Lecture 2: Authentication (Password)

2.1. Overview

2.2 Password (weak authentication)

- 2.2.1 Intercept the password while bootstrapping
- 2.2.2 Searching password (Dictionary, guessing, exhaustive)
- 2.2.3 Stealing of password
- 2.2.4 Preventive measure
- 2.2.5 Example on ATM
- 2.2.6 Password Reset: Security Questions

2.3 Biometric

2.4 Multi-factor authentication

- 2.4.1: Case studies: Sms vs Token (tutorial)

(in fact, Lecture 2,3,4 are on authenticity)

2.1 Overview

See [PF2.1] excluding Federated Identity Management, [Gollman] also has good coverage on Password (Chapter 4.1 to 4.5)

STATE OF HAWAII

CERTIFICATE OF LIVE BIRTH

FILE NUMBER 151

DEPARTMENT OF HEALTH 61 10641

1a. Child's First Name (Type or print): BARACK
1b. Middle Name: HUSSEIN
1c. Last Name: OBAMA, II

2. Sex: Male
3. This Birth: Single [X] Twin [ ] Triplet [ ]
4. If Twin or Triplet, Was Child Born: 1st [ ] 2nd [ ] 3rd [ ]
5a. Birth Date: Month August Day 4, Year 1961
5b. Hour: 7:24 P.M.

6a. Place of Birth: City, Town or Rural Location: Honolulu
6b. Island: Oahu
6c. Name of Hospital or Institution (If not in hospital or institution, give street address): Kapiolani Maternity & Gynecological Hospital
6d. Is Place of Birth Inside City or Town Limits? If no, give judicial district: Yes [X] No [ ]

7a. Usual Residence of Mother: City, Town or Rural Location: Honolulu
7b. Island: Oahu
7c. County and State or Foreign Country: Honolulu, Hawaii
7d. Street Address: 6085 Kalanianaole Highway
7e. Is Residence Inside City or Town Limits? If no, give judicial district: Yes [X] No [ ]
7f. Mother's Mailing Address
7g. Is Residence on a Farm or Plantation? Yes [ ] No [X]

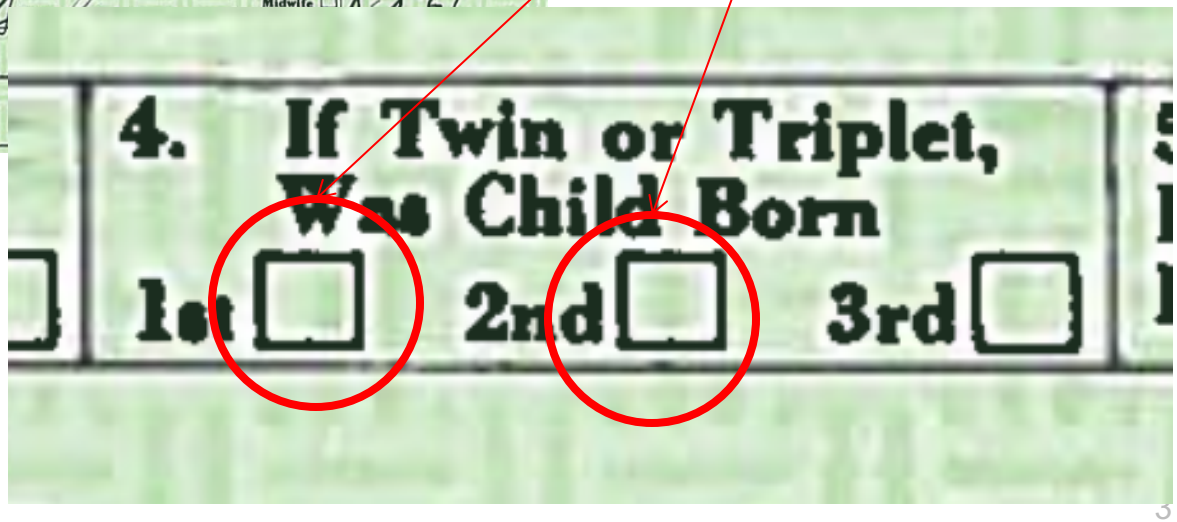
8. Full Name of Father: BARACK HUSSEIN OBAMA
9. Race of Father: African
10. Age of Father: 25
11. Birthplace (Island, State or Foreign Country): Kenya, East Africa
12a. Usual Occupation: Student
12b. Kind of Business or Industry: University
13. Full Maiden Name of Mother: STANLEY ANN DUNHAM
14. Race of Mother: Caucasian
15. Age of Mother: 18
16. Birthplace (Island, State or Foreign Country): Wichita, Kansas
17a. Type of Occupation Outside Home During Pregnancy: None
17b. Date Last Worked

I certify that the above stated information is true and correct to the best of my knowledge.
18a. Signature of Parent or Other Informant: Stanley Ann Dunham Obama — Parent [✓] Other [ ]
18b. Date of Signature: 8-7-61

I hereby certify that this child was born alive on the date and hour stated above.
19a. Signature of Attendant: David A. [illegible] — M.D. [ ] D.O. [ ] Midwife [ ]
19b. Date of Signature: 8-8-61

20. Date Accepted by Local Reg.: AUG -8 1961
21. Signature of Local Registrar: [illegible]

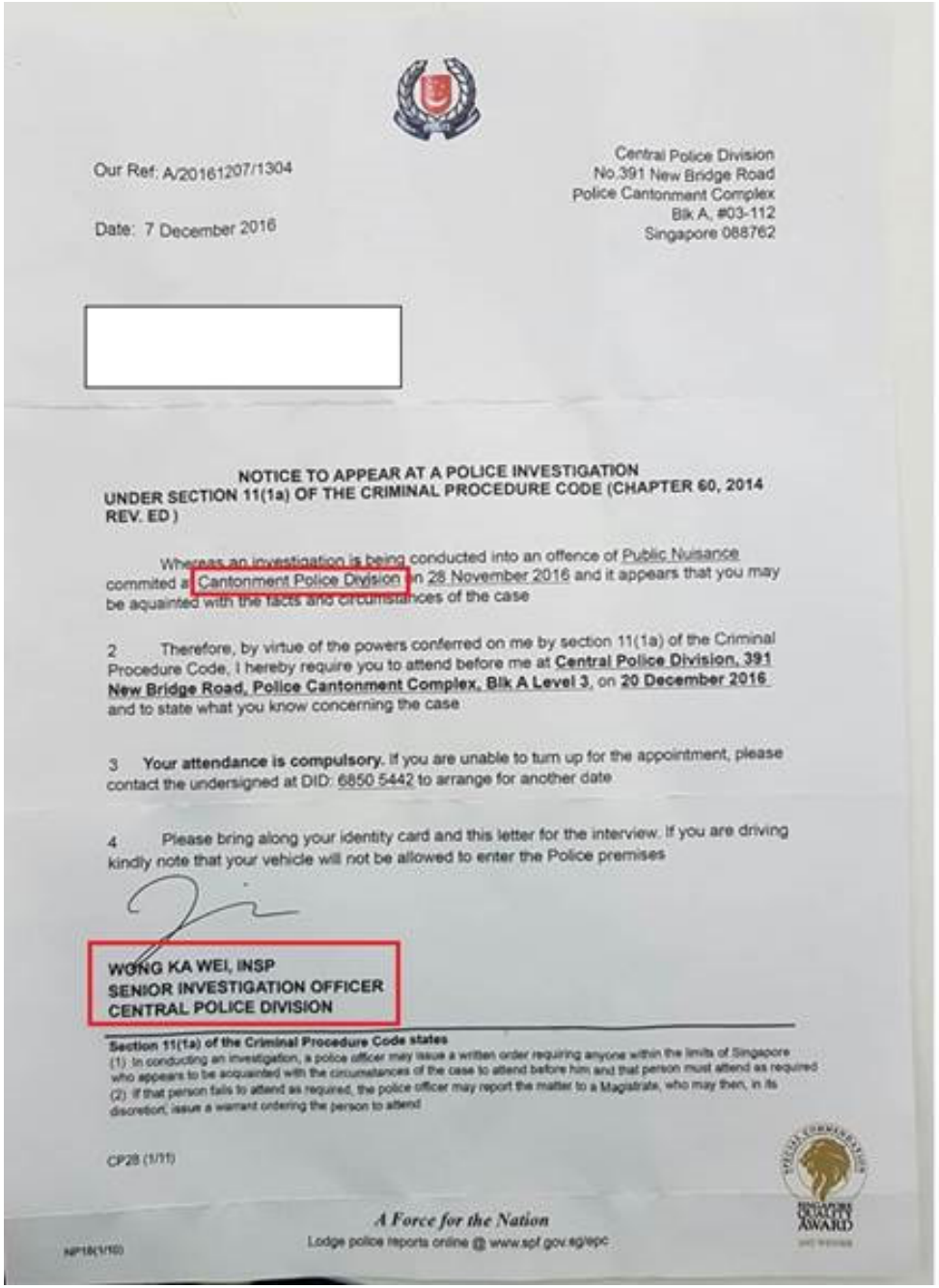
23. Evidence for Delayed Filing or Alteration



Is this letter Authentic?

