more stringent in accepting).



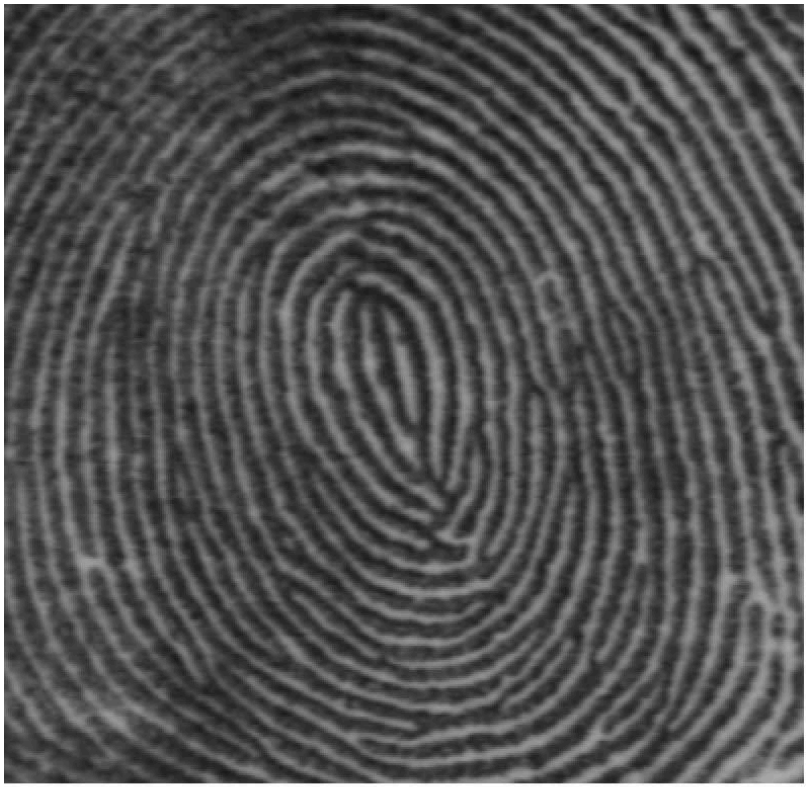
how to set the threshold? Depend on application.

Biometric

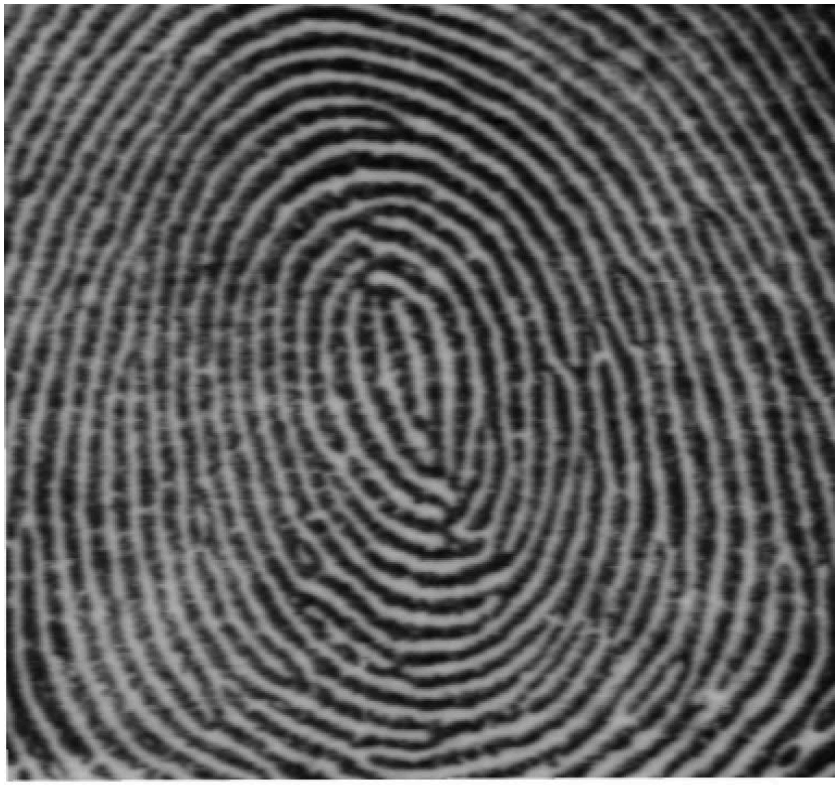
Other type of errors:

- ***Equal error rate (EER):*** Rate when FNMR = FMR.
- ***False-to-enroll rate (FER):*** Some users' biometric data can't be captured. For example due to injury.
- ***Failure-to-capture rate (FTC):*** An user's biometric data may fail to be captured during authentication, for example fingers are too dry, dirty, etc.

