Lecture 2: 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

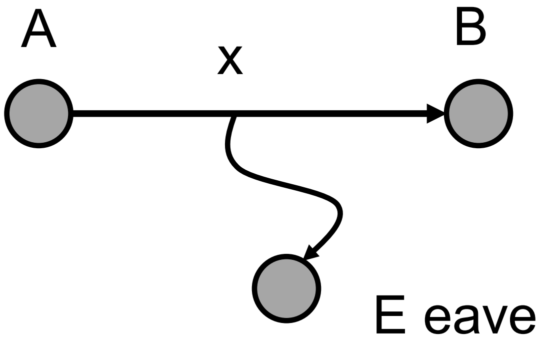
[Gollman] also has good coverage on Password (Chapter 4.1 to 4.5)

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

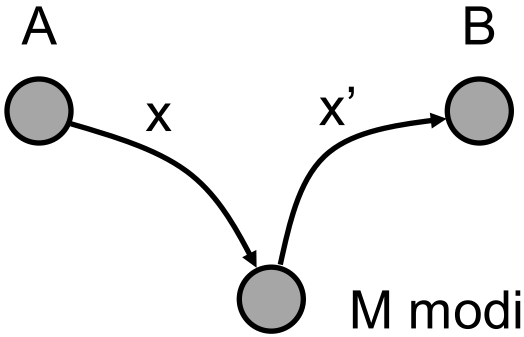
Threats to Confidentiality, Integrity & Authenticity: Illustration

- Confidentiality:



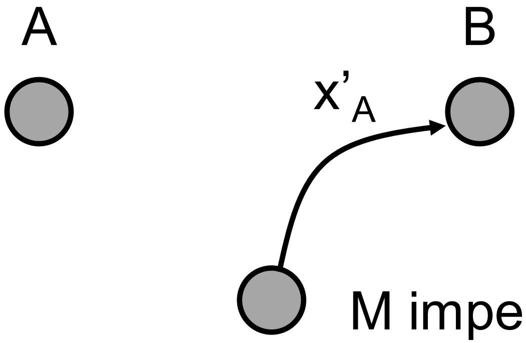
E eavesdrops x

- Integrity:



M modifies m

- Authenticity:



M impersonates A

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”) → 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:
  ¬*Q* ("an authentic message") →
  ¬*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 later*)