From:
https://www.police.gov.sg/news-and-publications/media-releases/20161217_others_advisory_spf_letters,

December 16, 2016



Our Ref: A/20161207/1304

Date: 7 December 2016

Central Police Division
No.391 New Bridge Road
Police Cantonment Complex
Blk A, #03-112
Singapore 088762

NOTICE TO APPEAR AT A POLICE INVESTIGATION UNDER SECTION 11(1a) OF THE CRIMINAL PROCEDURE CODE (CHAPTER 60, 2014 REV. ED)

Whereas an investigation is being conducted into an offence of Public Nuisance commited at Cantonment Police Division on 28 November 2016 and it appears that you may be aquainted with the facts and circumstances of the case

2 Therefore, by virtue of the powers conferred on me by section 11(1a) of the Criminal Procedure Code, I hereby require you to attend before me at **Central Police Division, 391 New Bridge Road, Police Cantonment Complex, Blk A Level 3**, on **20 December 2016** and to state what you know concerning the case

3 **Your attendance is compulsory.** If you are unable to turn up for the appointment, please contact the undersigned at DID: 6850 5442 to arrange for another date

4 Please bring along your identity card and this letter for the interview. If you are driving kindly note that your vehicle will not be allowed to enter the Police premises

WONG KA WEI, INSP
SENIOR INVESTIGATION OFFICER
CENTRAL POLICE DIVISION

Section 11(1a) of the Criminal Procedure Code states
(1) In conducting an investigation, a police officer may issue a written order requiring anyone within the limits of Singapore who appears to be acquainted with the circumstances of the case to attend before him and that person must attend as required
(2) If that person fails to attend as required, the police officer may report the matter to a Magistrate, who may then, in its discretion, issue a warrant ordering the person to attend

CP28 (1/11)

A Force for the Nation
Lodge police reports online @ www.spf.gov.sg/epc

Authentication

Authentication: The process of assuring that the communicating entity, or origin of a piece of information, is the one that it claims to be.

Authentic (adjective): the claimed origin/entity is assured by supporting evidences.

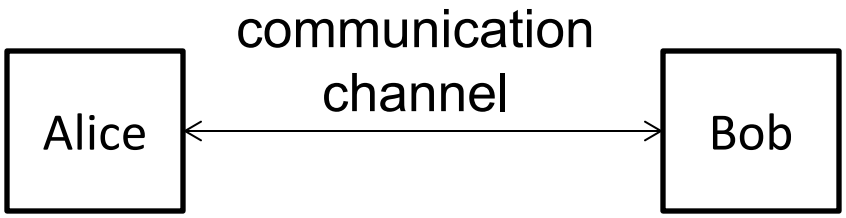
Authenticity: condition of being authentic.

Authenticity implies integrity.

(again, some documents use the term “integrity” to mean authenticity, and some claimed that we can’t compare authenticity with integrity. When reading a document, pay attentions to the context and the applications involved.)

Example

Communication Channel:



- Alice received a phone call, which claimed to be from the police department and asked for information regarding her brother. Authentic?
- Alice logged-in to "Luminus". Alice wondered, was the server indeed the authentic "Luminus"? Conversely, the Luminus's server might wonder whether the entity logged in is the authentic "Alice"?
- Alice tried to connect to wifi using her phone while in NUH's bus-stop. Among the available wifi Network Name (SSID), an item "NUS" is listed. Alice connected and keyed in her userid and password. Is that wifi access point authentic?

Example

Data-origin authentication:

Bob submitted a medical certificate to the lecturer, indicating that he was unfit for exam. Was the certificate authentic, i.e. was it issued by the clinic? Had Bob altered the date?

Is the birth certificate released by White House authentic? (i.e. issued by the claimed Local Registrar)

Alice downloaded an apps, say DBSPaylah, from some apps store. Is the app authentic? (i.e. from DBS?)

Authentication

The above two examples illustrate two types of information.

- *Entity authentication.*
  - For connection-oriented communication
  - Verifying authenticity of *entities* involved in a connection
  - Mechanisms: password, challenge and response, cryptographic protocol

- *Data-origin authentication*:
  - For connection*less* communication
  - Verifying the origin of a piece of information
  - Mechanisms: Crypto primitives such as MAC or digital signature. (Forensic can also be viewed as a verification mechanism. This is not covered in this module)

2.2 Password

Password system for authentication

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.

The server authenticates an entity. If the entity gives the correct password corresponds to the claimed identity, the entity is deemed as authentic.

Password is a secret, only the authentic user and the server know it. The identity is not necessary to be kept secret. The fact that an entity knows the password implies that the entity is either the server or the authentic user.

The identity could be: username in computer system, bank account number, customer id, etc.

(Question: Describe a password system where no identity is involved, i.e., just password.)

Stage 1: Bootstrapping

- The password is to be established during bootstrapping.

- This can be done by

1) The server/user chooses a password and sends it to the user/server through another communication channel.

2) Default password.

Question: Describe some bootstrapping mechanisms that you have encountered. (NUSNET, Singpass, wifi router)

What is WPS (Wi-Fi Protected Setup)? Why a physical button is required?

https://www.digitalcitizen.life/simple-questions-what-wps-wi-fi-protected-setup

Stage 2: Password Authentication

- Protocol.

  User $\rightarrow$ Server: My name is ***Alice***

  Server $\rightarrow$ User : What is your password

  User $\rightarrow$ Server: ***OpenSesame***

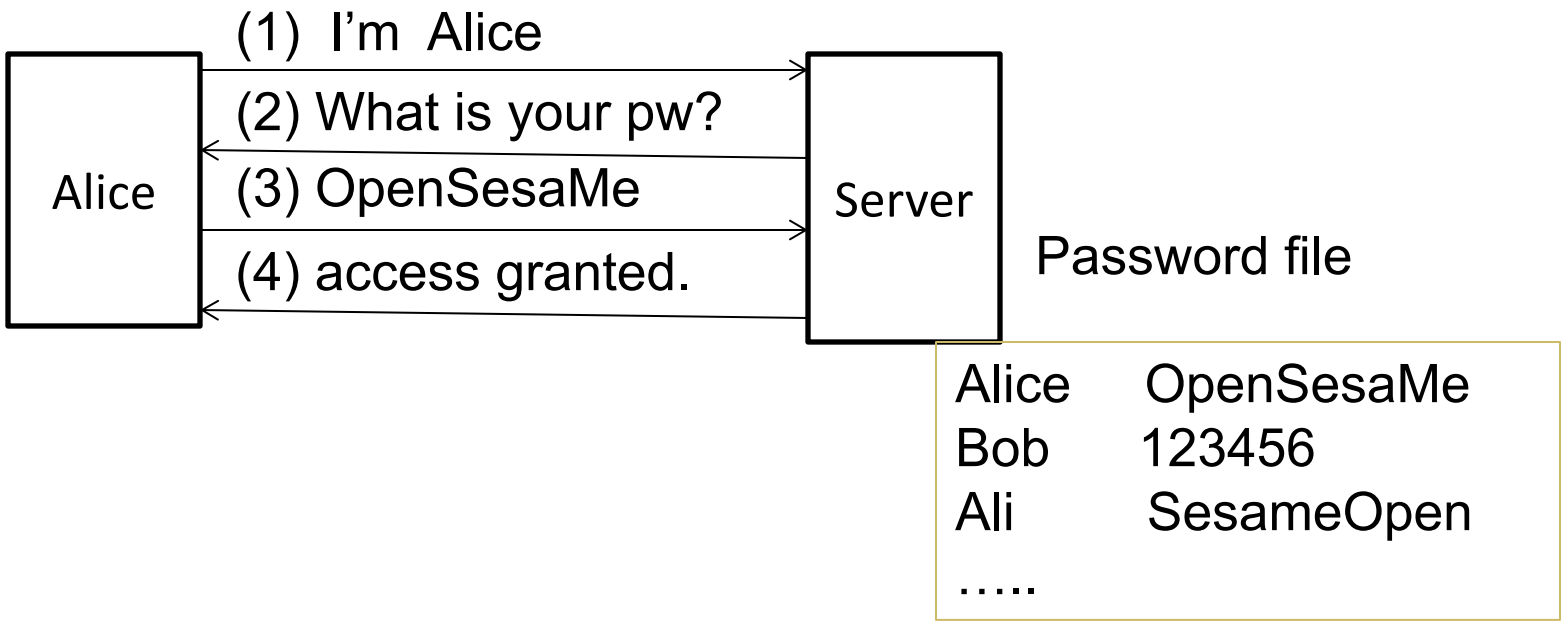
  Server verifies whether password is correct and takes corresponding subsequent actions.

- Alternatively, authentication can be carried out without interactions:

User sends a sms to a server:

Userid: ***Alice@nus.edu.sg.*** Password:***OpenSesame***. Instructions: Unsubscribe from your mailing list. No more junk mail.

Password file



Weak authentication system and Replay attack

- Password system is classified as a "***weak authentication***" system. A weak authentication is one that subjected to the simple "***replay attack***": information sniffed from the communicated channel can be replayed to impersonate the user.

- (under "*strong authentication*", information sniffed during the process can't be used to impersonate the user (to be covered later).)

Question: Terminologies. What are "***Sniff***", "***Spoof***"?

Attacks on password system

- Attack the bootstrapping.
- Search for the correct password (two settings: online vs offline)
  - Guessing
  - Dictionary attacks
  - Exhaustive attacks
- Steal the password:
  - Eavesdropping: sniff the network, key-logger.
  - Phishing
  - Spear-phishing
  - Spoofing login screen
  - Password Caching
  - Insider attacks

- 2.2.1 Attack the Bootstrapping

Attacker may intercept the password during bootstrapping. For example, if the password is sent through postal mail, an attacker could steal the mail to get the password.

Attacker uses the “default” passwords. There are many reported incidents on this simple attack.

(for e.g. IP camera, Wifi router)

see http://www.pcworld.com/article/2033821/widely-used-wireless-ip-cameras-open-to-hijacking-over-the-internet-researchers-say.html

Read (Mirari attack, Sep 2016)

http://www.computerworld.com/article/3134097/security/chinese-firm-admits-its-hacked-products-were-behind-fridays-ddos-attack.html

Default Password on IP Camera

Question: ([Gollmann] Pg 64)

You are shipping WLAN access points. Access to these devices is protected by password. What are the implications of shipping all access points with the same default password? What are the implications of shipping each access point with its individual password?

