

Some Announcements

- **Assignment 1** is already out!
- Open consultation sessions on Assignment 1 next week
- **Tutorials**
- **Mid-term e-exam**: more information to be shared next week
- For those who need to use a **loaned notebook** from NUS CIT: please email me by **11 Sept (preferably ASAP)**
- **Demo videos** uploaded to Multimedia on LumiNUS!
- **Lectures**: please **join live** whenever you can!

Lecture 2: Entity Authentication (Password)

Topics:

2.1. Overview

2.2 Password (weak authentication)

2.2.1 Intercepting password while bootstrapping

2.2.2 Searching password (dictionary, guessing, exhaustive attacks)

2.2.3 Stealing password

2.2.4 Preventive measures

2.2.5 ATM attacks

2.2.6 Password reset: Security questions

2.3 Biometrics

2.4 Multi-factor authentication

2.4.1: Case studies: SMS vs token (in tutorial)

2.1 Overview

Reading:

[PF2.1] excluding Federated Identity Management

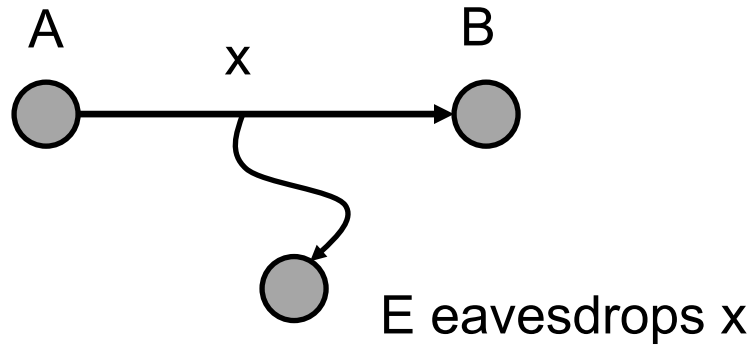
[Gollman] also has good coverage on Password (Chapter 4.1 to 4.5)

Authentication

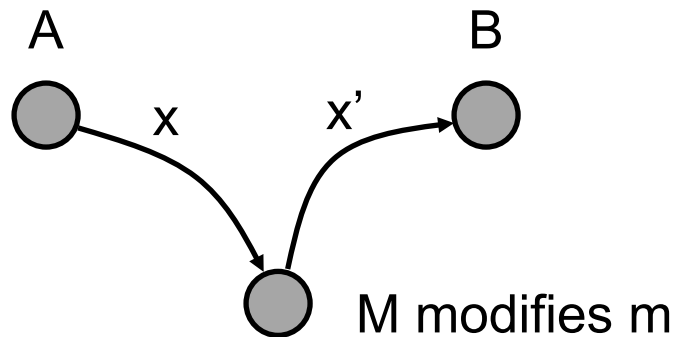
- **Authentication**: the process of assuring that the **communicating entity**, or **the origin** of a piece of information, is the one that it claims to be
- **Two types** of authentication:
 - **Entity authentication**:
 - For connection-oriented communication
 - Communicating entity is *an entity involved in a connection*
 - Mechanisms: password, challenge and response, biometrics
 - **Data-origin authentication**:
 - For connection/less communication
 - Communicating entity is *the origin of a piece of information*
 - Data-origin **authenticity** implies data **integrity** (see next slides)
 - Mechanisms: MAC or digital signature (to be cover in Lecture 3)

Threats to Confidentiality, Integrity & Authenticity: Illustration

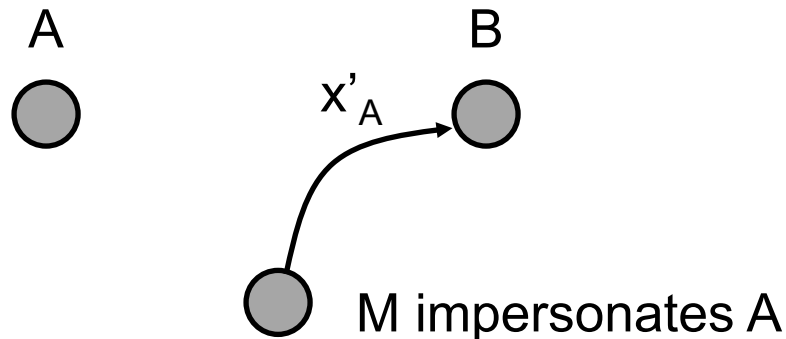
- Confidentiality:



- Integrity:



- Authenticity:



Authenticity and Integrity

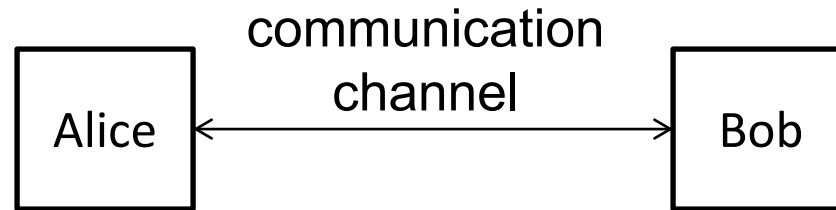
- **Authentic** (adjective): the claimed entity/origin is assured by supporting evidence
- **Authenticity**: the condition of being authentic
- **Authenticity and integrity**: are they related? Yes
- Example: in the context of an insecure channel, we can say that: “a message that *has been modified* in transit” means that “it *no longer* comes from its original source”
- In other words:
 P (“a message whose integrity is compromised”) \rightarrow
 Q (“a message is not authentic”)
- In logic, we know **contraposition**: $(P \rightarrow Q) \leftrightarrow (\neg Q \rightarrow \neg P)$

Authenticity and Integrity

- We can thus say:
 - $\neg Q$ (“an authentic message”) \rightarrow
 - $\neg P$ (“a message whose integrity is preserved”)
- Hence, **data-origin authenticity implies data integrity**
- But data integrity does *not* imply data-origin authenticity
- Authenticity is a stronger requirement than integrity
- Authenticity-preserving techniques also ensure integrity:
MAC & digital signature vs hash (*to be discussed next week*)
- Some notes & cautions:
 - Some documents use the term “integrity” to mean “authenticity”
 - Some even claim that authenticity does not necessarily give integrity
 - Hence, when reading a document, do pay attention to the context and the applications involved

Examples of Problem Ensuring Authenticity

Over *different* **communication channels**:



- 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** and wondered whether the server that her laptop was interacting with is the *authentic* “LumiNUS”? Conversely, why the LumiNUS server would be convinced that the user logged in is the *authentic* “Alice”?
- Alice tried to connect to WiFi using her phone while at NUH’s bus-stop. Among the available WiFi network names (SSIDs), an item “NUS” is listed. Was that WiFi **access point** *authentic*?

More Examples of Problem Ensuring Authenticity

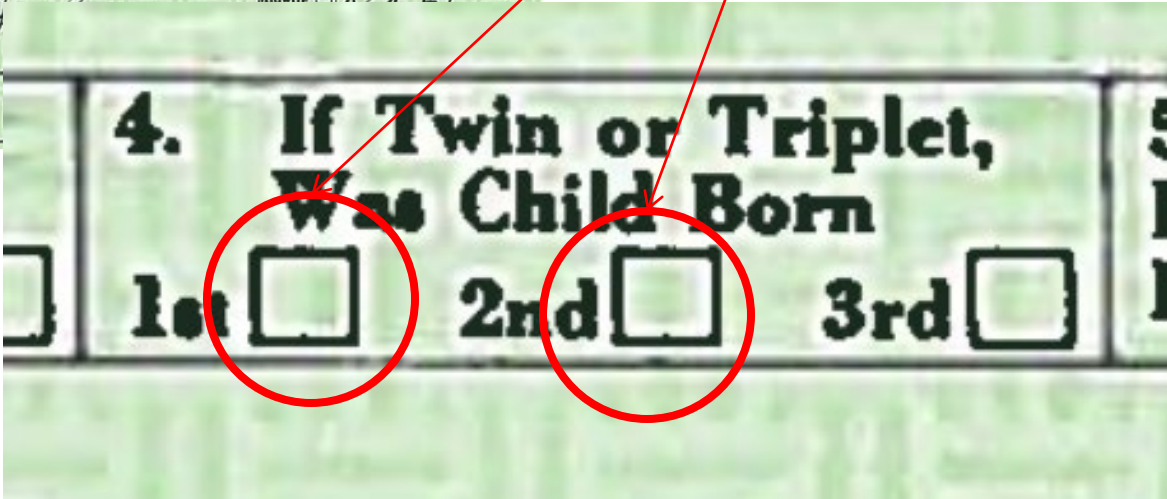
Involving presented **physical document** or **digital data**:

- Bob submitted a **medical certificate (MC)** to the lecturer, indicating that he was unfit for exam.
Was the MC *authentic* (i.e. issued by the purported clinic)?
Or had Bob altered the date?
- Is the **birth certificate** (see next slide) released by the White House *authentic* (i.e. issued by the claimed Local Registrar)?
- Alice received an **email** from her lecturer notifying her that the quiz is cancelled.
Was the email *authentic* (i.e. sent by the lecturer)?

Is This Birth Certificate Authentic?

STATE OF HAWAII
CERTIFICATE OF LIVE BIRTH
DEPARTMENT OF HEALTH
FILE NUMBER 151 61 10641

1a. Child's First Name (Type or print)		1b. Middle Name		1c. Last Name	
BARACK		HUSSEIN		OBAMA, II	
2. Sex	3. This Birth	4. If Twin or Triplet, Was Child Born		5a. Birth Date	5b. Hour
Male	Single <input checked="" type="checkbox"/> Twin <input type="checkbox"/> Triplet <input type="checkbox"/>	1st <input type="checkbox"/> 2nd <input type="checkbox"/> 3rd <input type="checkbox"/>		August 4, 1961	7:24 P.M.
6a. Place of Birth: City, Town or Rural Location				6b. Island	
Honolulu				Oahu	
6c. Name of Hospital or Institution (If not in hospital or institution, give street address)				6d. Is Place of Birth Inside City or Town Limits?	
Kapiolani Maternity & Gynecological Hospital				Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>	
7a. Usual Residence of Mother: City, Town or Rural Location		7b. Island		7c. County and State or Foreign Country	
Honolulu		Oahu		Honolulu, Hawaii	
7d. Street Address				7e. Is Residence Inside City or Town Limits?	
6085 Kalaniana'ole Highway				Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>	
7f. Mother's Mailing Address				7g. Is Residence on a Farm or Plantation?	
				Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>	
8. Full Name of Father			9. Race of Father		
BARACK HUSSEIN OBAMA			African		
10. Age of Father	11. Birthplace (Island, State or Foreign Country)	12a. Usual Occupation		12b. Kind of Business or Industry	
25	Kenya, East Africa	Student		University	
13. Full Maiden Name of Mother			14. Race of Mother		
STANLEY ANN DUNHAM			Caucasian		
15. Age of Mother	16. Birthplace (Island, State or Foreign Country)	17a. Type of Occupation Outside Home During Pregnancy		17b. Date Last Worked	
18	Wichita, Kansas	None			
I certify that the above stated information is true and correct to the best of my knowledge.		18a. Signature of Parent or Other Informant		18b. Date of Signature	
		Stanley Ann Dunham Obama		8-7-61	
I hereby certify that this child was born alive on the date and hour stated above.		19a. Signature of Attendant		19b. Date of Signature	
		David A. Lee		8-8-61	
20. Date Accepted by Local Reg.		21. Signature of Local Registrar			
AUG - 8 1961		V. Lee			
23. Evidence for Delayed Filing or Alteration					