- Some notes:
  - 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:**

communication channel
Alice
Bob

- 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

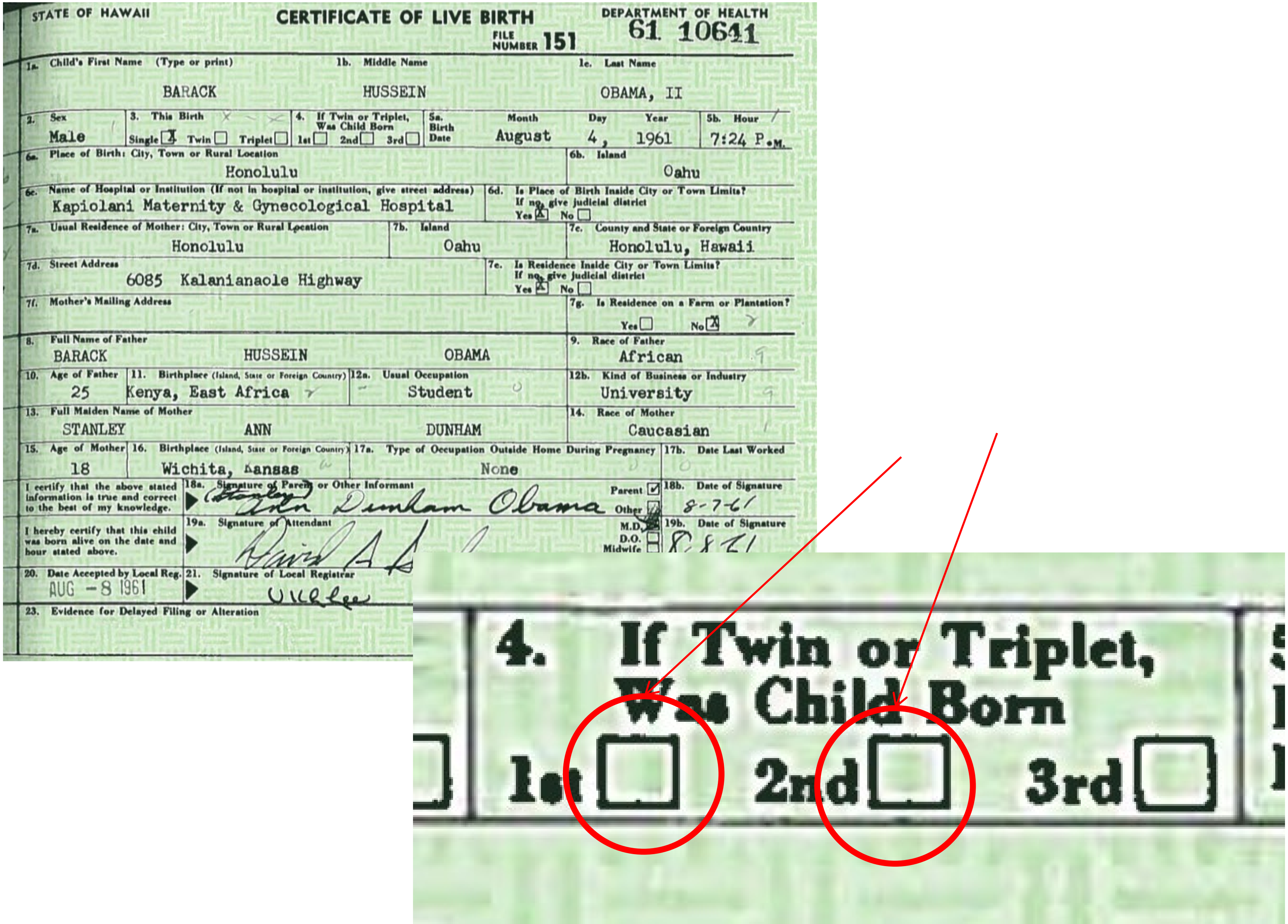
Involving presented **physical document** or **digital data:**

- 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

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 ☒ 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 ☒ 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 ☒ No □

7f. Mother's Mailing Address:

7g. Is Residence on a Farm or Plantation? Yes □ No ☒

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 S

M.D. ☒ D.O. □ Midwife □

19b. Date of Signature: 8-8-61

20. Date Accepted by Local Reg.: AUG - 8 1961

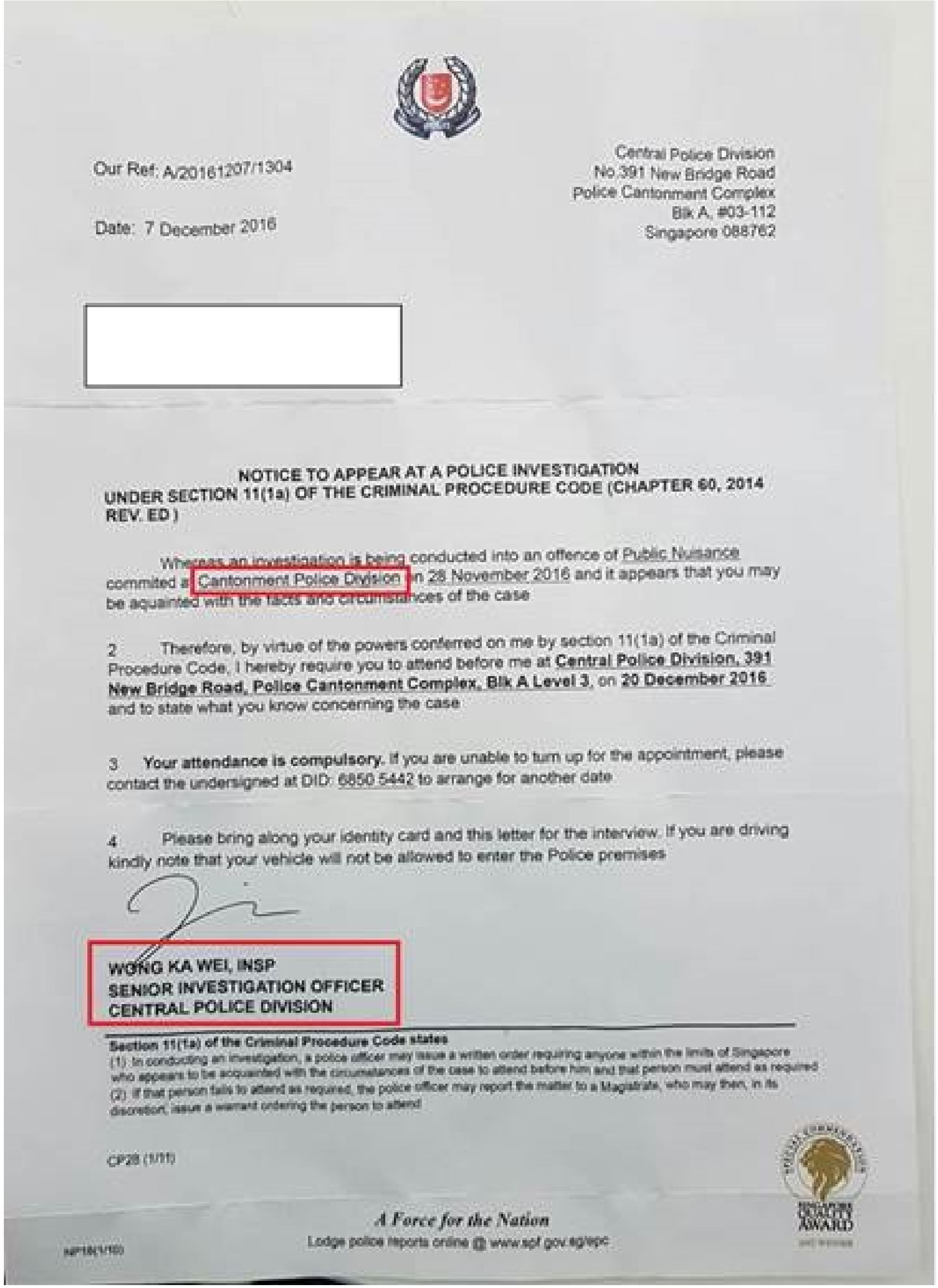
21. Signature of Local Registrar: UKLee

23. Evidence for Delayed Filing or Alteration

4. If Twin or Triplet, Was Child Born

1st □ 2nd □ 3rd □

Is This Letter Authentic?
(Actual Case in Singapore)



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

[redacted]

**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

NP18(1/10)

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

December 16, 2016

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)