(hint: argue from the viewpoint of usability vs security)

Current practice: ship with the default password (or none), and require the user to change password after first login.

- 2.2.2 Searching for the Password

[PF2.1] Guessing the password from social information

The attacker gathers some social information about the user, and infer the password, e.g. mobile phone number.

Dictionary attacks

- The attacker tries different passwords during login sessions. The attacker can employ exhaustive search, i.e. tries all combinations.
- The attacker can restrict the search space to a large collection of probable passwords. The collection can include words from English dictionary, known compromised passwords, other language dictionaries, etc. This is known as ***Dictionary attack.***
- It is possible to carried out exhaustive search together with the dictionary. For e.g. tries all combinations of 2 words from the dictionary, exhaustively try all possible capitalizations of each word, substituting "a" by "@", etc

see list of "2014 worst password" reported by SplashData
http://www.prweb.com/releases/2015/01/prweb12456779.htm

Question: Download a password dictionary. Is your password in the dictionary?

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)

Dictionary attacks

Two scenarios in dictionary attacks (there is a crucial implication on the defense mechanisms, to be discussed later.):

- ***Online dictionary*** *attack*: an attacker must interact with the authentication system during the searching process.

  In other words, attacker must be online. (e.g. choose a password and ask the system (oracle) whether it is authentic)

- ***Offline dictionary*** *attack*: There are two phases.
  1. The attacker obtains some information ***D*** about the password from the authentication system, possibly via some interactions. (e.g. steal the password file, or sniffs from interactions)
  2. Next, the attacker carries out searching using ***D*** without interacting with the system.

2.2.3 Stealing the password

1. Sniffing

- ***Shoulder surfing***: This is the look-over-the-shoulder attack.

- ***Sniffing*** the communication: Some systems simply send the password over the public network in clear (i.e. not encrypted). E.g. FTP, Telnet, HTTP. (secure version sftp, ssh)

Other methods:

- ***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.

(L. Zhuang, F. Zhou, J.D. Tygar, Keyboard Acoustic Emanations Revisited, 2005. http://www.cs.berkeley.edu/~tygar/papers/Keyboard_Acoustic_Emanations_Revisited/ccs.pdf)

Question: Terminologies. What is ***"side channel attack"*** ?

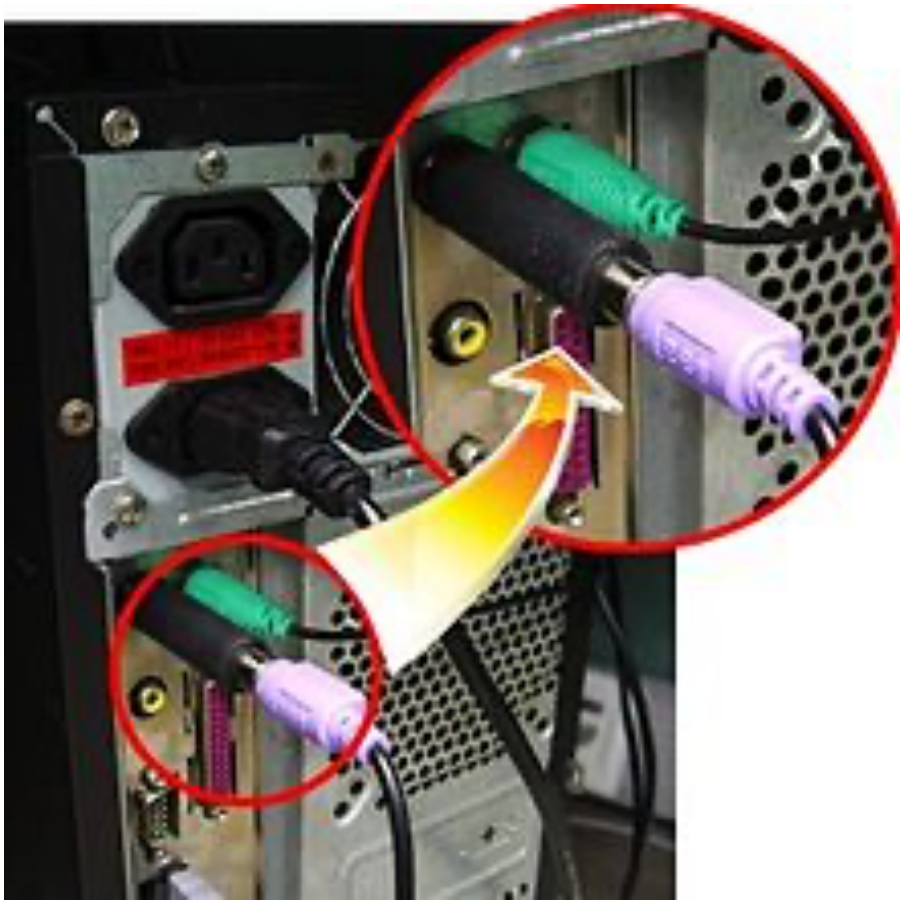
Viruses, Keylogger.

A key-logger captures/records the keystrokes, and sends the information back to the attacker via a “covert channel”.

- (software) Some computer viruses are designed as a ***key-logger***.

- (hardware) Hardware key-logger: the image in the next slide is self-explanatory.

see “Hardware-based keyloggers” in http://en.wikipedia.org/wiki/Keystroke_logging



from http://en.wikipedia.org/wiki/Keystroke_logging

Question: Terminologies. What is a covert channel?

2. Login spoofing

Attacker displays a “spoofed” login screen.

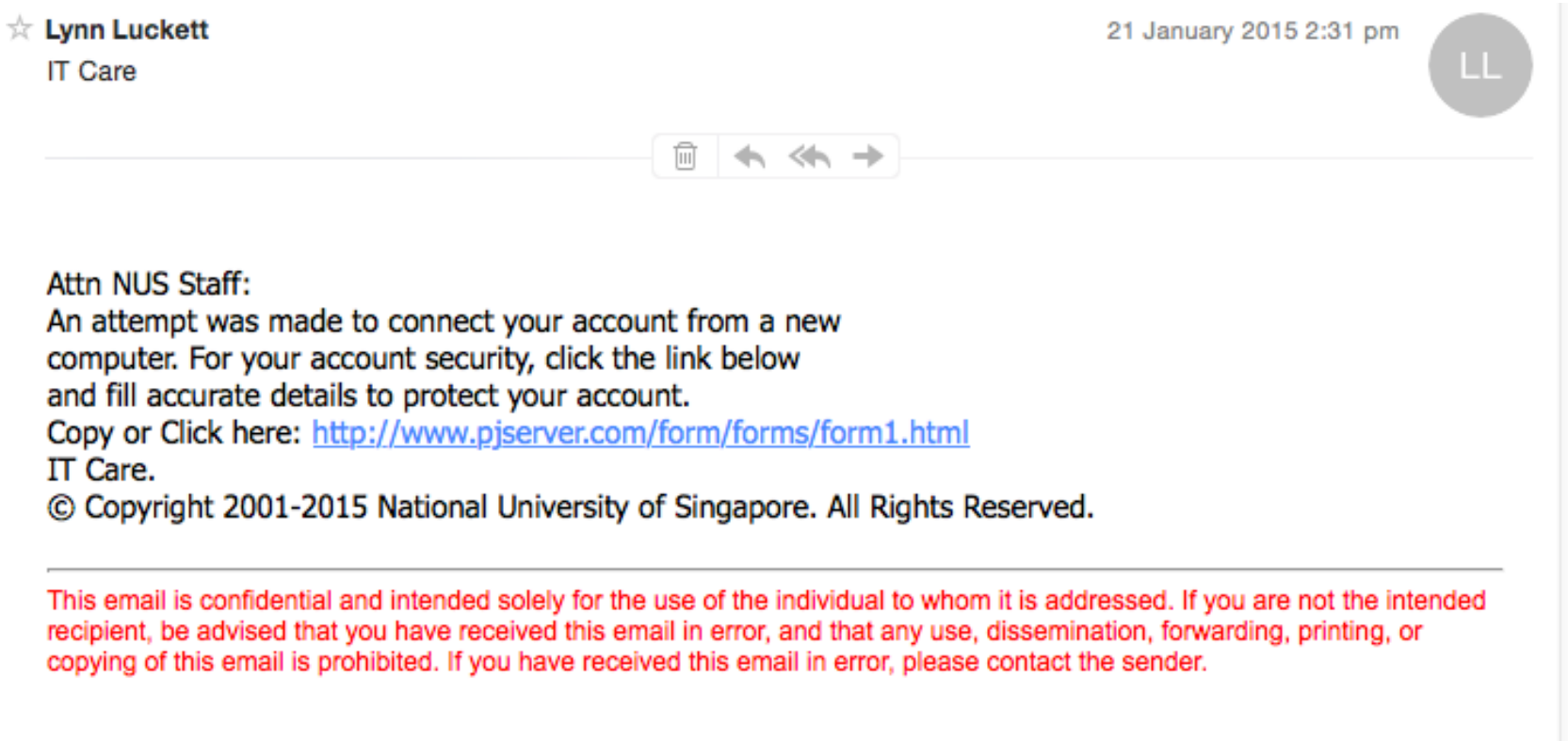
Prevention: Some systems have a ***secure attention key*** or ***secure attention sequence***. When they are pressed, the system starts the trusted login processing.

(e.g. Ctrl+Alt+Del for Window NT)

3. Phishing

- Same as login spoofing, here, the user is tricked to voluntarily sends the password to the attacker.