Is This Letter Authentic? (Actual Case in Singapore)

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 committed at Cantonment Police Division on 28 November 2016 and it appears that you may be acquainted 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



POLICE COMMENDATION
AWARD
2015

NP18(1/16)

2.2 Password (Weak Authentication)

Password: An Authentication System

Stage 1: Bootstrapping

- Server and a user **establish** a common password
- The server keeps track of a file recording the ***identity*** (i.e. *userid, username*) and the corresponding ***password***

Stage 2: Authentication

- The server authenticates an entity
- If the entity gives the correct password corresponding to the claimed identity, the entity is deemed authentic

Password: An Authentication System

- The **identity** does *not* need to be kept secret:
 - It could be: username in a computer system, bank account no, customer id, etc.
- The **password** *is* a secret:
 - Only the authentic user and the server know it
 - The fact that an entity knows the password implies that it is either the server or the authentic user

Question: Analyze a password system where **no identity** is involved, i.e., just password.

You can read:

<https://technet.microsoft.com/en-us/library/cc512578.aspx>

Identification, Authentication, Authorization

The differences?

Process	Provided By	To Answer	Attributes	Uniqueness Requirement
Identification	Principal	“Who are you?”	Public assertion	Yes (locally)
Authentication	Principal	“How can you prove it?”	Secret response	No
Authorization	System	“What can I do?”	Token/ticket, access control	-

From: <https://technet.microsoft.com/en-us/library/cc512578.aspx>

Stage 1: Bootstrapping

- The password is to be established during bootstrapping
- This can be done by either:
 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 (e.g. NUSNET, Singpass, WiFi router)

Stage 2: Password-based Authentication

- Typical interaction:

User → Server : My name is ***Alice***

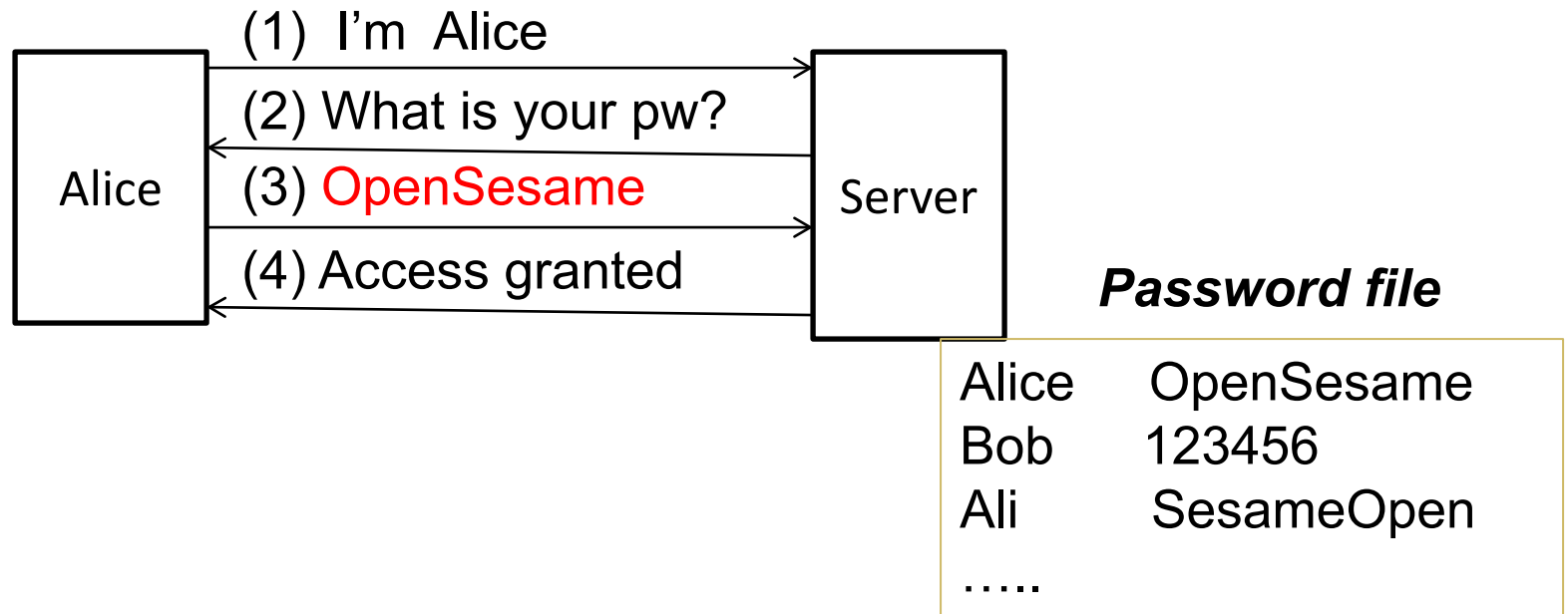
Server → User : OK. *Alice*, what is your password?

User → Server : ***OpenSesame***

Server : OK. You are indeed *Alice*.

- Alternatively, authentication can be carried out without interactions:
 - User just sends the following SMS to a server:
Userid: ***Alice@nus.edu.sg***. Password: ***OpenSesame***.
Instruction: Unsubscribe (from your mailing list.
No more junk mail please)

System Diagram



Weak Authentication System and Replay Attack

- Password system is classified as a “***weak authentication***” system
- A weak authentication is one that subjected to this simple “***replay attack***”: information sniffed from the communication channel can be used to impersonate the user at a later time
- In contrast, under “**strong authentication**”:
 - Information sniffed during the process can’t be used to impersonate the user
 - We will briefly look into this in subsequent lectures

Question (Terminologies): What are “***Sniff***” and “***Spoof***”?

Attacks on Password System

Different **possible attacks**:

- Attack the bootstrapping
- **Searching** for the password:
 - Guessing
 - Dictionary attacks
 - Exhaustive attacks
- **Stealing** the password:
 - Eavesdropping: sniff the network, use keylogger
 - Spoofing login screen
 - Phishing
 - Password caching
 - Insider attacks

2.2.1 Attack the Bootstrapping

Possible Attacks on Bootstrapping

- Attacker may **intercept** the password during bootstrapping:
 - Example: if the password is sent through postal mail, an attacker could steal the mail to get the password
- An attacker uses the “**default**” passwords:
 - There are many reported incidents on this attack (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 (Mirai botnet attack):

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

Default Password on IP Camera: Real Example



Question

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**)

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, spouse's name
- Password guessing types:
 - **Online guessing**: an attacker directly interacts with the authentication system
 - **Offline guessing**: an attacker can obtain the password file from the authentication system

Exhaustive Search & Dictionary Attacks

- The attacker tries different passwords during login sessions
- The attacker can employ **exhaustive search**: tries all combinations
Is it feasible? See the table on possible *key space sizes* of different character sets and password lengths
- Alternatively, the attacker can restrict the search space to a large collection of **probable passwords**:
 - Words from English **dictionary**, known compromised passwords, other language dictionaries, etc.
 - This is known as ***dictionary attack***

Table 3-1. Possible Keyspaces by Password Length and Character Set Size

Char. Set Size	Character Types				Password Length				
	Digits	Letters	Symbols	Other	4	8	12	16	20
10	Decimal				$1 \cdot 10^4$	$1 \cdot 10^8$	$1 \cdot 10^{12}$	$1 \cdot 10^{16}$	$1 \cdot 10^{20}$
16	Hexa- decimal				$7 \cdot 10^4$	$4 \cdot 10^9$	$3 \cdot 10^{14}$	$2 \cdot 10^{19}$	$1 \cdot 10^{24}$
26		Case- insensitive			$5 \cdot 10^5$	$2 \cdot 10^{11}$	$1 \cdot 10^{17}$	$4 \cdot 10^{22}$	$2 \cdot 10^{28}$
36	Decimal	Case- insensitive			$2 \cdot 10^6$	$3 \cdot 10^{12}$	$5 \cdot 10^{18}$	$8 \cdot 10^{24}$	$1 \cdot 10^{31}$
46	Decimal	Case- insensitive	10 common ⁷		$4 \cdot 10^6$	$2 \cdot 10^{13}$	$9 \cdot 10^{19}$	$4 \cdot 10^{26}$	$2 \cdot 10^{33}$
52		Upper and lower			$7 \cdot 10^6$	$5 \cdot 10^{13}$	$4 \cdot 10^{20}$	$3 \cdot 10^{27}$	$2 \cdot 10^{34}$
62	Decimal	Upper and lower			$1 \cdot 10^7$	$2 \cdot 10^{14}$	$3 \cdot 10^{21}$	$5 \cdot 10^{28}$	$7 \cdot 10^{35}$
72	Decimal	Upper and lower	10 common		$3 \cdot 10^7$	$7 \cdot 10^{14}$	$2 \cdot 10^{22}$	$5 \cdot 10^{29}$	$1 \cdot 10^{37}$
95	Decimal	Upper and lower	All symbols on standard keyboard		$8 \cdot 10^7$	$7 \cdot 10^{15}$	$5 \cdot 10^{23}$	$4 \cdot 10^{31}$	$4 \cdot 10^{39}$
222	Decimal	Upper and lower	All symbols on standard keyboard	All other ASCII characters	$2 \cdot 10^9$	$6 \cdot 10^{18}$	$1 \cdot 10^{28}$	$3 \cdot 10^{37}$	$8 \cdot 10^{46}$

Table from: Guide to Enterprise Password Management (Draft), NIST, 2009 <http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf>

Dictionary Attacks

- **Hybrid attack:** it is possible to carry out exhaustive search together with dictionary attack
- Example: try all combinations of 2 words from the dictionary, and 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 listed 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)

Famous Case



From: Wikipedia

**Ben Hall**
@Ben_Hall

[Follow](#)

Ouch. Mark Zuckerberg's social media accounts have been hacked

7 Replies

**Mark Zuckerberg** @finkd
Hey, @finkd You were in LinkedIn Database with the password "dadada" ! DM for proof..

12 Faves9 Retweets

5 Jun 2016 at 20:01via Twitter Web Client



Pinterest for iPhone
★★★★★
700,000+ 5-star reviews

Continue

Log in with browser

**Hacked By OurMine Team - Read**
@zuck

12:08 PM - 5 Jun 2016

575 Retweets 368 Likes



His hacked password was: *****

2.2.3 Stealing the Password

1. Eavesdropping: With Various Different Ways

- ***Shoulder surfing***: look-over-the-shoulder attack
- ***Sniffing***: listening/intercepting **the communication channel**:
 - Some systems and protocols simply send the password over a public network in clear (i.e. unencrypted)
 - Examples: FTP, Telnet, HTTP
- ***Sniffing*** a wireless keyboard:
See <http://arstechnica.com/security/2015/01/meet-keysweeper-the-10-usb-charger-that-steals-ms-keyboard-strokes/>
- Other method: using **sound** made by a keyboard:
([L. Zhuang, F. Zhou, J.D. Tygar, “Keyboard Acoustic Emanations Revisited”, 2005](#))

Question (Terminology): What is a “*side channel attack*” ?