Example on Fingerprint



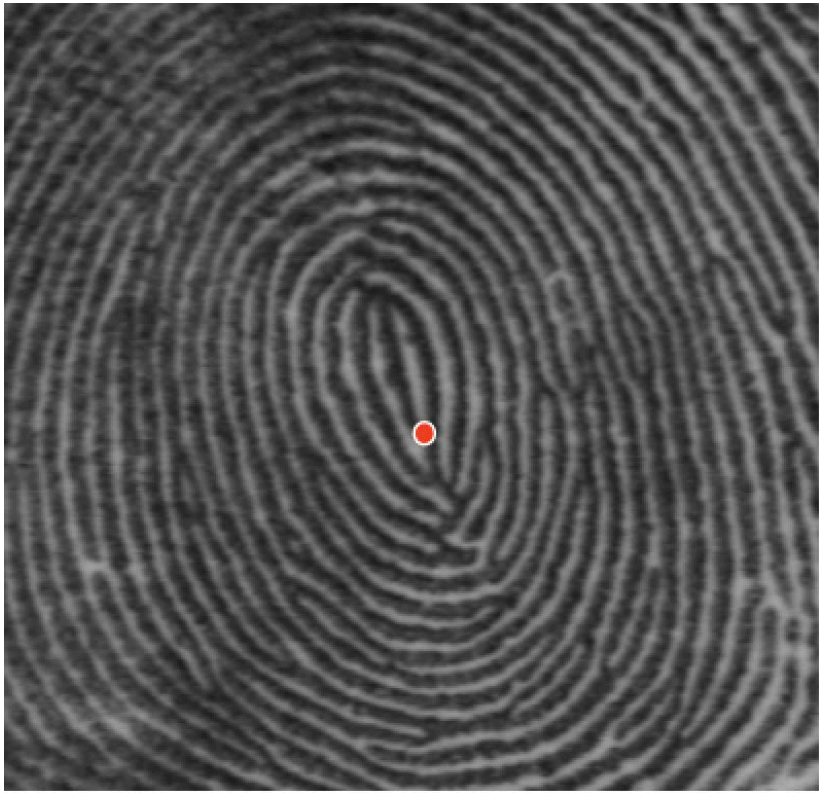
First scan of a finger

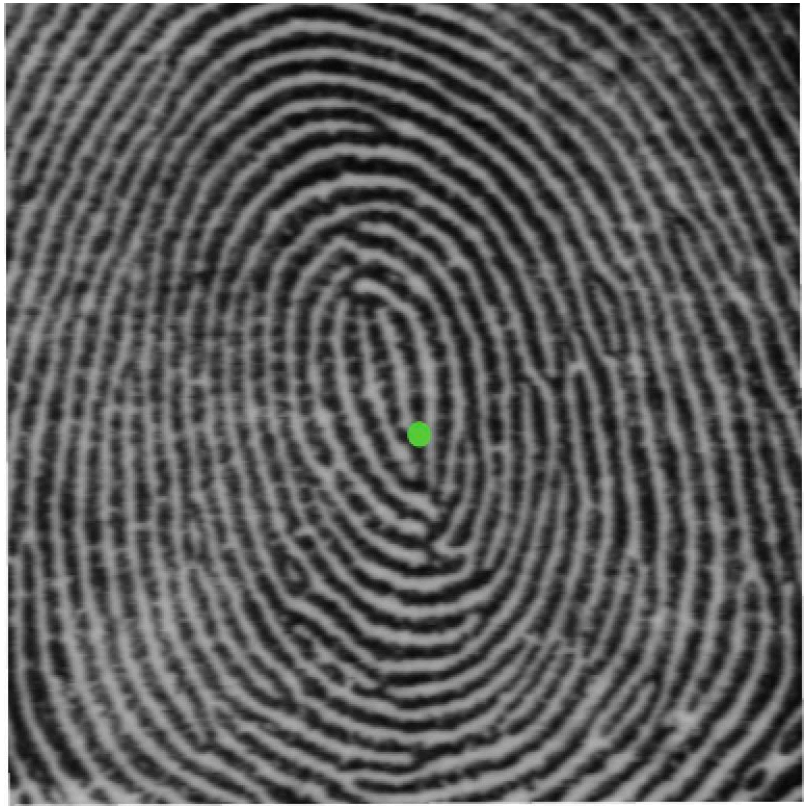


Another scan of the same finger

Example on Fingerprint