- Phishing attacks ask for password under some false pretense. For example:



☆ **Lynn Luckett** 21 January 2015 2:31 pm

IT Care

LL

Attn NUS Staff:
An attempt was made to connect your account from a new computer. For your account security, click the link below and fill accurate details to protect your account.
Copy or Click here: http://www.pjserver.com/form/forms/form1.html
IT Care.
© Copyright 2001-2015 National University of Singapore. All Rights Reserved.

Phishing attack is a ***social engineering*** attack.

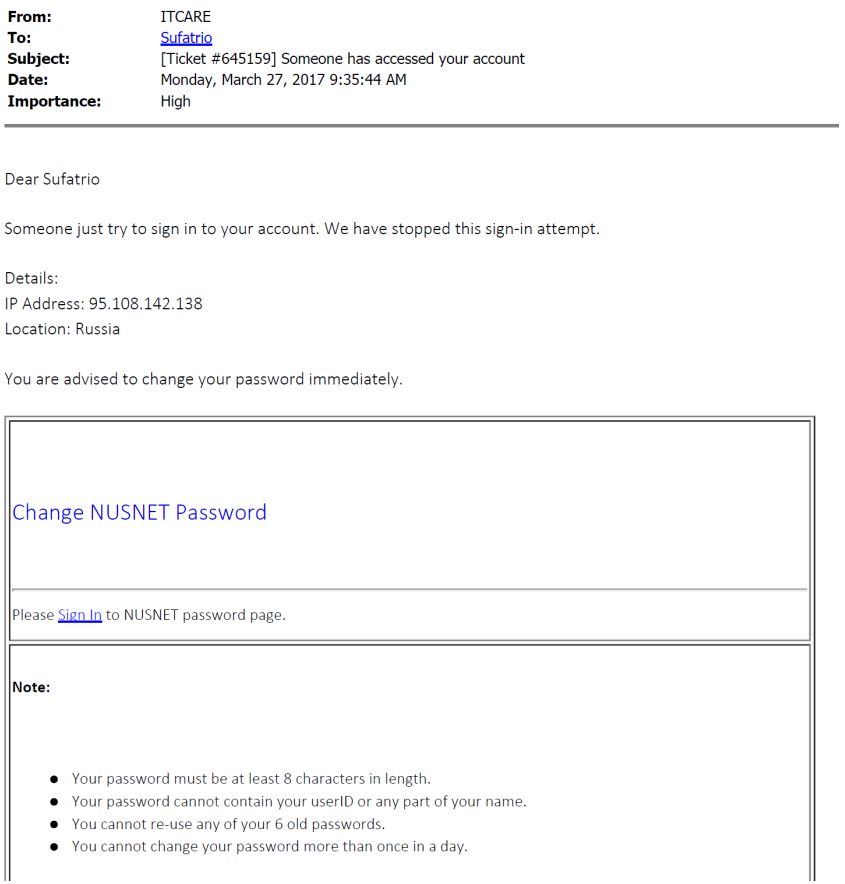
Wiki definition of social engineering:

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

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

4. Spear Phishing

Phishing can be targeted to a particular small group of users (for example, NUS staff in the above example). Such attack is generally known as ***spear phishing***, which is an example of ***targeted attacks***.



From: ITCARE
To: Sufatrio
Subject: [Ticket #645159] Someone has accessed your account
Date: Monday, March 27, 2017 9:35:44 AM
Importance: High

Dear Sufatrio

Someone just try to sign in to your account. We have stopped this sign-in attempt.

Details:
IP Address: 95.108.142.138
Location: Russia

You are advised to change your password immediately.

Change NUSNET Password

Please Sign In to NUSNET password page.

Note:

- Your password must be at least 8 characters in length.
- Your password cannot contain your userID or any part of your name.
- You cannot re-use any of your 6 old passwords.
- You cannot change your password more than once in a day.

Spear-phishing is extremely effective

"Spear phishing is the number one infection vector employed by 71 percent of organized groups in 2017." *Internet Security Threat Report*, Symantec, Vol 23, 2018.

Read the paragraph on phishing.
https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

> organizations. Spearphishing is the number one infection vector, employed by 71 percent of organized groups in 2017. The use of zero days continues to fall out of favor. In fact, only 27 percent of the 140 targeted attack groups that Symantec tracks have been known to use zero-day vulnerabilities at any point in the past.

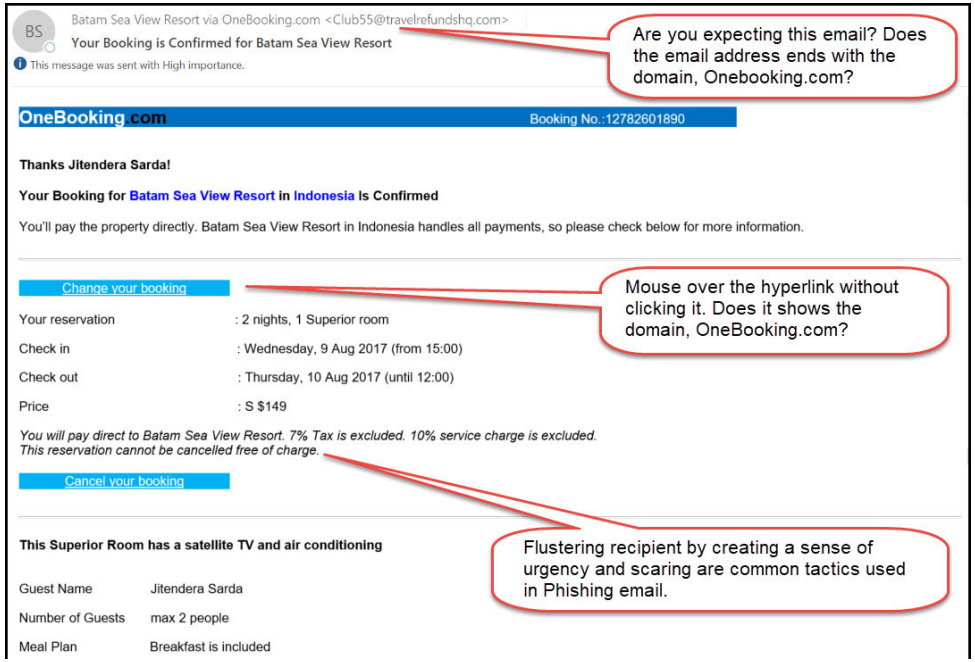
- Phishing of passwords is typically done through fake/spoofed website. They can also be carried out over phone calls.

Terminologies: ***Phishing***, ***Pharming***, ***Vishing*** and ***Smishing***.

See http://csbweb.com/phishing.htm)

Phishing Prevention

- User education



From: NUS IT Care

- Embedded Phishing Exercise:
  - Similar to fire drill, authorized entities send out "phishing" emails to employees. Effectiveness of such exercise not well studied.

Phishing Prevention

- Phishing repository site:
  - Example: phishtank.com (submit suspected phishes, track the status of your submissions, verify other users' submissions)

- Blocking. (with false positive and negative)

From: NUS IT Care

5. Cache

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

  (close the browser when using shared workstation)

6. 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.

2.2.4 Preventive measure

Using Strong Password

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

  3n5dcvUD9cfm (10 characters)

- User selection:

  - Mnemonic Method Pbmbval!
  - Altered Passphrases Dressed*2*tge*9z
  - Combining and Altering Word B@nkC@mera

(see **see** https://en.wikipedia.org/wiki/Password_strength#Guidelines_for_strong_passwords)

- Usability:

  - Strong passwords are difficult to remember.
  - It is difficult to enter alphanumeric passwords into mobile devices. There are alternatives, e.g. graphical or gesture-based.

remark: Pbmbval! is no longer a good choice since it had appeared as examples in many document on password selection.

$\log_2 (N)$

Entropy per symbol for different symbol sets

Symbol set	Symbol count *N*	Entropy per symbol *H*
Arabic numerals (0–9) (e.g. PIN)	10	3.322 bits
hexadecimal numerals (0–9, A–F) (e.g. WEP keys)	16	4.000 bits
Case insensitive Latin alphabet (a–z or A–Z)	26	4.700 bits
Case insensitive alphanumeric (a–z or A–Z, 0–9)	36	5.170 bits
Case sensitive Latin alphabet (a–z, A–Z)	52	5.700 bits
Case sensitive alphanumeric (a–z, A–Z, 0–9)	62	5.954 bits
All ASCII printable characters except space	94	6.555 bits
All ASCII printable characters	95	6.570 bits
All extended ASCII printable characters	218	7.768 bits
Binary (0–255 or 8 bits or 1 byte)	256	8.000 bits
Diceware word list	7776	12.925 bits

From https://en.wikipedia.org/wiki/Password_strength#Guidelines_for_strong_passwords

Guideline on Password strength (online vs offline)

see https://en.wikipedia.org/wiki/Password_strength#Guidelines_for_strong_passwords

- Note that typical human generated password of 10 alphanumeric characters do not have entropy of $10 \log_2(36)$. It is much less than that.

- NITS (**NIST Special Publication 800-63-2)** suggested an approach to estimate entropy of human-generated password. Read section on **NIST Special Publication 800-63-2** in https://en.wikipedia.org/wiki/Password_strength#Guidelines_for_strong_passwords**.** Note that 2017 revision of SP 800-63 (Revision 3) drops this approach.

- Recommendation by RFC 4086 (Randomness Required for Security) https://tools.ietf.org/html/rfc4086 suggests the password to have at least 29 bits of entropy to be secure against ***online attacks***.

- If cryptographic keys are to be generated from the password, and ***offline attacks*** are possible, then the password should have at least 128 bits of entropy, based on NITS recommendation of 128 bits for crypto keys (Actually, RFC 4086 recommends 96 bits for crypto applications, which in my opinion, is not sufficient.)