Some Fun Videos to Watch: Live Password Leakage



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

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

In a live interview, a TV5Monde staffer accidentally revealed a password used to access the broadcaster's social media account!

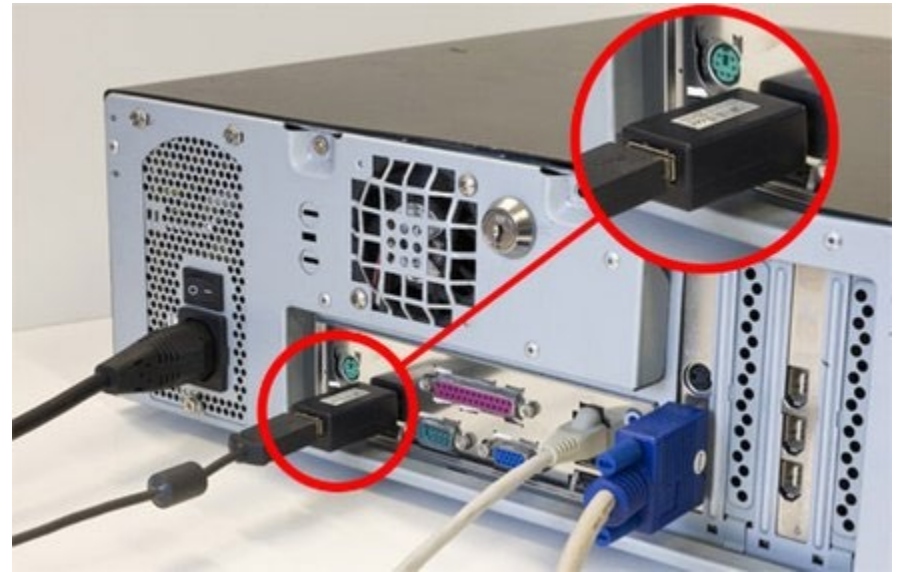
Keylogger

- A **keylogger** captures/records the keystrokes, and sends the information back to the attacker, via a “covert channel”
- By **software**:
Some computer viruses are designed as a **keylogger**
- By **hardware**:
Hardware keylogger: see the next slide for an example
- **See** “Hardware-based keyloggers” in http://en.wikipedia.org/wiki/Keystroke_logging

Hardware Keylogger



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



https://en.wikipedia.org/wiki/Hardware_keylogger

Question (Terminology): What is a “*covert channel*”?

2. Login Spoofing

- Attacker displays a “spoofed” (fake) login screen



- Prevention:
 - Some systems have a ***secure attention key*** or ***secure attention sequence*** (e.g. Ctrl+Alt+Del for Window NT)
 - When they are pressed, the system starts the **trusted login processing**

3. Phishing

- Similar to login spoofing
- The user is tricked to voluntarily sends the password to the attacker **over the network**
- Phishing attacks ask for password under some false pretense. For example:

☆ Lynn Luckett
IT Care

21 January 2015 2:31 pm



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.

This email is confidential and intended solely for the use of the individual to whom it is addressed. If you are not the intended recipient, be advised that you have received this email in error, and that any use, dissemination, forwarding, printing, or copying of this email is prohibited. If you have received this email in error, please contact the sender.

A Real Recent Phishing Attempt (in NUS)

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

Dear [REDACTED]

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.

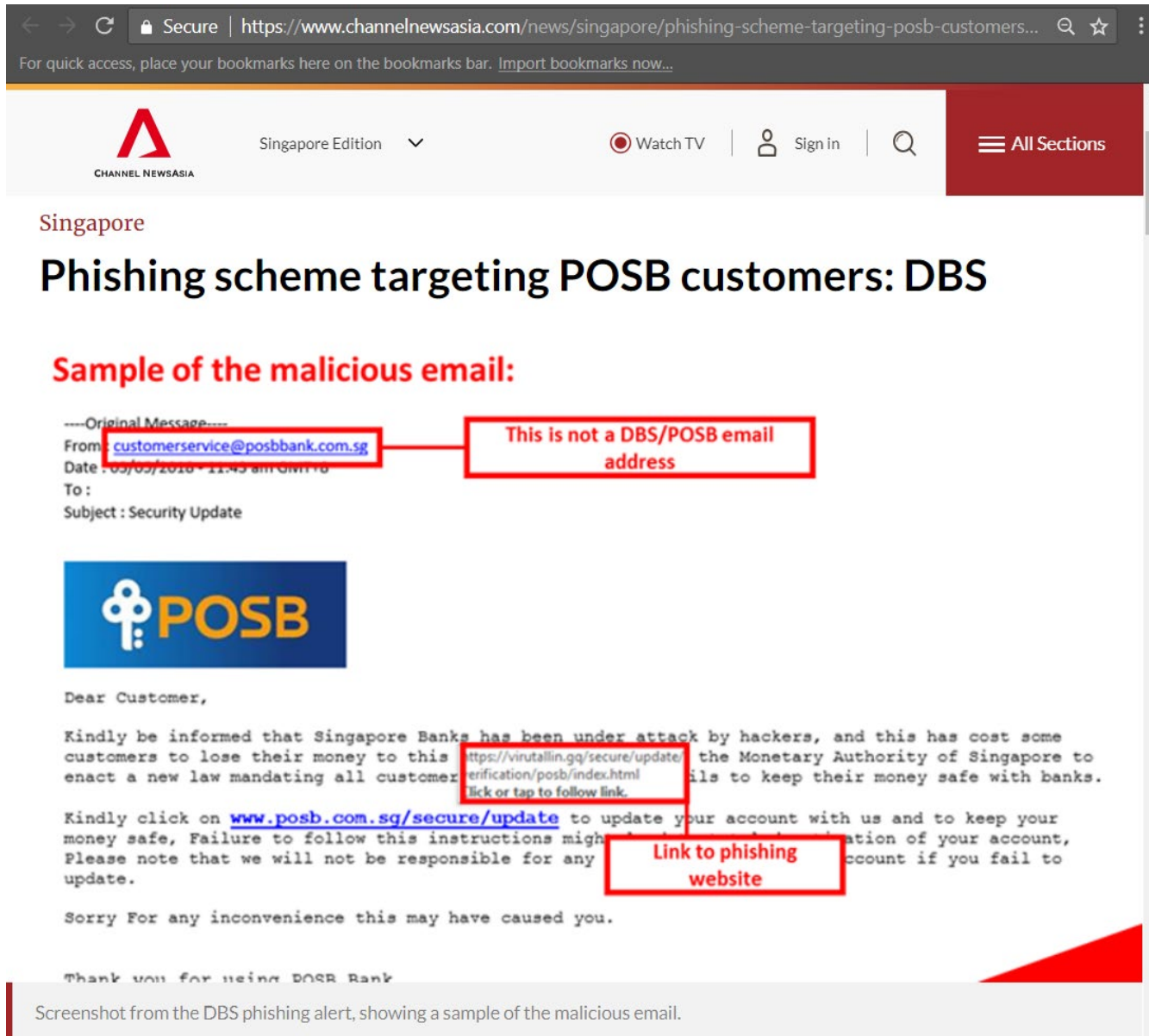
[Change NUSNET Password](#)

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.

Another Example: POSB Phishing



Spear Phishing

- Phishing can be targeted to a particular small group of users (e.g. NUS staff in the above example)
- Such attack is generally known as ***spear phishing***, which is an example of ***targeted attacks***
- Phishing attack is a type of ***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.”
See http://en.wikipedia.org/wiki/Social_engineering_%28security%29

Although It's Relatively Low Tech....: A Warning for You!

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.

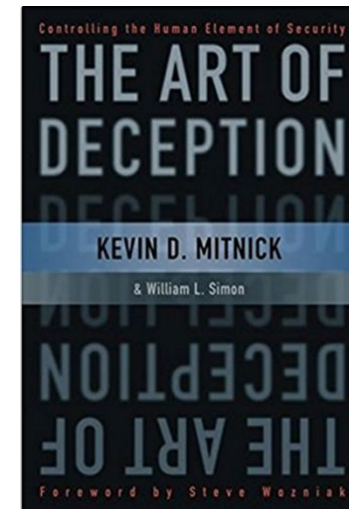
Read the paragraph on phishing.

<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.

More on Phishing

- Phishing of passwords is typically done through emails, but can also be carried out over phone calls
- Spear-phishing can be **very effective**
See [PFpage275], Sidebar 4-11
- More on social engineering techniques: Kevin D. **Mitnick** and William L. Simon, *“The Art of Deception: Controlling the Human Element of Security”*, 2003



Question (Terminology):

What are ***Phishing, Pharming, Vishing*** and ***Smishing***?

(You can read for e.g.: <http://csbweb.com/phishing.htm>)

Preventing Phishing

- User education: phishing drill

The screenshot shows a phishing email designed to look like a booking confirmation. It includes a header with a logo, a subject line, and a 'High importance' tag. The body contains a 'OneBooking.com' banner, a thank you message, and booking details. Two callout boxes point to the email address and a 'Change your booking' link. A third callout box points to a paragraph of text at the bottom.

Callout 1: Are you expecting this email? Does the email address end with the domain, Onebooking.com?

Callout 2: Mouse over the hyperlink without clicking it. Does it show the domain, OneBooking.com?

Callout 3: Flustering recipient by creating a sense of urgency and scaring are common tactics used in Phishing email.

Email Content:

BS Batam Sea View Resort via OneBooking.com <Club55@travelrefundshq.com>
Your Booking is Confirmed for Batam Sea View Resort
This message was sent with High importance.

OneBooking.com Booking No.:12782601890

Thanks Jitendera Sarda!

Your Booking for **Batam Sea View Resort** in **Indonesia** Is Confirmed

You'll pay the property directly. Batam Sea View Resort in Indonesia handles all payments, so please check below for more information.