Background: Fingerprint

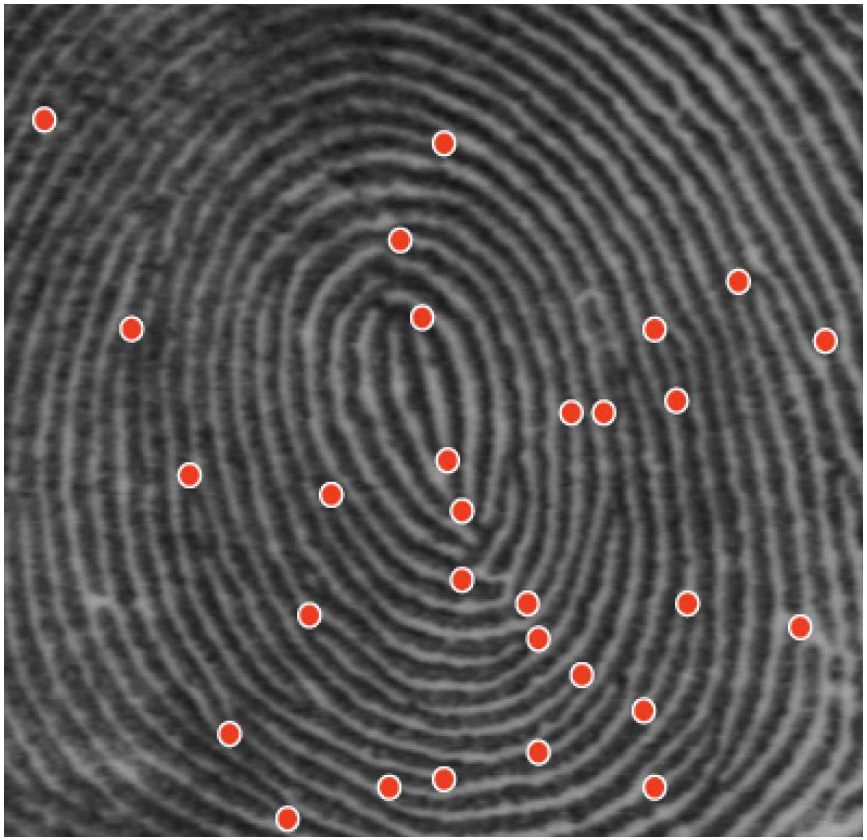


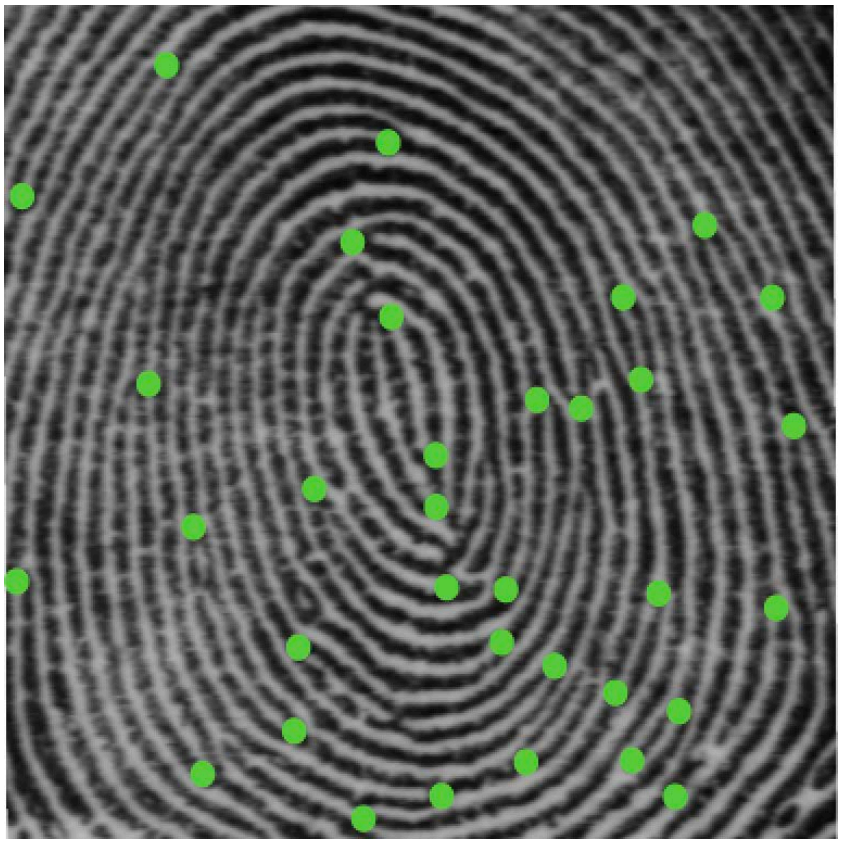


A feature point

Example on Fingerprint

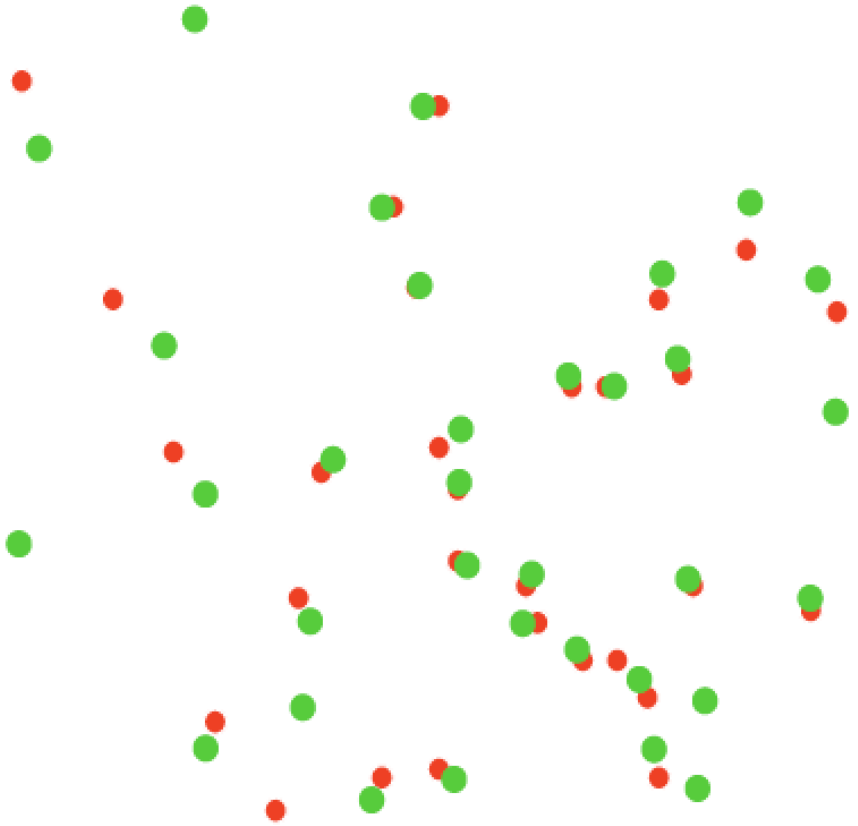
The set of feature points (known as minutiae for fingerprint).





Example on Fingerprint

- The features points extracted from the two scans are similar but not exactly the same.