Online vs offline attack:

- **Online**: To check whether a password is correct, the attacker need to communicate with a server not under his control. E.g.
  - Attacker obtained a list of 1000 valid nusnet id. The attacker wants to find the password for some of them. The attacker write an automated script that attempt to login to LumiNUS using guessed passwords for each of these 1000 valid nusnet id.
  - Attacker obtained the list of 1000 valid nusnet id. The attack script attempts to login to NUS wifi router.

- **Offline**: To check whether a password is correct, the attacker can execute some algorithm without connecting to a server.
  - Attacker has an AES encrypted pdf file. The key is derived from a password. The attacker wants to find the password.
  - In some password authentication protocols, some “hash” of the password is sent in clear. The attacker first obtained the hash by eavesdropping a valid login session. Next, the attacker went offline and search for the password.

Remark: Password Entropy

- We often encounter this term "entropy" when quantifying strength of password. Entropy is a measurement of randomness. In this module we won't go into the definition of entropy. We can use the following example to have a sense of its meaning.

- Suppose a set ***P*** contains ***N*** unique passwords. Alice chooses her passwords by randomly & uniformly picking a password from the set ***P.*** Every password in ***P*** has an equal chance to be chosen (i.e. 1/N). In this case, by definition, the entropy of Alice's password is:

  (log_2 *N*) bits

- What if Alice doesn't choose the passwords uniformly, for e.g., the probability that she picks a word starting with letter "A" is higher than the probability that she picks a word starting with "z"? In such case, the entropy is not ($\log_2$ N). By the definition of entropy, it is

$$-\sum_{i=1}^{N} p_i \log_2 p_i$$

  where p_i is the probability that Alice picks the *i*-th word in ***P***. (if we put $p_i = 1/N$, then we get $\log_2 N$.)

- It can be shown that, for the entropy to be highest for a set of *N* itmes, p_i must be 1/*N*. In other words, uniform choices. So, to increase entropy, we can either make more uniform choices, or increase the size *N*.

- (omit if this further confuse you) Another way to measure randomness is min-entropy, which is

$$\min_i(-\log_2 p_i)$$

Suppose with probability 0.5, Alice picks her password as "Alice", and for probability 0.5, she uniformly chooses from ***P.*** That is, each word in P has probability 1/(2N) being chosen, and "Alice" has 0.5. Now, the entropy is roughly N/2, which is high. However, there is good chance in correctly guessed her password. So, entropy might not be a good measure of password strength. Note that in this case, the min-entropy is low and is 1, correctly reflects the poor choice. (here, the string "Alice" is not in ***P***)

Password Policy

- To make online dictionary attack more difficult, many systems intentionally add delay into login session, (for example, has to wait for 1 second before next attempt), or locked the account after a few failed attempts.

- System checks for weak password when user registers/changes password. (for e.g. using the password dictionary).

- Some systems require regular changes of passwords, which is controversial. (Many believe that frequent changes of passwords could lower security.)
  See https://www.schneier.com/blog/archives/2016/08/frequent_passwo.html

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

  (for e.g. the policy may state that the password must be at least 10 characters)

Additional protection to password files

- Recap: the *password file* stores userid and password
- The password file could be leaked, due to insider attack, accidental leakage, system being hacked, etc. Recap: the password file store the userid+password.
- There are many well-known incidents where unprotected or weakly protected password files are leaked, leading to a large number of passwords being compromised. (2012 Linkedin https://en.wikipedia.org/wiki/2012_LinkedIn_hack)
- Hence, it is desired to add an additional layer of protection to the password file. (not all files are equally important.)

(revisit this slide after hash is covered)

Passwords should be "hashed" and stored in the password files.

(textbook ([PF]pg 46) uses the term "encrypted". IMHO, this is a wrong choice of term. For encryption, by definition, there is a way to decrypt and get back the original password. For cryptographically secure hash, it is infeasible to recover the password from the hashed value. In fact, to be secure, we don't want to have a way to recover the password.)

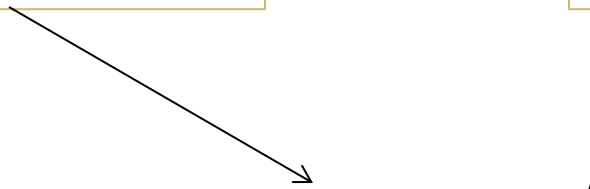
- During authentication, the password entered by the entity is being hashed, and compared with the the value stored in the password file.

Password in clear

Alice	OpenSesaMe
Bob	123456
Ali	SesameOpen
Charles	SesameOpen

Hashed Password

Alice	X3lad=3adfv
Bob	3Dv6usgawer
Ali	da5DGDSDFd3
Charles	da5DGDSDFd3



*Hashed, *not* encrypted.*

"da5DGDSDFd3"= Hash("SesameOpen")

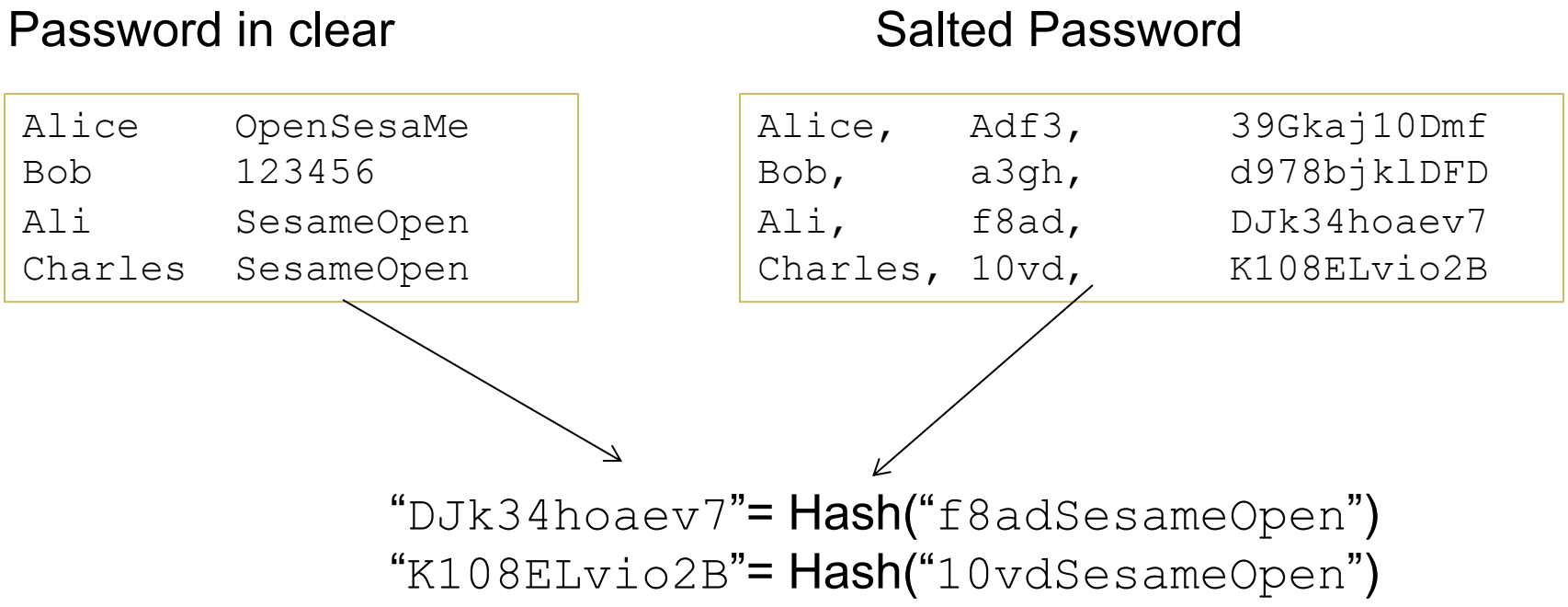
To verify whether a password ***P*** belongs to a user ***U***, the following are carried out:

1. Compute d = Hash (***P***).
2. If <***U***, d> is in the password file, then accept, else reject.

(revisit this slide after hash is covered)

It is desired that the same password would be hashed to two different values for two different userid. Why? (*rainbow table*)

This can be achieved using salt.



(Optional) How Facebook protects the passwords

PW-Onion(pw)

$h_1 \leftarrow \text{MD5}(pw)$

$sa \leftarrow^{\$} \{0,1\}^{160}$

$h_2 \leftarrow \text{HMAC[SHA-1]}(h_1, sa)$

$h_3 \leftarrow \text{PRF-Cl}(h_2) = \text{HMAC[SHA-256]}(h_2, msk)$

$h_4 \leftarrow \text{scrypt}(h_3, sa)$

$h_5 \leftarrow \text{HMAC[SHA-256]}(h_4)$

Ret (sa, h_5)

Figure 7: The Facebook password onion. PRF-Cl(h_2) invokes the Facebook PRF service HMAC[SHA-256](h_2, K_s) with PRF-service secret key K_s.

from A. Everspaugh et. al. The Pythia PRF Service, USENIX Security 2015

PRF-C1(h2) is computed by a remote server, using a master-key stored only in that server.

Q. What is scrypt?

2.2.5 Security Questions

read https://www.owasp.org/index.php/Choosing_and_Using_Security_Questions_Cheat_Sheet

optional:
Ariel Rabkin, *Personal knowledge questions for fallback authentication: security questions in the era of Facebook*, Usable privacy and security 2008.

Security-Cost-Usability tradeoff

- Security Questions can be viewed as a mechanism for ***fallback authentication***, or a ***self-service password reset***.
  - *Enhance **usability***: a user can still login even if password is lost.
  - *Reduce **cost***: reduces operating cost of helpdesk.
  - *Weaken **security***: attackers have another mean to obtain access.

see [PF2.1]page 39 SideBar 2-1 on a known incident.