[Change your booking](#)

Your reservation : 2 nights, 1 Superior room
Check in : Wednesday, 9 Aug 2017 (from 15:00)
Check out : Thursday, 10 Aug 2017 (until 12:00)
Price : S \$149

*You will pay direct to Batam Sea View Resort. 7% Tax is excluded. 10% service charge is excluded.
This reservation cannot be cancelled free of charge.*

[Cancel your booking](#)

This Superior Room has a satellite TV and air conditioning

Guest Name Jitendera Sarda
Number of Guests max 2 people
Meal Plan Breakfast is included

Preventing Phishing

- **Phishing repository** site:
 - Example: phishtank.com (submit suspected phishes, track the status of your submissions, verify other users' submissions)
- However, it can be tricky to accurately determine if an unsolicited email is a phishing
 - Example: SonicWall **Phishing IQ Test**
<https://www.sonicwall.com/phishing/>
 - *You can test your own phishing-spotting skill!*
- Any good/secure way of verifying a suspected phishing email?
 - When in doubt, call for help/clarification!?

4. Password Caching

- When using a shared workstation (for e.g. a browser in airport), information keyed-in could be cached
- The next user may be able to see the cache
- Prevention: Clear the **browser's cache** and close the browser when using a shared workstation

5. Insider Attack

Some examples:

- A **malicious system admin** who steals the password file
- The system admin's account is compromised (e.g. password stolen via phishing), leading to a loss of password file

2.2.4 Preventive Measures

Use Strong Password

- **Randomly chosen:**

- A password is chosen randomly among all possible keys using an **automated password generator**
- High “entropy” but difficult to remember:
e.g. 3n5dcvUD9cfm (10 characters)

- **User selection:**

- Mnemonic method: Pbmbval!
- Altered passphrases: Dressed*2*tge*9z
- Combining and altering word: B@nkC@mera

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

- **Read** page 3-10 of “Guide to Enterprise Password Management (Draft)”, NIST, 2009

<http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf>

Password Protection

- **Limited login attempts:**
 - Add delay into login session
 - Add security questions
 - Auto-lock the account after a few failed attempts
- **Password checker:**
 - Check for weak password when user registers/changes password (for e.g. using password dictionary)
- **Password metering:**
 - Indicate weak, average, strong passwords

Password Protection

- **Password ageing:**
 - Users must regularly change passwords
 - Nevertheless, many believe that frequent changes of passwords actually lower security
 - See https://www.schneier.com/blog/archives/2016/08/frequent_passwo.html
- **Password usage policy:**
 - Rule set by an organization to ensure that users use strong passwords, and minimize password loss
 - Example: the policy may state that a password has to be at least 10 characters

Question:

What is NUSNET password policy?
Does the password expire?

Protecting Password File

- Recap: the **password file** stores userid+password
- It could be leaked, due to:
insider attack, accidental leakage, hacked system, etc.
- There are many well-known incidents where **unprotected or weakly protected** password files are leaked, leading to a large number of passwords being compromised
- See “2012 LinkedIn Hack”:
https://en.wikipedia.org/wiki/2012_LinkedIn_hack
- Hence, it is desired to add an **additional layer of protection** to the password file

Hashed Password (To 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**”. Note that this is **inaccurate**. For encryption, there is a way to recover the password from the ciphertext. For cryptographically secure hash, it is infeasible to recover the password from its hashed value.)
- During authentication, the password entered by the entity is 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

$\text{Hash}(\text{“SesameOpen”}) = \text{“da5DGDSDFd3”}$

Hashed Password (To revisit This Slide after Hash is Covered)

- It is desired that the same password will be hashed into *two different values* for two different userid. Why?
- This can be achieved by using **salt**

Password in clear

Alice	OpenSesame
Bob	123456
Ali	SesameOpen
Charles	SesameOpen

Salted-hashed password

Alice,	Adf3,	39Gkaj10Dmf
Bob,	a3gh,	d978bjklDFD
Ali,	f8ad,	DJk34hoaev7
Charles,	10vd,	K108ELvio2B

$\text{Hash}(\text{"f8adSesameOpen"}) = \text{"DJk34hoaev7"}$
 $\text{Hash}(\text{"10vdSesameOpen"}) = \text{"K108ELvio2B"}$

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

Usage and Attacks

- 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*: it reduces operating cost of helpdesk
 - *Weakening security*: attackers have another mean to obtain access
- Common “secret” questions?
 - Name your pet, aunt’s middle name, movie...
 - Problem: not really secret!
- See [PF2.1] SideBar 2-1 & 2-2 on **known past incidents**:
 - US vice presidential candidate Sarah Palin’s Yahoo! email hack
 - Attack by George Bronk by scanning Facebook pages

Choices of Security Questions

(From:https://www.owasp.org/index.php/Choosing_and_Using_Security_Questions_Cheat_Sheet)

- **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)
- **Memorable:** If users can't remember their answers to their security questions, you have achieved nothing
- **Nearly universal:** The security questions should apply to a wide audience of possible
- **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

Question: Give example of “bad” security questions

Other Forms of Self-Service Password Reset

- There are many other mechanisms/forms of **password reset**
- The next slide gives a **negative example** where the password reset was not designed/implemented properly

Zoom 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.

2.2.6 ATM Attacks

ATM Card

- To get authenticated, the user has to present a *card* and the *PIN*
- ***The card*** contains a magnetic stripe, which stores the **user account id**
- Essentially, the magnetic stripe ***simplifies the input of account id*** into the ATM system: instead of keying it in, just insert the card
- ***The PIN*** plays the role of password
- Data are encoded into the magnetic stripe 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.



This card can be purchased from ebay 😊

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
 - (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>

Self-Explanatory Images of 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

See also: https://www.youtube.com/watch?v=F_D7NS3H3Rc

Fun Video to Watch: Very Big ATM Skimmer



<https://www.youtube.com/watch?v=gJo9PfsplsY> (at 5:03)

Another (really big) ATM skimmer!

See also: <https://krebsonsecurity.com/2013/12/the-biggest-skimmers-of-all-fake-atms/>

Preventive Measures

- Install ***anti-skimmer device***: a device that prevents external card reader to be attached onto the ATM



- **Shield** the keypad



- User awareness
- Use newer ***chip-based (EMV) cards***, which use encryption

See: <https://en.wikipedia.org/wiki/EMV>,
https://www.youtube.com/watch?v=B2iABG53h_0

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>

2.3 Biometrics

Reading:

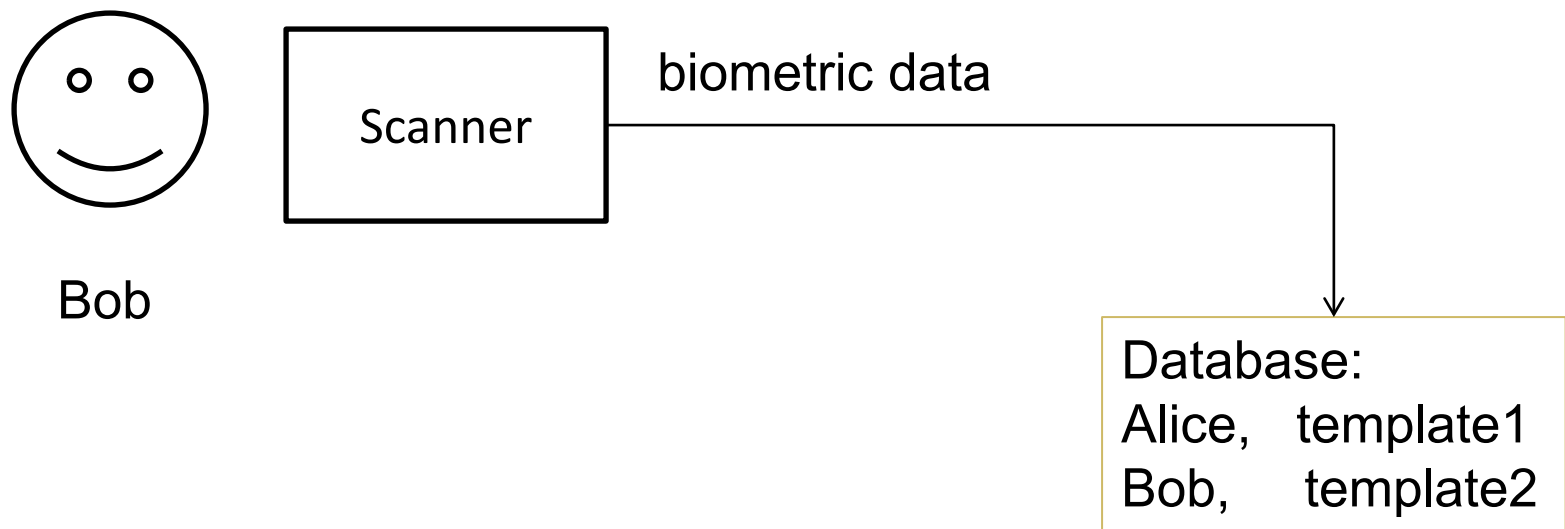
[PF] page 53-64

Biometrics

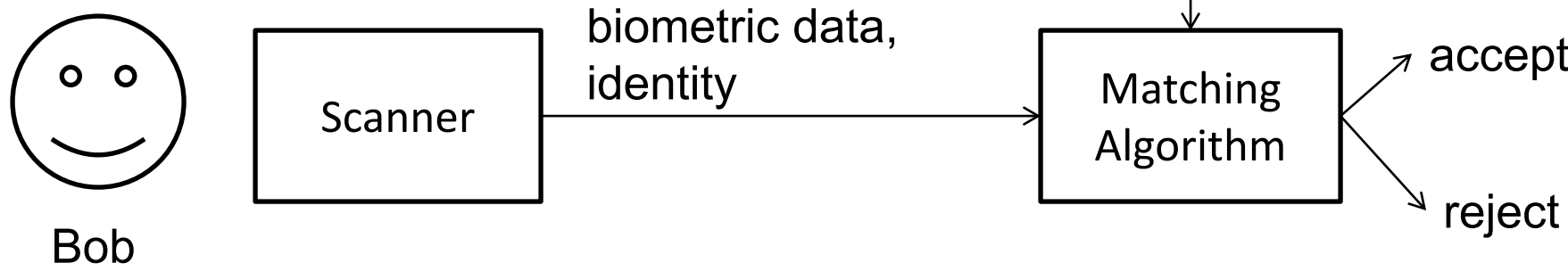
- Biometrics use **unique physical characteristics** of a person for authentication
- During ***enrollment***, a ***reference template*** of an user's biometric data is constructed and stored (similar to bootstrapping in password system)
- During ***verification***, biometric sample data of the person-in-question is captured and compared with the template using a ***matching algorithm***
- The algorithm decides whether to accept or reject
- Biometrics can be used for:
 - ***Verification*** (our focus in this lecture): 1:1 verification whether the person is the claimed person
 - ***Identification***: 1: n comparison to identify the person from a database of many persons