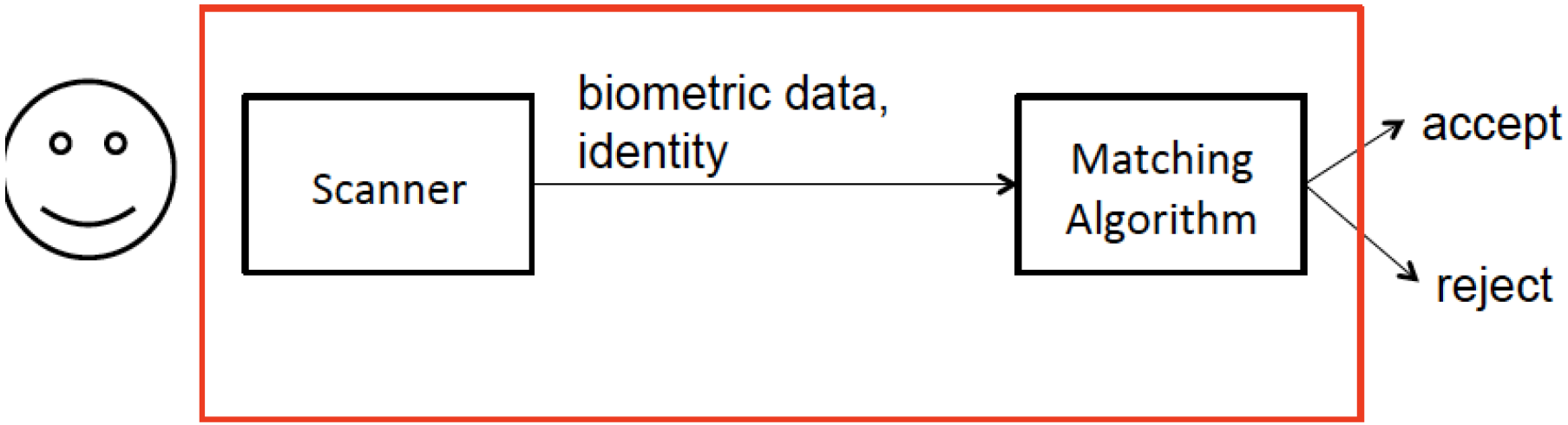


How good is fingerprint as a biometric?

- Performance depends on the quality of the scanner.
- EER can range from 0.5 to 5% depending on quality of scanners.
- see result of Fingerprint Verification Competition (FVC2006 http://bias.csr.unibo.it/fvc2006/default.asp)

Security of biometric system

- The scanner is assumed to be secured. That is, no tampering is possible.



- Yes, some biometric data could be spoofed as seen in movies.

see http://www.wikihow.com/Fake-Fingerprints on how to make a fake fingerprint. I haven't verified whether this would work.

Security of biometric system

- Some biometric systems include **liveness detection** to verify that the entity scanned by the scanner is indeed “live”, instead of spoofed materials, say a photograph.
- Example, temperature scanner in fingerprint scanner

Differences of biometric and passwords

Password	Biometric
Can be changed (revoked)	Can't
Need to remember	Don't have to
Zero non-matched rate	Error
Users can pass the password to another	Not possible

n-Factor Authentication (2FA)

- Require at least two different authentication “factors.”
- Three factors:
  - 1) Something you know: password, Pin.
  - 2) Something you have: security token, smart card, mobile phone, ATM card.
  - 3) Who you are: Biometric.
- Also known as 2-factor authentication (if 2 factors are used). A typical combination is (1) & (2).
- MAS (Monetary Authority of Singapore) expects all banks in Singapore to provide 2-factor authentication for e-banking.

n-Factor Authentication

Something you have

- Example: ATM card, mobile phone, OTP token.
- ***One Time Password token***: A hardware that generates one time password (i.e. password that can be used only once).
- ***Time-based***: Based on the shared secret and current time interval, a password K is generated. Now, both server and the user has a common password K.
- ***Sequence-based:*** An event (for e.g. user pressing the button) triggers the change of the password.

Example of 2FA: Password + SMS

Registration:

- User gives the server his mobile phone number and password.

Authentication:

(1) User sends password and username to server.

(2) Server verifies that the password is correct. Server sends aone-6me-password (OTP) to the user through SMS.

(3) User receives the SMS and enters the OTP.

(4) Server verifies that the OTP is correct.

Example of 2FA: Password + OTP Token

Registration:

The server issues a OTP token to the user. The token contains a "secret key" that the server knows. User sets a password.

Authentication:

(1) User "presses" the token. The token computes and displays a one-time-password.

(2) User sends password, username, and OTP to server.

(3) Since the server has the "secret key", the server can also compute the OTP. Server verifies that the OTP and password are correct.