Choices of Security Questions

from
https://www.owasp.org/index.php/Choosing_and_Using_Security_Questions_Cheat_Sheet

- ***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. For instance, asking "What is the name of your significant other?" may have a different answer 5 years from now.
- ***Nearly universal***: The security questions should apply to a wide audience of possible.
- ***Safe***: The answers to security questions should not be something that is easily guessed, or research (e.g., something that is matter of public record)

Other forms of self-service password reset

- There are many other forms of password reset.

- Next slide gives a negative example where the password reset was not designed/implemented properly.

Zoom's account hijacking

optional

https://www.tomsguide.com/news/zoom-security-privacy-woes

Zoom flaw allowed account hijacking

A Kurdish security researcher said Zoom paid him a bug bounty -- a reward for finding a serious flaw -- for finding how to hijack a Zoom account if the account holder's email address was known or guessed.

The researcher, who calls himself "s3c" but whose real name may be Yusuf Abdulla, said if he tried to log into Zoom with a Facebook account, Zoom would ask for the email address associated with that Facebook account. Then Zoom would open a new webpage notifying him that a confirmation email message had been sent to that email address.

The URL of the notification webpage would have a unique identification tag in the address bar. As an example that's much shorter than the real thing, let's say it's "zoom.com/signup/123456XYZ".

When s3c received and opened the confirmation email message sent by Zoom, he clicked on the confirmation button in the body of the message. This took him to yet another webpage that confirmed his email address was now associated with a new account. So far, so good.

But then s3c noticed that the unique identification tag in the Zoom confirmation webpage's URL was identical to the first ID tag. Let's use the example "zoom.com/confirmation/123456XYZ".

The matching ID tags, one used before confirmation and the other after confirmation, meant that s3c could have avoided receiving the confirmation email, and clicking on the confirmation button, altogether.

In fact, he could have entered ANY email address -- yours, mine or billgates@gmail.com -- into the original signup form. Then he could have copied the ID tag from the resulting Zoom notification page and pasted the ID tag into an already existing Zoom account-confirmation page.

Boom, he'd have access to any Zoom account created using the targeted email address.

"Even if you already linked your account with a Facebook account Zoom automatically unlink it and link it with the attacker Facebook account," s3c wrote in his imperfect English.

And because Zoom lets anyone using a company email address view all other users signed up with the same email domain, e.g. "company.com", s3c could have leveraged this method to steal ALL of a given company's Zoom accounts.

"So if an attacker create an account with email address attacker@companyname.com and verify it with this bug," s3c wrote, "the attacker can view all emails that created with *@companyname.com in Zoom app in Company contacts so that means the attacker can hack all accounts of the company."

Zoom is fortunate that s3c is one of the good guys and didn't disclose this flaw publicly before Zoom could fix it. But it's such a simple flaw that it's hard to imagine no one else noticed it before.

STATUS: Fixed, thank God.

Social engineering + password reset

optional

Is the following feasible? (I read something like this somewhere but can't remember the details. Let me know if you find the concrete example)

- Suppose an attacker already knew Bob's password of a social media platform XXXXX . Bob was in a group ABC in XXXXX.
- The attacker (using Bob's account) posted in the group ABC, mentioning that he received a phishing email who claimed to be from XXXXX, and the email showed an QR code. Bob posted the email with the QR code with some ha, ha and lol.
- Attacker went to XXXXX's site and attempted to reset ABC members' accounts, prompting XXXXX to automatically send confirmation emails to the members. The emails contained some info embedded in QRcode, and asked the members to scan the QRcode using XXXXX's apps.
- A friend in ABC replied to Bob's post "I also received this" and posted the QRcode.
- Attacker used the QRcode to confirm the password change.

2.2.6 Example on ATM

ATM Card

- To get authenticated, the user presents (1) a card, and (2) a PIN.
  - 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.
  - The PIN plays the role of password.

Data are encoded into the magnetic strip using well-known standards. Given access to a card, anyone (including attackers) can "copy" the card by reading the info from the card and writing it to the spoofed card.

this card can be purchased from ebay.

http://colnect.com/en/bank_cards/bank_card/4130-ATM_Card-Bank_of_America-United_States

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.

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

Yet another self-explanatory image

ATM SKIMMING

Synopsis:

Fictitious card reader and cellular telephone with a video camera attached to ATM machine. The fictitious card reader is flush to compromised ATM whereas the others are recessed. A façade of ATM colored molding is attached to upper part of ATM. The façade conceals a cellular phone camera which records the PIN number.

http://pbgcrimewatch.org/images/reports/ATM_Skimming.jpg

Some Fun Videos to Watch: POS Skimmer Installation

https://www.youtube.com/watch?v=_BFRD8_LrcM

CCTV caught someone deploying a Point-Of-Sale skimmer (similar to ATM skimmer)

More video:
"Why Chip Credit Cards Are Still Not Safe From Fraud"
https://www.youtube.com/watch?v=gJo9PfsplsY

Measures

- Anti-Skimmer device: A device that prevents external card reader to be attached onto the ATM.

Shielding the keypad.

- Awareness among users.

2.3 Biometric

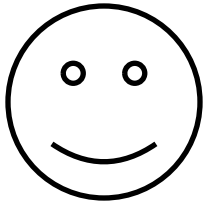
- Biometric uses unique physical characteristics of a person for authentication.

- During ***enrollment***, a ***template*** of an user's biometric data is captured and stored (same as bootstrapping in password system).

- 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.

Biometric can be used for *identification* (identify the person from a database of many persons), or *verification* (verify whether the person is the claimed person). Here, we focus on verification.

Enrollment

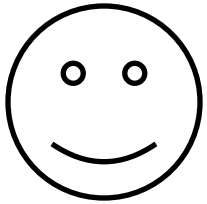


Scanner

biometric data

Database:
Alice, template1
Bob, template2

Verification (Authentication)



Scanner

biometric data,
identity

Matching
Algorithm

accept

reject

Differences between Biometric and Password

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

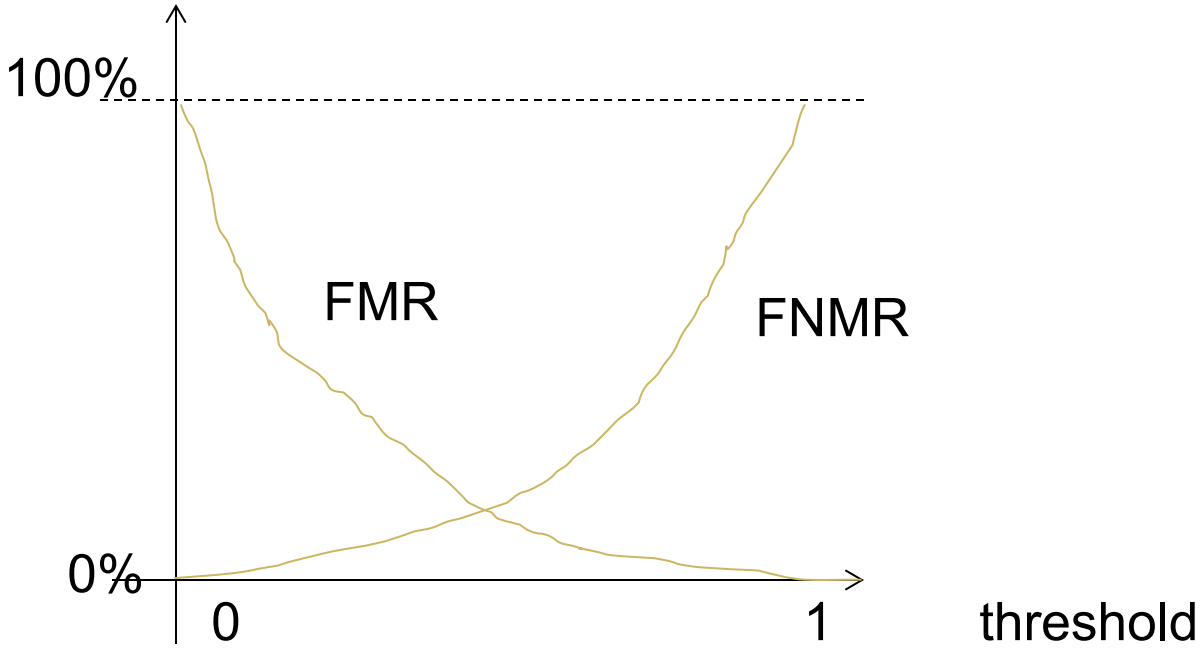
- Unlike password, there are inevitable noise in capturing the biometric data, leading to error in making the matching decision: FMR (False match rate) and FNMR (false non-match rate) .

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

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

	accept	reject
genuine attempt	A	C
false attempt	B	D

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.