Process Diagram

Enrollment



Verification (Authentication)



Differences between Biometric and Password

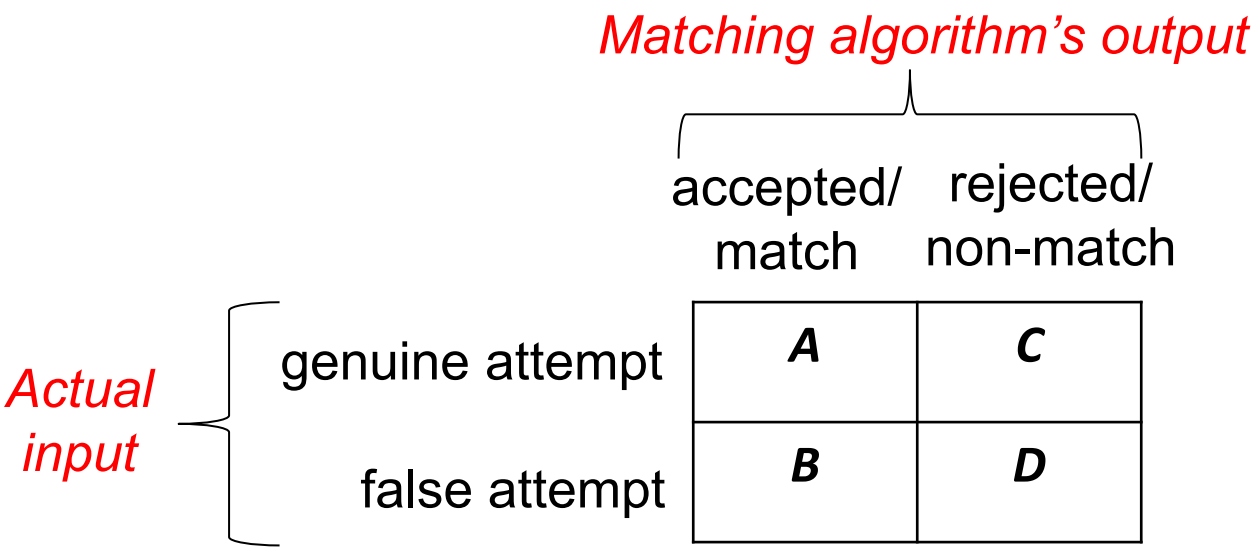
Password	Biometric
Can be changed (revoked)	Can't
Need to remember	Don't have to
<i>Zero non-matched rate</i>	<i>Probability of error</i>
Users can pass the password to another person	Not possible

Matching Algorithm: Similarity/Inexact Matching

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

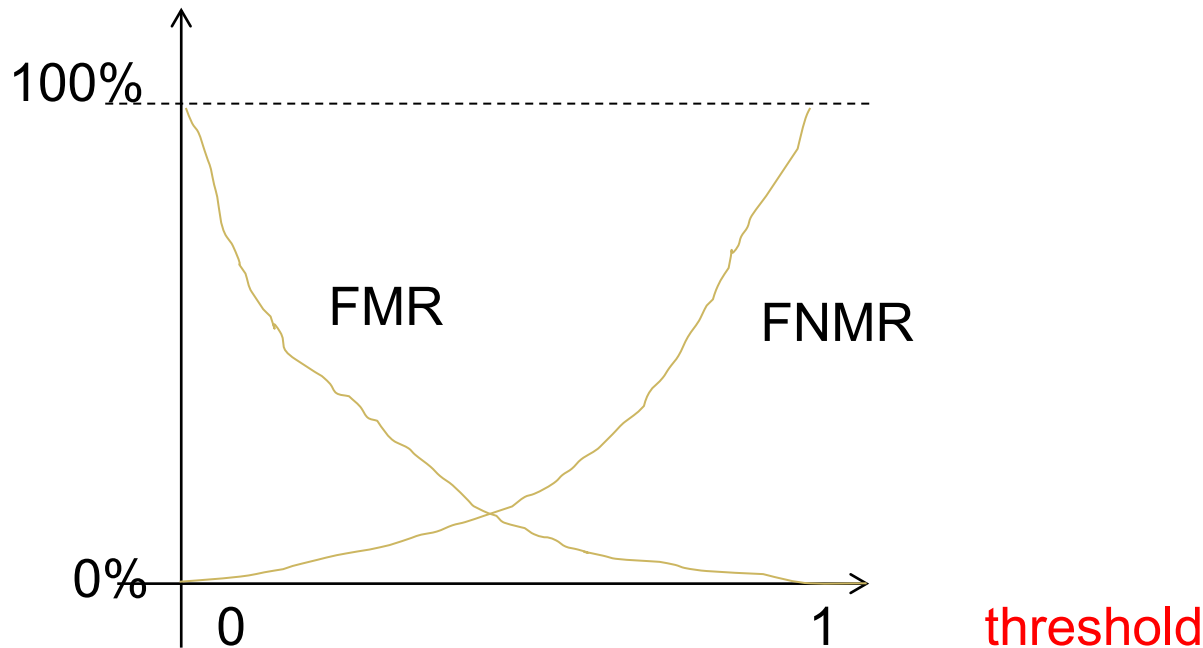
FMR =
$$\frac{\text{number of successful false matches (B)}}{\text{number of attempted false matches (B+D)}}$$

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



Threshold Value Selection

- 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? It depends on **applications**

Other Types of Errors

Equal error rate (EER):

- The rate when **FNMR = FMR**

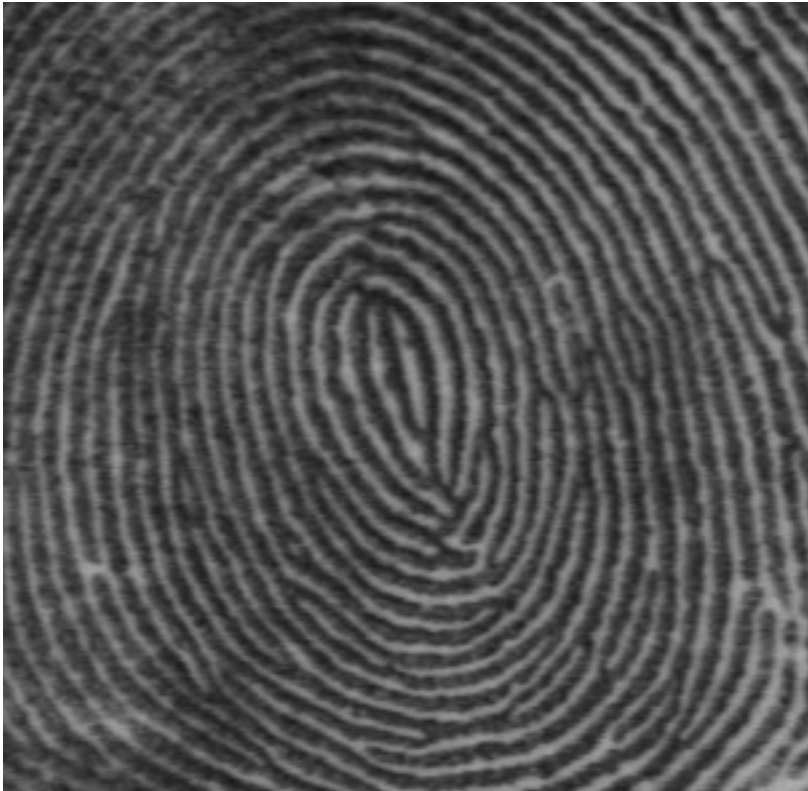
Failure-to-enroll rate (FER):

- Some users' biometric data can't be captured for **enrollment**
- For example: due to past injury

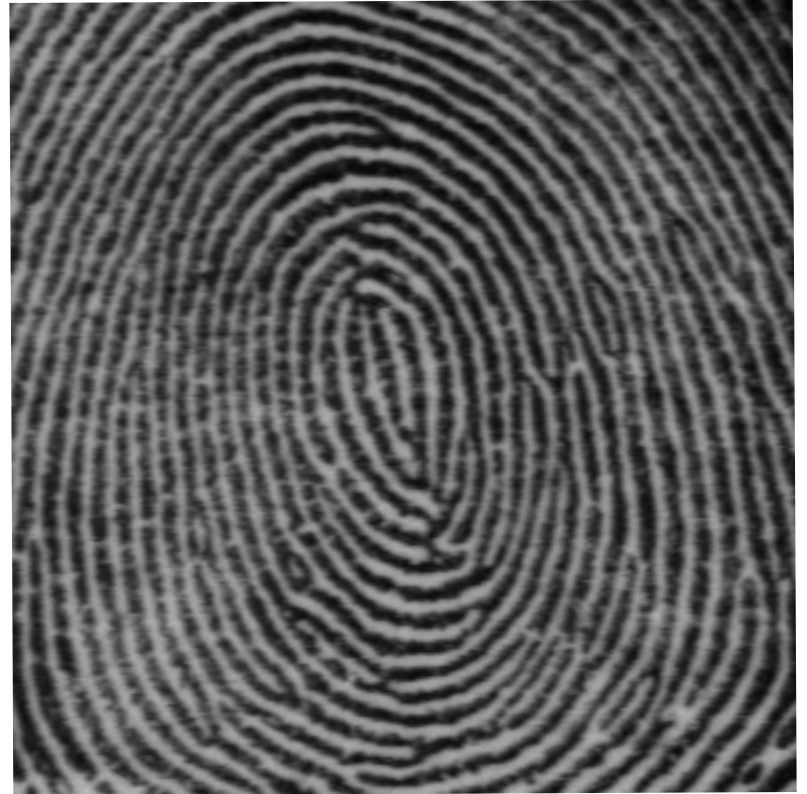
Failure-to-capture rate (FTC):

- A user's biometric data may fail to be **captured** during authentication
- For examples: fingers are too dry, dirty, etc.