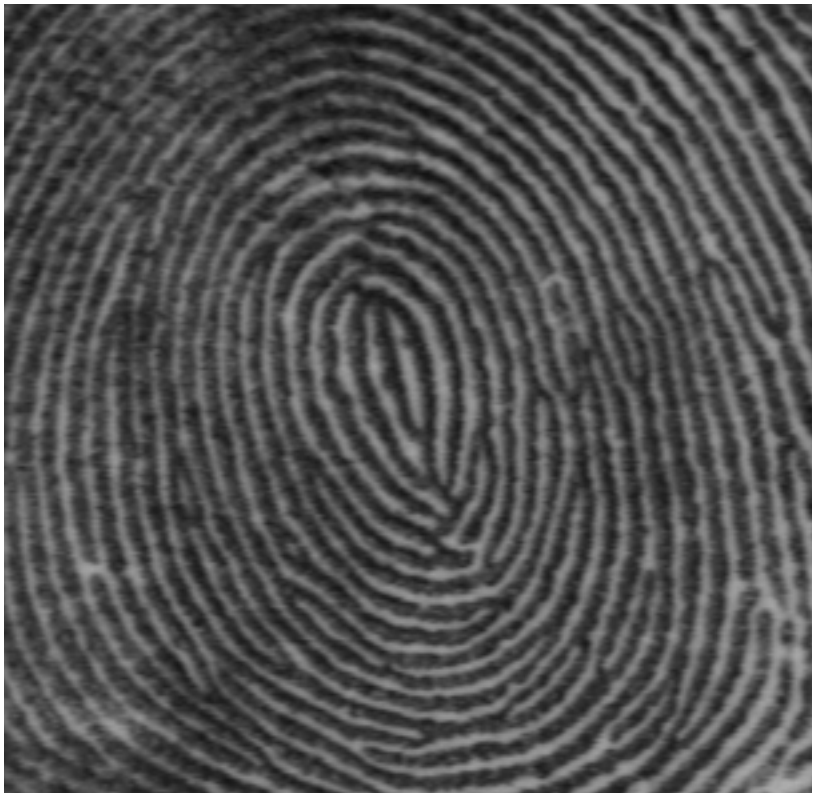
Other type of errors:

Equal error rate (EER): Rate when FNMR = FMR.

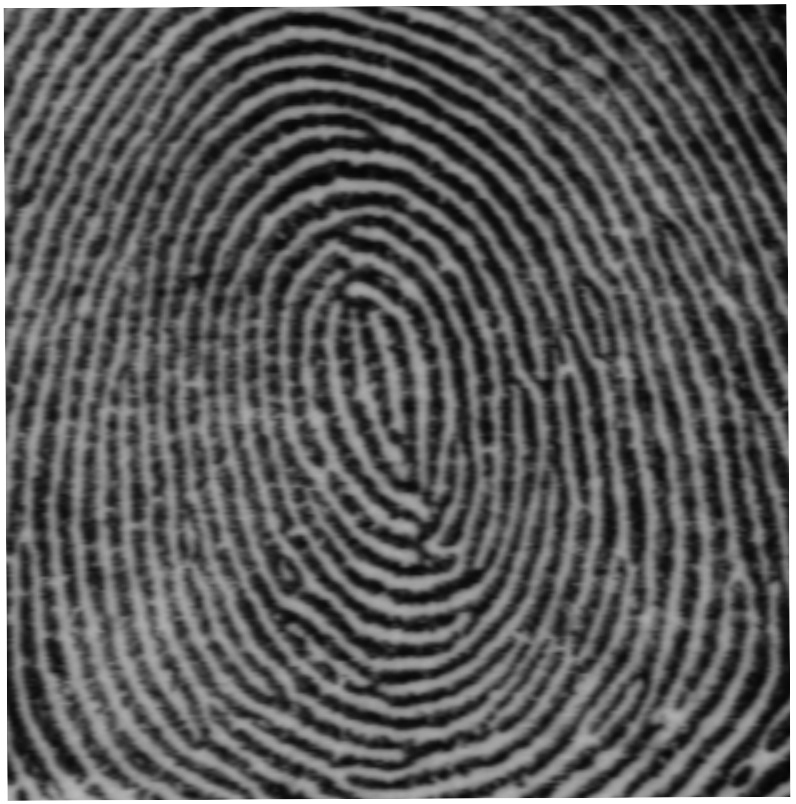
False-to-enroll rate (FER). Some users' biometric data can't be captured. For example due to injury.