Examples on Fingerprint

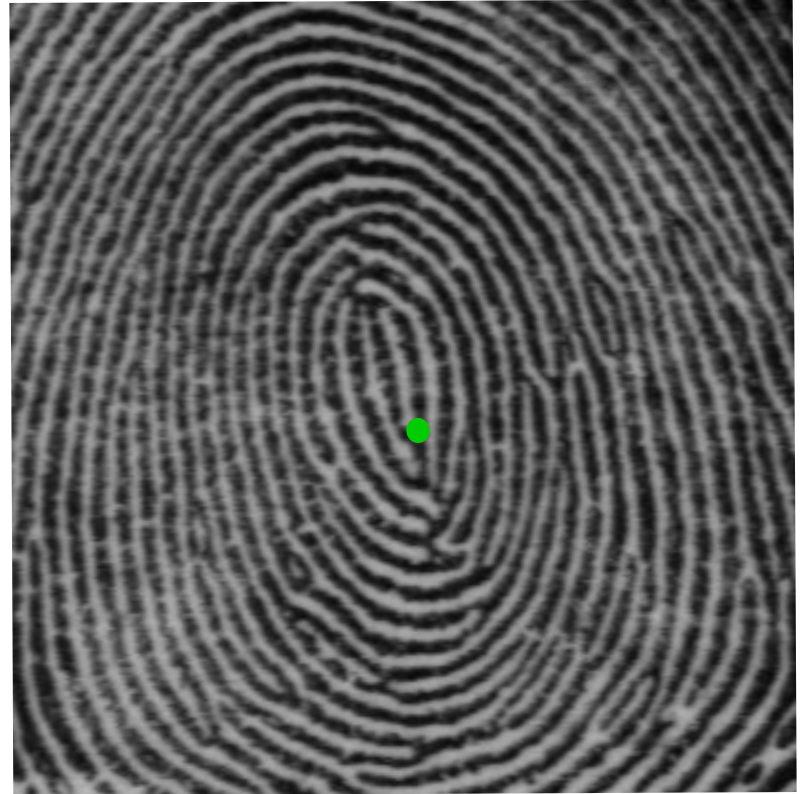
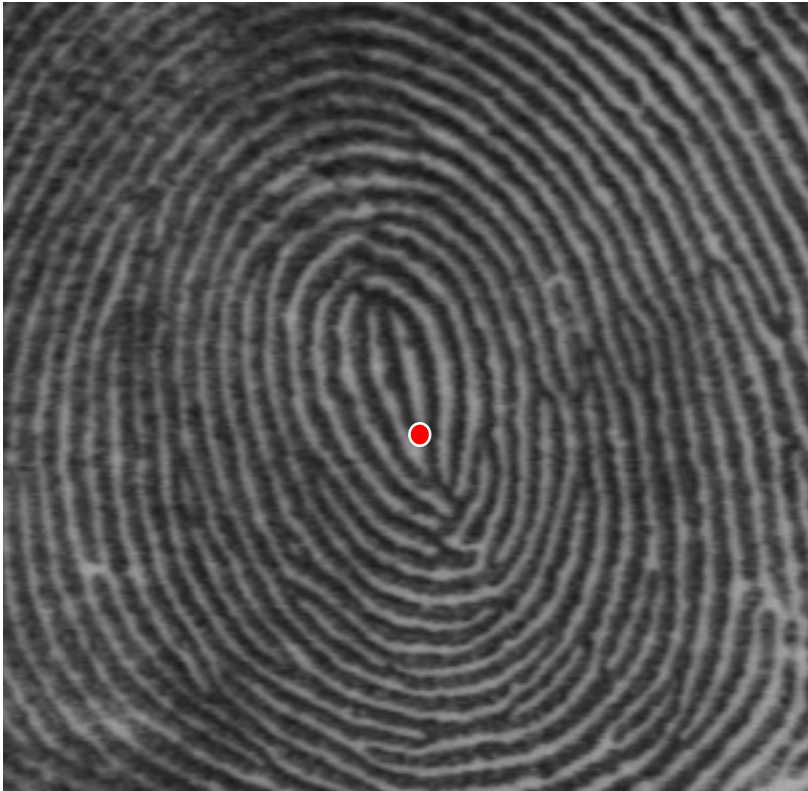


First scan of a finger



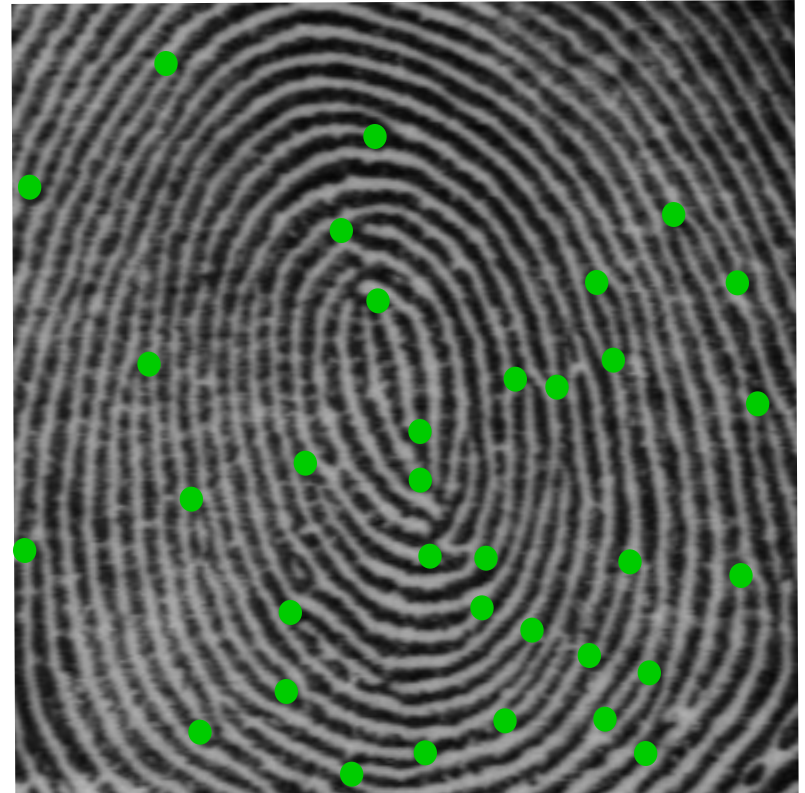
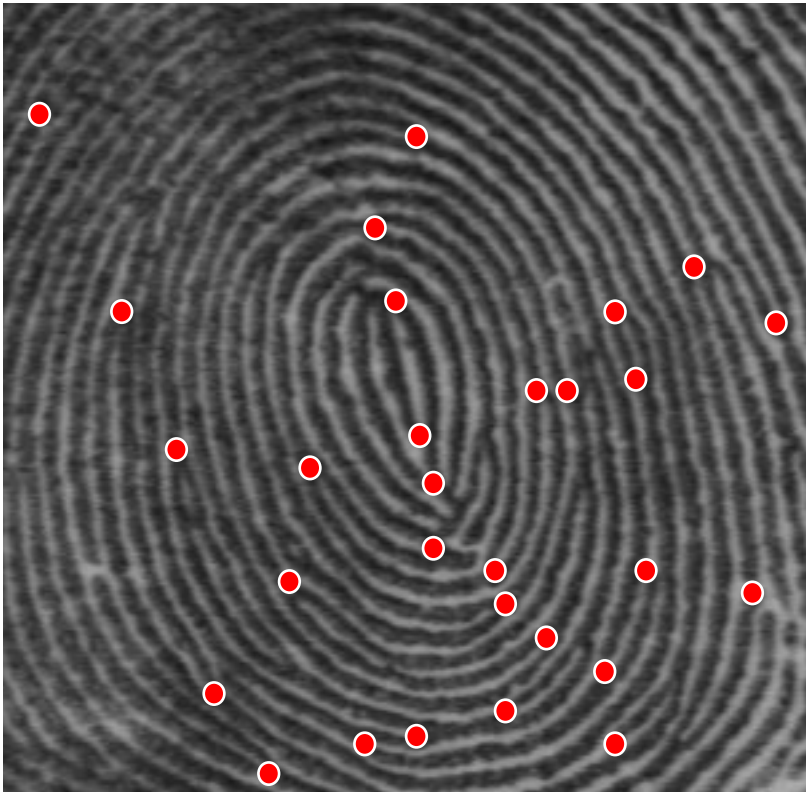
Another scan
of the same finger

Fingerprint: Background



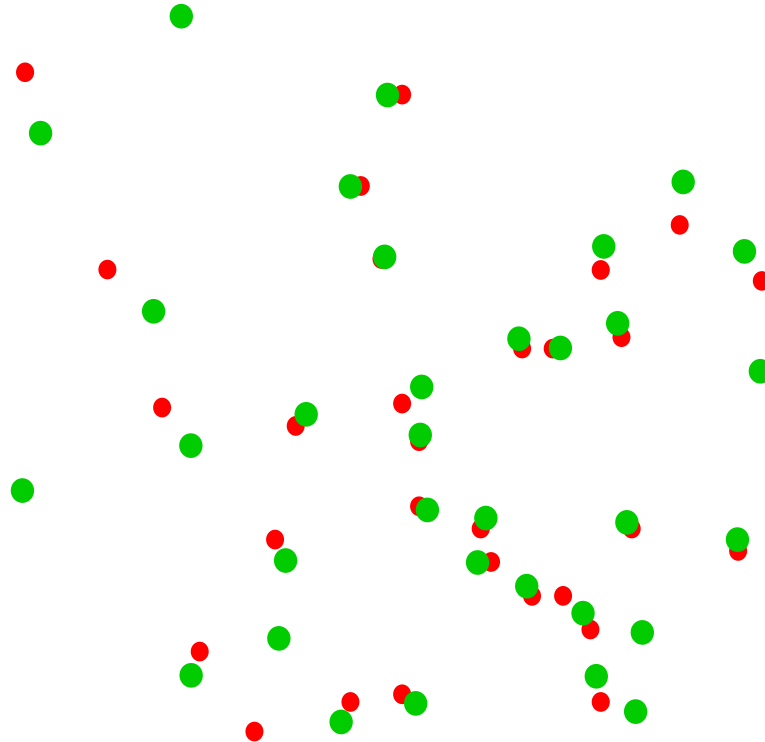
A feature point

Fingerprint: Background



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*!



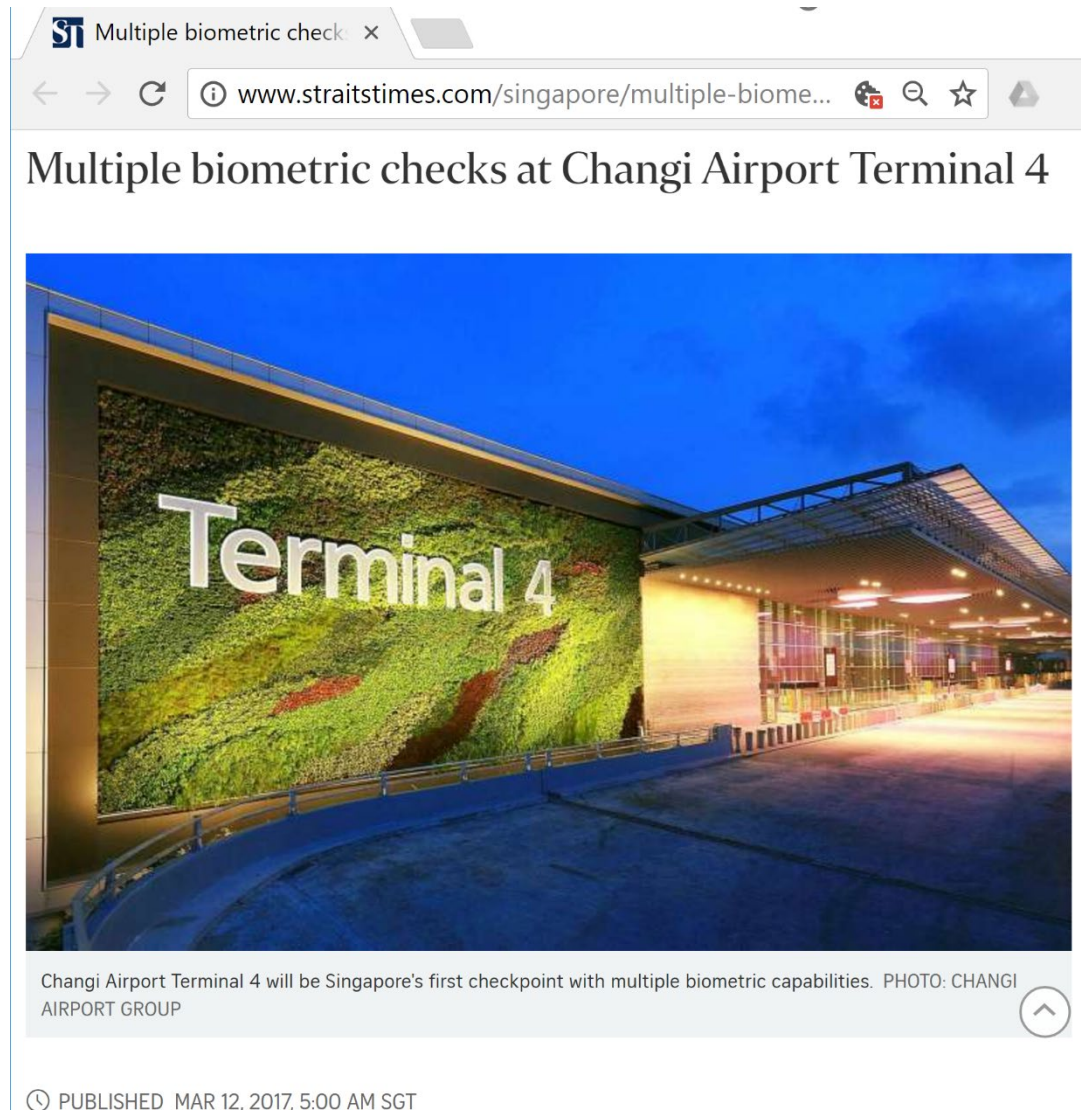
How Good is Fingerprint as a Biometric?

- Performance depends on the quality of the scanner
- See result of Fingerprint Verification Competition FVC2006
<http://bias.csr.unibo.it/fvc2006/default.asp>

Other Forms of Biometrics

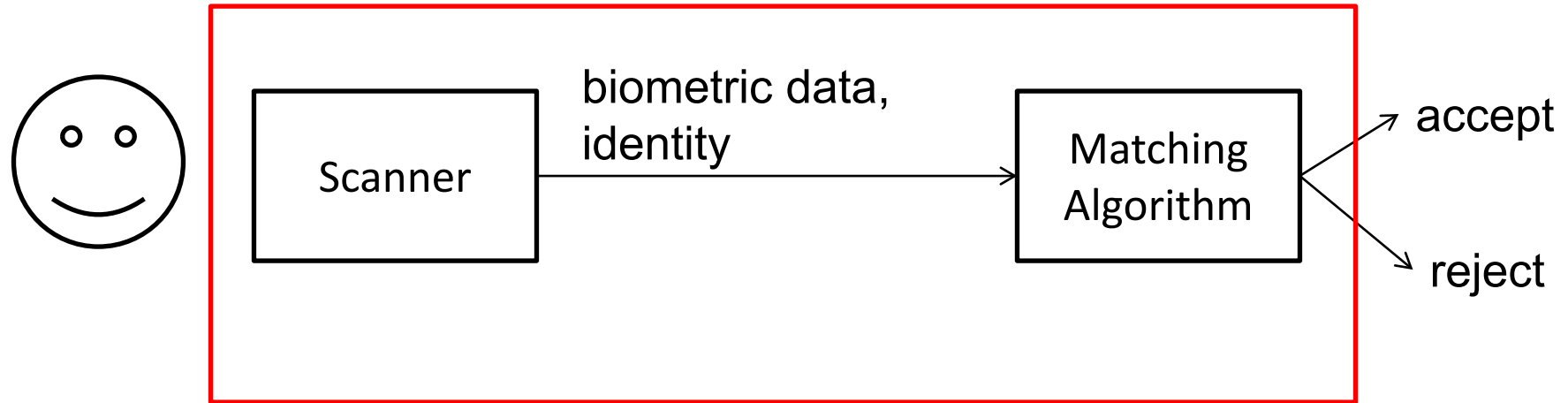
- Palm print, palm veins, hand geometry, **face**, **iris**, retina, DNA
- Others?
Tounge, odour/scent

The Straits Times,
Mar 12, 2017



Security of a Biometric System

- The scanner is assumed to be secured: **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
- 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
(For example: temperature detection in fingerprint scanner)

2.4 *n*-Factor Authentication (2FA)

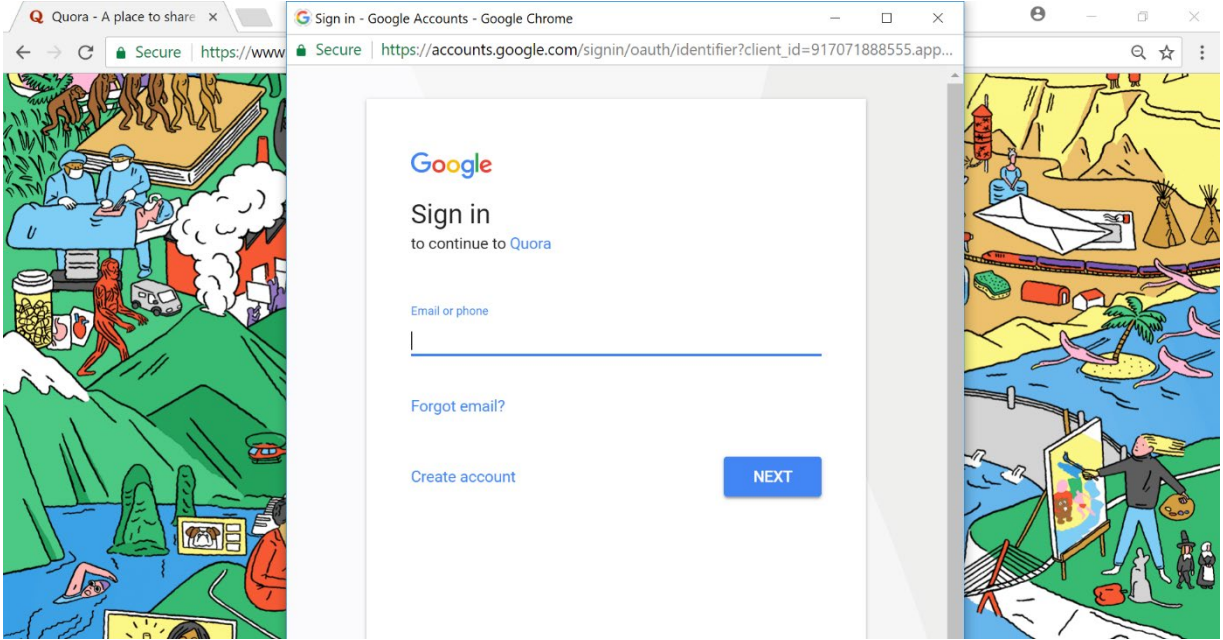
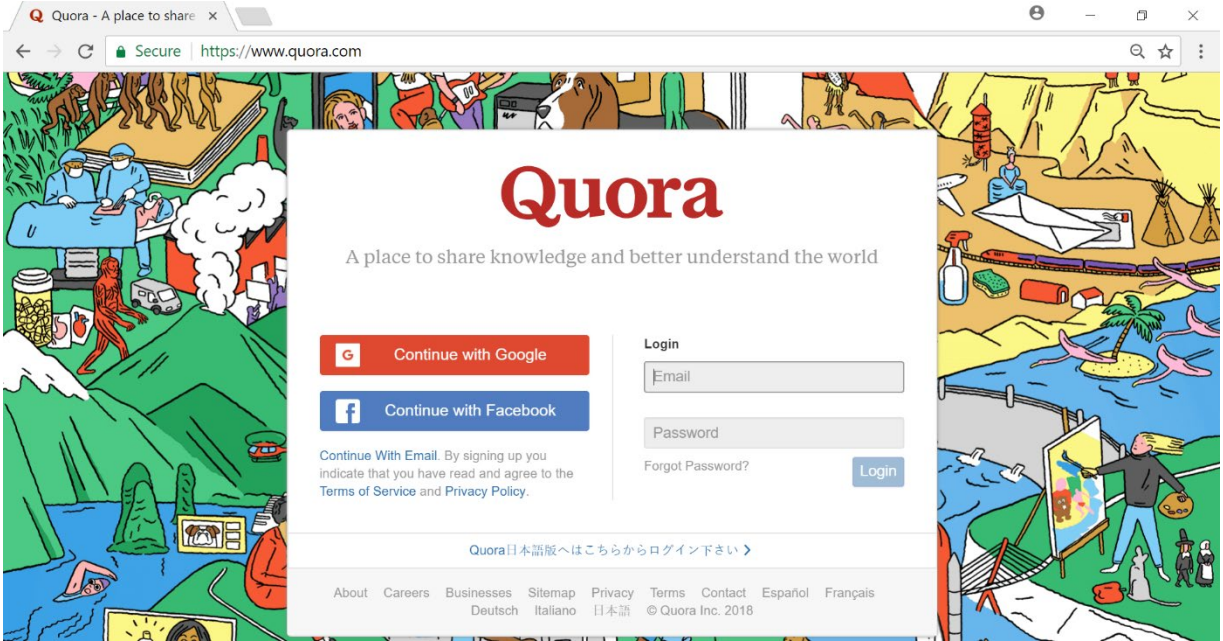
Reading:

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

***n*-factor Authentication**

- Multiple different **authentication “factors”**: at least 2 factors
- Commonly-used factors:
 1. What you **know**: password, PIN
 2. What you **have**: smart card, ATM card, mobile phone, mobile SIM card, security/OTP token
 3. Who you **are**: biometrics
- Other possible factors [Gollmann]:
 1. Where you **are**: geolocation
 2. What you do
- **Recently-used factors**:
 1. Who (some trusted system) can confirm you: PKI certificate, single sign-on (SSO)
 2. Whom you know: social authentication (in social media)
- It is called a ***2-factor authentication*** if 2 factors are employed

Example of Single Sign-On: Quora and Google



MAS Compliance Checklist

- MAS (Monetary Authority of Singapore):
 - Expects all banks in Singapore to provide 2-factor authentication for **e-banking**
 - **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.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
26.	4.4.2	Two-factor authentication at login for all types of internet banking systems and for authorising transactions is implemented.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
27.	4.4.3	For high value transactions or for changes to sensitive customer data (e.g., customer office	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

What You Have: OTP Token

One-Time Password (OTP) token:

- A hardware that generates one time password (i.e. password that can be used only once)
- Each token and the server share *some secret*
- 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***.
(See “TOTP: Time-Based One-Time Password Algorithm”, RFC 6238)
 2. **Sequence-based:** An event (for e.g. user pressing the button) triggers the change of the password

**: Not to be confused with “One-Time Pad”*

Example of 2FA (1): Password + OTP Token

Registration:

- The server issues a **OTP token** to the user, which contains a “secret key” that the server knows
- User sets a **password**

Authentication:

- (1) User “presses” **the token**, which then computes and displays a **one-time-password (OTP)**
- (2) User sends username, **password** and **OTP** to server
- (3) Since the server has the “secret key”, the server can also compute the OTP
- (4) Server verifies that both OTP and password are correct

New Trend of OTP Token: Mobile App as a Soft Token!