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

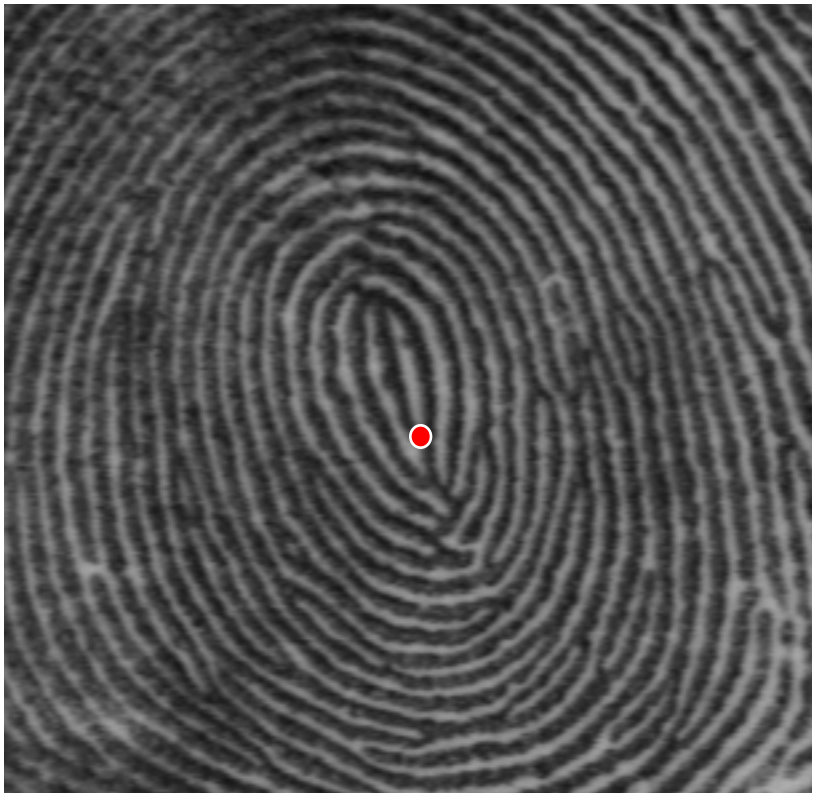


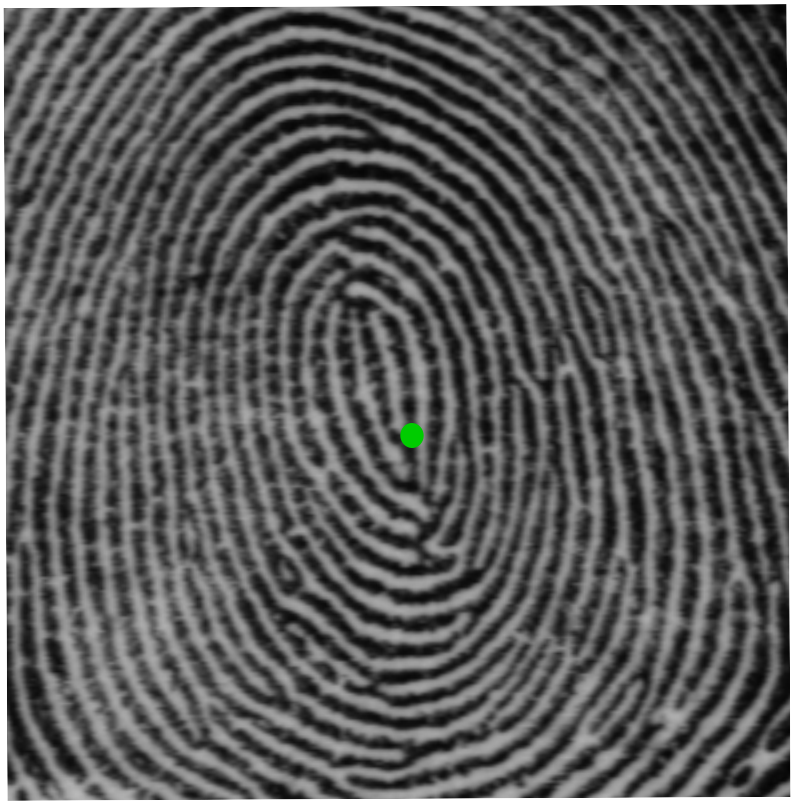
First scan of a
finger



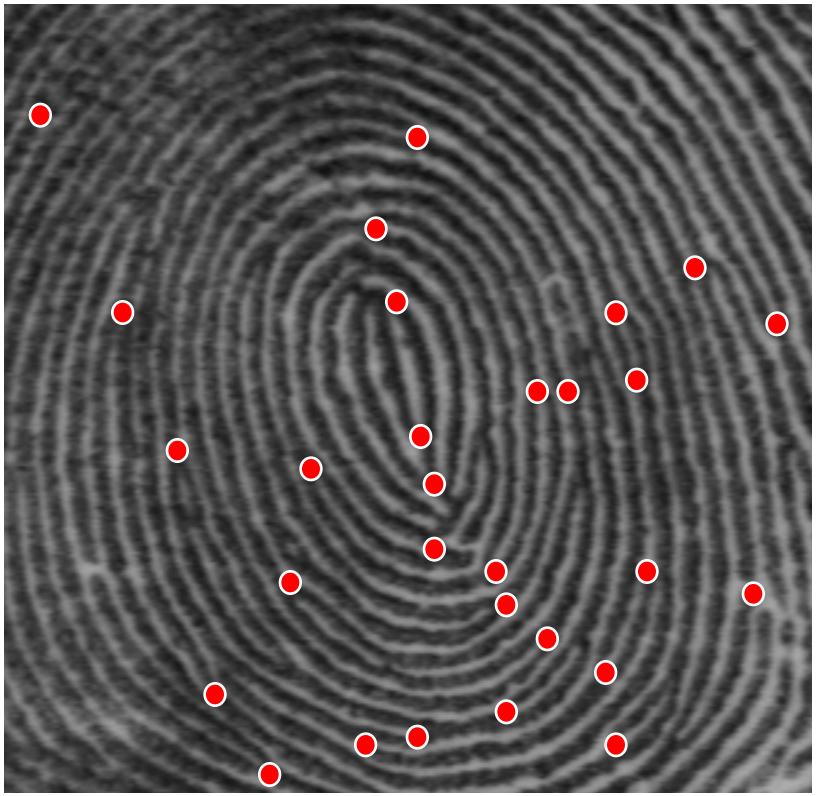
Another scan
of the same finger

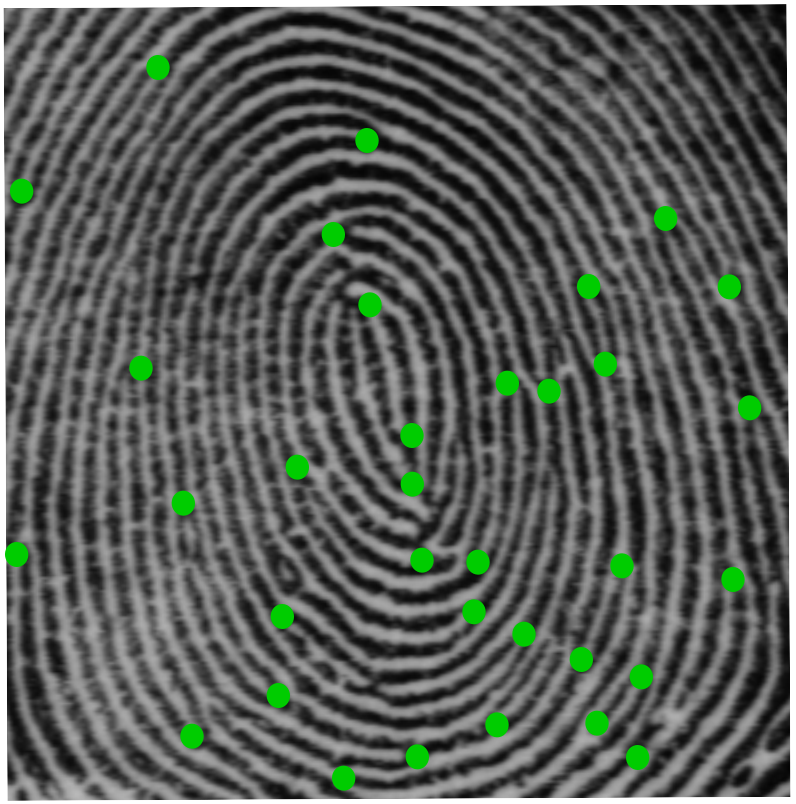
Background: Fingerprint





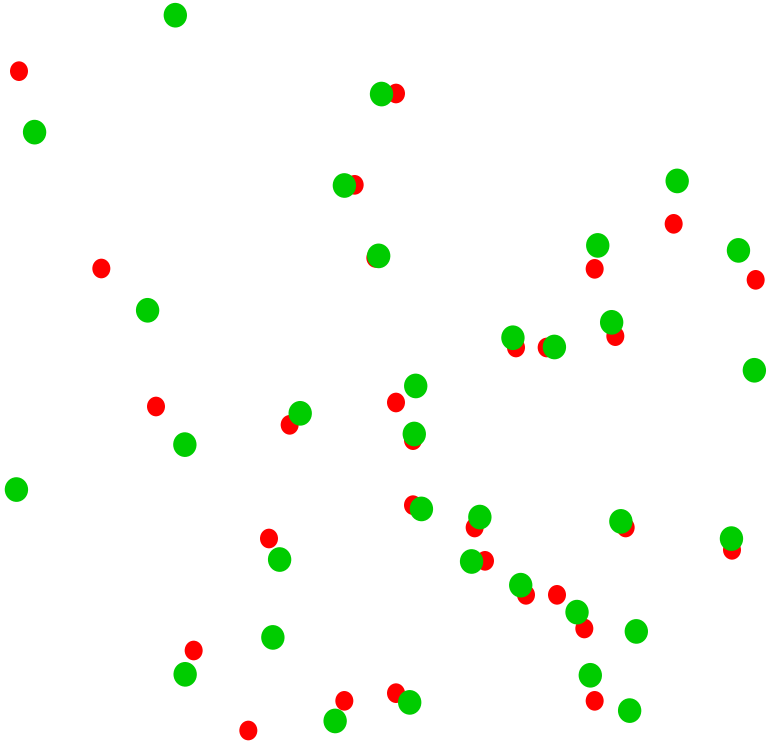
A feature point





The set of feature points
(known as *minutiae* for 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.

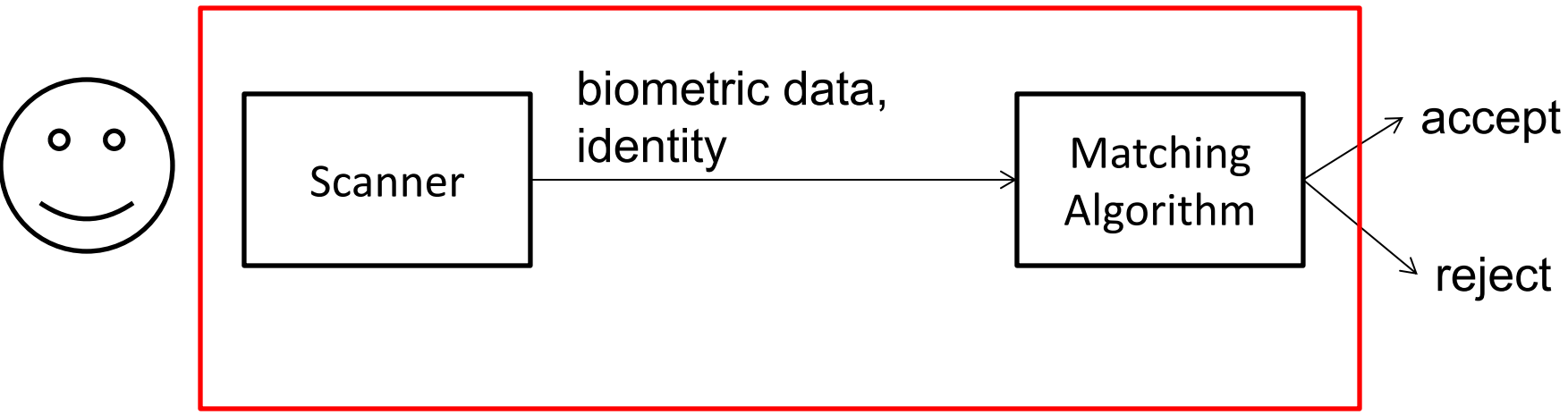
EER can range from 0.5 to 5% depending on quality of scanners.

see result of Fingerprint Verification Competition

FVC2006 http://bias.csr.unibo.it/fvc2006/default.asp

Security of biometric system

- The scanner has to be secure, that is, no tampering of the scanner is possible. (Mobile phones have some hardware+crypto protection to secure the scanner, so as to prevent the attacker, who has access to the phone, in bypassing or tempering the scanner).



- Some biometric data could be easily spoofed as seen in movies. see http://www.wikihow.com/Fake-Fingerprints on how to make a fake fingerprint.
- 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)

See [PF2.1] pg 65-70 (excluding Federated Identity Management)

2.4 *n*-Factor Authentication (2FA)

n-factor Authentication

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.

It is called an 2-factor authentication if 2 factors are employed.

MAS (Monetary Authority of Singapore) expects all banks in Singapore to provide 2-factor authentication for e-banking.

[Gollmann] listed 2 additional factors (what you do, where you are). Most literatures only listed the above 3.

MAS compliance checklist for Internet Banking and technology risk management guidelines, item 26.

http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/IBTRM%20Checklist.pdf

25.	4.3.5	Procedures and monitoring tools to track system performance, server processes, traffic volumes, transaction duration and capacity utilisation on a continual basis are put in place to ensure a high level of availability of internet banking services.	☐	☐	☐	☐
26.	4.4.2	Two-factor authentication at login for all types of internet banking systems and for authorising transactions is implemented.	☐	☐	☐	☐
27.	4.4.3	For high value transactions or for changes to sensitive customer data (e.g., customer office	☐	☐	☐	☐

Something you have

Examples: 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). Each token and the server share some secrets. There are two types:

1. **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.***

2. **Sequence-based:** An event (for e.g. user pressing the button) triggers the change of the password.

Note: Not to be confused with "one-time pad"

Example of 2FA (1): Password + Mobile phone(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 a one-time-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 (2): Password + OTP Token

Registration:

The server issues a hardware OTP token to the user. The token contains a "secret key" ***k*** that the server knows. User registers a password.

Authentication:

(1) User "presses" the token. The token generates (can be time-based or sequence-based) 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.

Question: some OTP includes a keypad for user to enter values. Give a scenario that such OTP can provide more security. (i.e. give a setting and attack that OTP+keypad can prevent but not the original version of OTP)

Soft Token

- Mobile phone with a secret key can takes the role of "hardware token". This is also known as "Soft Token".

- (What if the user carries out banking transaction on the same mobile phone which is the soft token. Do we have still have 2-factor?)

Example of 2FA (3): smartcard + fingerprint (Door access system)

Registration:

The server issues a smartcard to the user (note that the smartcard contain a secret key K). The user enroll his/her fingerprint.

Authentication:

(1) User insert smartcard to the reader. The reader obtains the user identity, and verifies whether the smartcard is authentic. If so, continue.

(2) User presents fingerprint to the reader. The reader performs matching to verify that it is authentic. If so, open door.

http://securityaffairs.co/wordpress/35856/cyber-crime/tv5monde-investigation-details.html

http://www.bbc.com/news/world-europe-32248779

A TV5Monde staffer accidentally revealed a password used to access the social media account of the broadcaster in an interview.