4/11/2017

DBS rolls out 'soft' tokens to replace all hardware tokens by June 2018, Singapore News & Top Stories - The Straits Times

THE STRAITS TIMES

DBS rolls out 'soft' tokens to replace all hardware tokens by June 2018



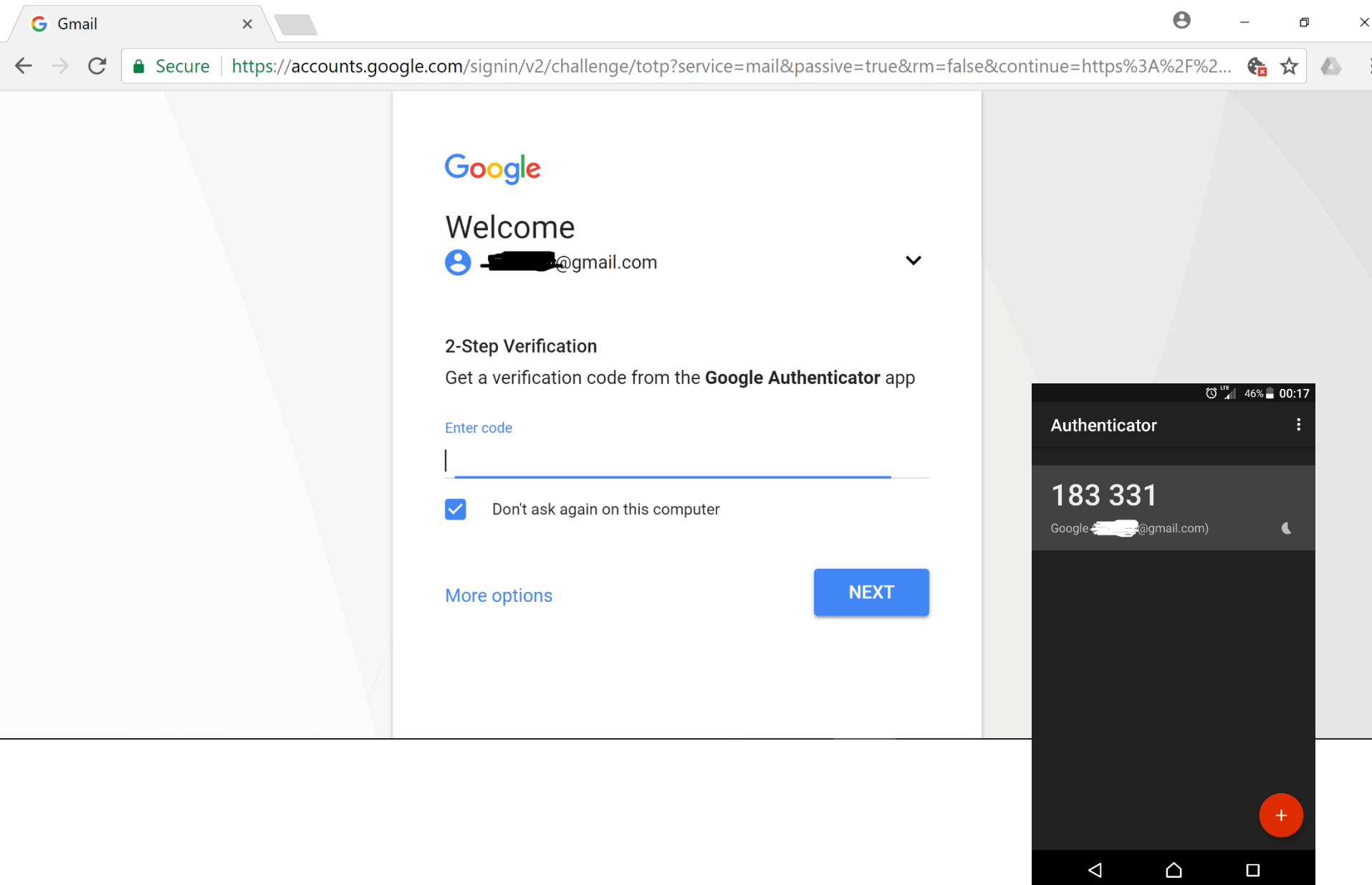
DBS digibank

Coming soon: The new digital token



An e-mail sent by DBS to customers this week informing them of the new digital token. PHOTO: DBS

Another New Trend of OTP Token: Authenticator App



Another New Trend of OTP Token: Authenticator App Setting


https://myaccount.google.com/signinoptions/two-70%

Search

← 2-Step Verification ?

Set up alternative second step


Set up at least one backup option so that you can sign in even if your other second steps aren't available.

**Backup codes**

These printable one-time passcodes allow you to sign in when away from your phone, like when you're traveling.


[SET UP](#)

Rectangular Snip

**Google prompt**


Get a Google prompt on your phone and just tap **Yes** to sign in.

[ADD PHONE](#)

**Authenticator app**


Use the Authenticator app to get free verification codes, even when your phone is offline. Available for Android and iPhone.

[SET UP](#)

**Backup phone**

Add a backup phone so you can still sign in if you lose your phone.

[ADD PHONE](#)

**Security Key**

A Security Key is a small physical device used for signing in. It plugs into your computer's USB port. [Learn more](#)

[ADD SECURITY KEY](#)

88

Example of 2FA (2): 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 *via SMS*
- (3) User receives the SMS and enters the OTP
- (4) Server verifies that the OTP is correct

Examples:

Singpass, Internet banking,

SMS OTP Security

- *Question: Is SMS OTP secure?*
- No!
- Read: https://www.schneier.com/blog/archives/2016/08/nist_is_no_long.html
- From NIST's "Digital Authentication Guideline":
"[Out of band verification] using SMS is deprecated, and will no longer be allowed in future releases of this guidance."
- Possible **security threats**:
 - Interception of cellular networks' channel
 - SMS messages are stored as plaintext by the Short Message Service Center (SMSC)
 - Malware/trojan on smartphones:
"Swearing Trojan" fakes base station in China attacking 2FA online banking: <https://blog.checkpoint.com/2017/03/21/swearing-trojan-continues-rage-even-authors-arrest/>
- Expert opinion: [still better than just userid+password](#)

Example of 2FA (3): Smartcard + Fingerprint (Door Access System)

Registration:

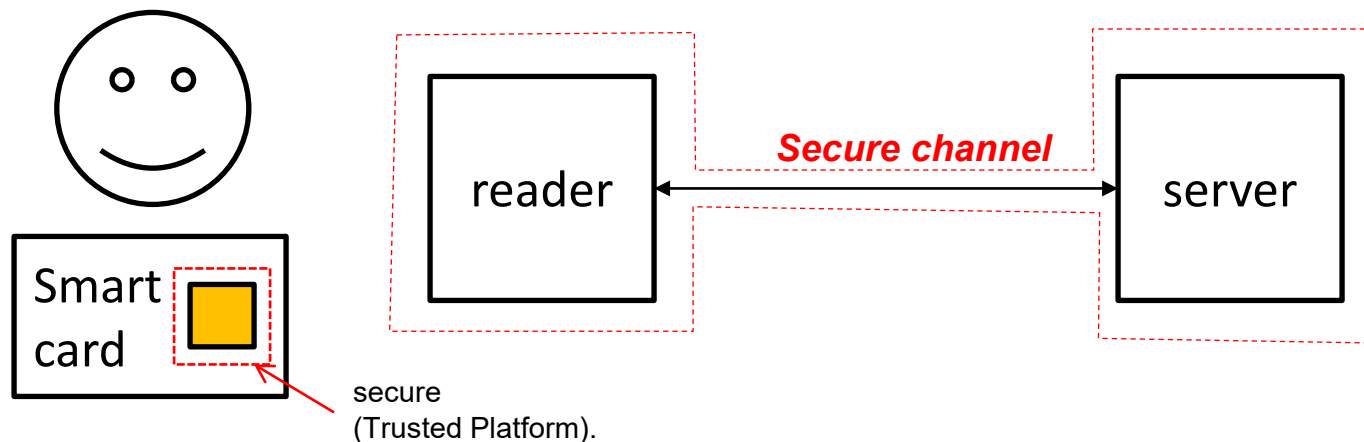
- The server issues a **smartcard** to the user (which contains a secret key K)
- The user enrolls his/her **fingerprint**

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 the door.

Security Requirements

- Very often, information on the user identity, the secret K , and the fingerprint template are *not* stored in the reader
- The reader has a secure communication channel to a **server** that stores these info



- In this case, we also assume that ***reader and server are secure***, i.e. attackers are unable to access them

Security Requirements

Some additional notes:

1. A **smart card** has this security feature:
Even if an attacker has a physical access to the card, it is extremely **difficult**, if not impossible, to **extract a secret** stored in the card
2. What are the actual two factors?
3. What is the role of the secret?
4. It is possible to eliminate the need of the server, e.g. by storing the fingerprint in the card, and storing a small secret key in the reader.
Question: how to achieve this?

Summary & Takeaways

- Two types of **authentication**:
entity authentication & data-origin authentication
- Data-origin authenticity **implies** data integrity
- **Password**: widely used for entity authentication,
but also with various potential security issues
(including **online & offline guessing attacks**)
- **ATM** attacks
- **Biometrics** (who you are): *more commonly used nowadays*
- ***n*-factor** & **2-factor** authentication

Sample Question (To be Discussed in Tutorial)

Tutorial Question:

Comparing the three 2-FA systems, which one is more “secure”?
Hypothetically, we also adopt the first two for door access system.
Are there attacks that one can prevent, but not the another?