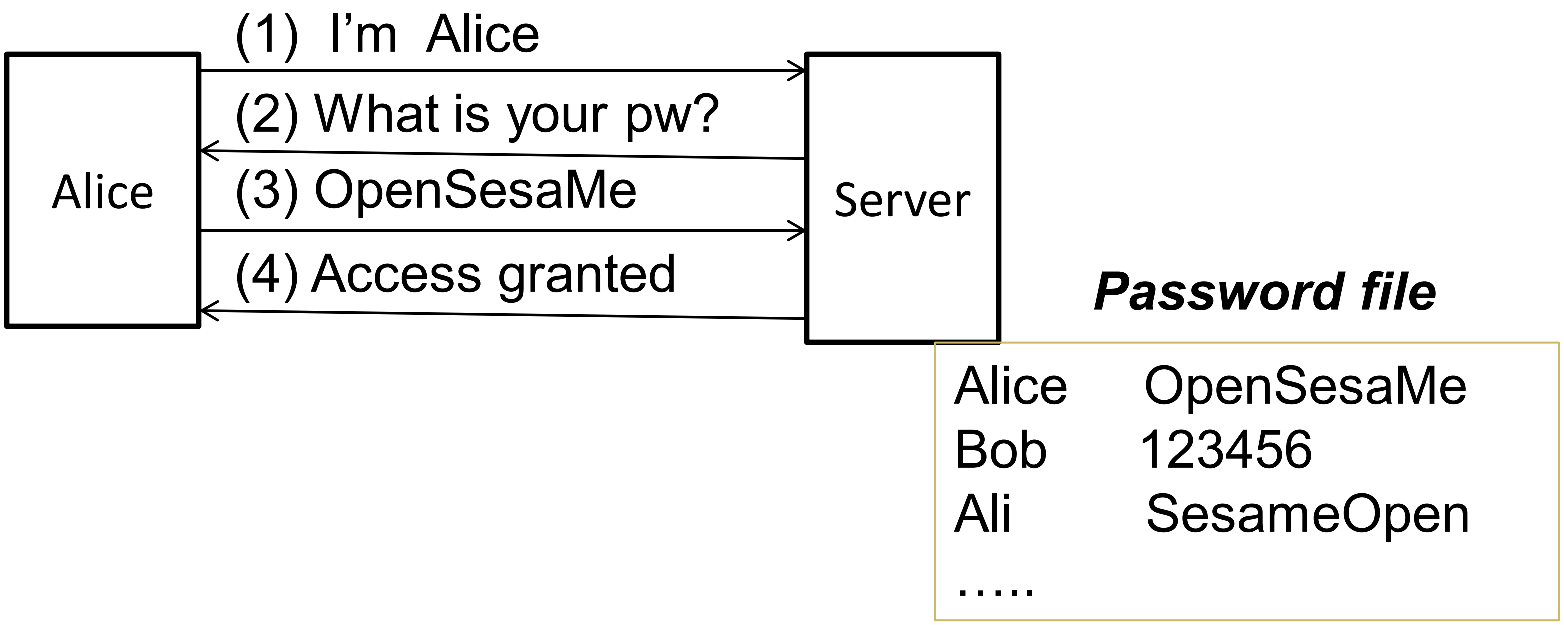
Stage 2: Password-based Authentication

- 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



(1) I’m Alice

(2) What is your pw?

(3) OpenSesaMe

(4) Access granted

Password file

Alice	OpenSesaMe
Bob	123456
Ali	SesameOpen
…..	

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 PKI later

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 key logger
  - Phishing
  - Spoofing login screen
  - Password caching
  - Insider attacks

2.2.1 Attack the Bootstrapping

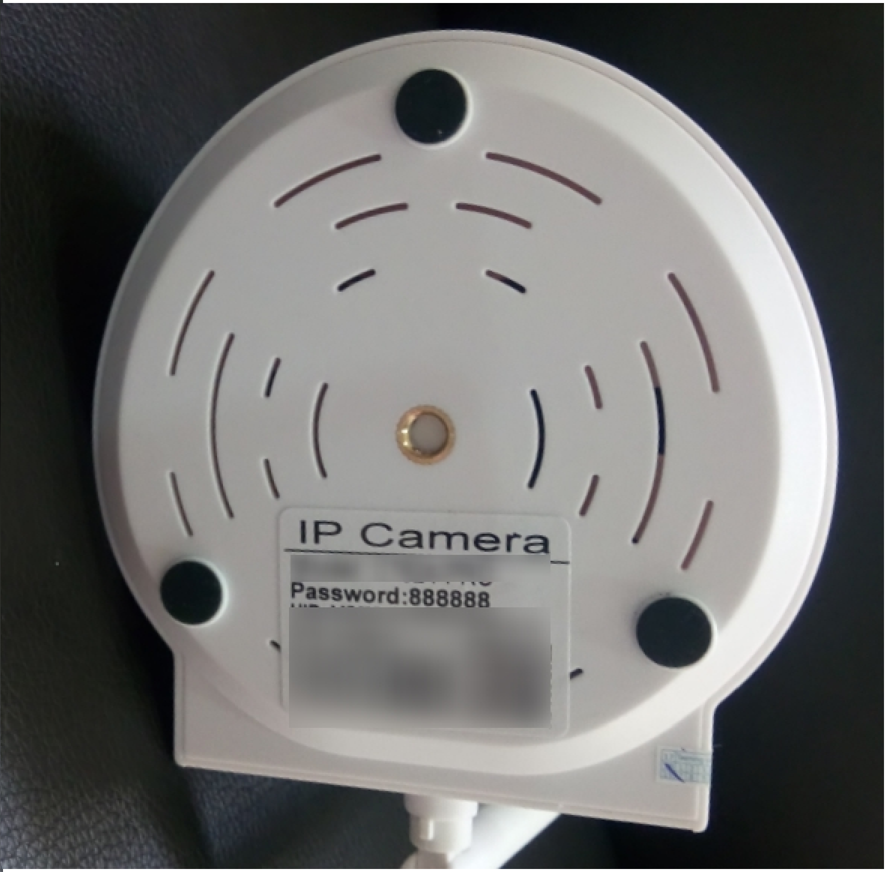
Possible Attacks on Bootstrapping

- 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***

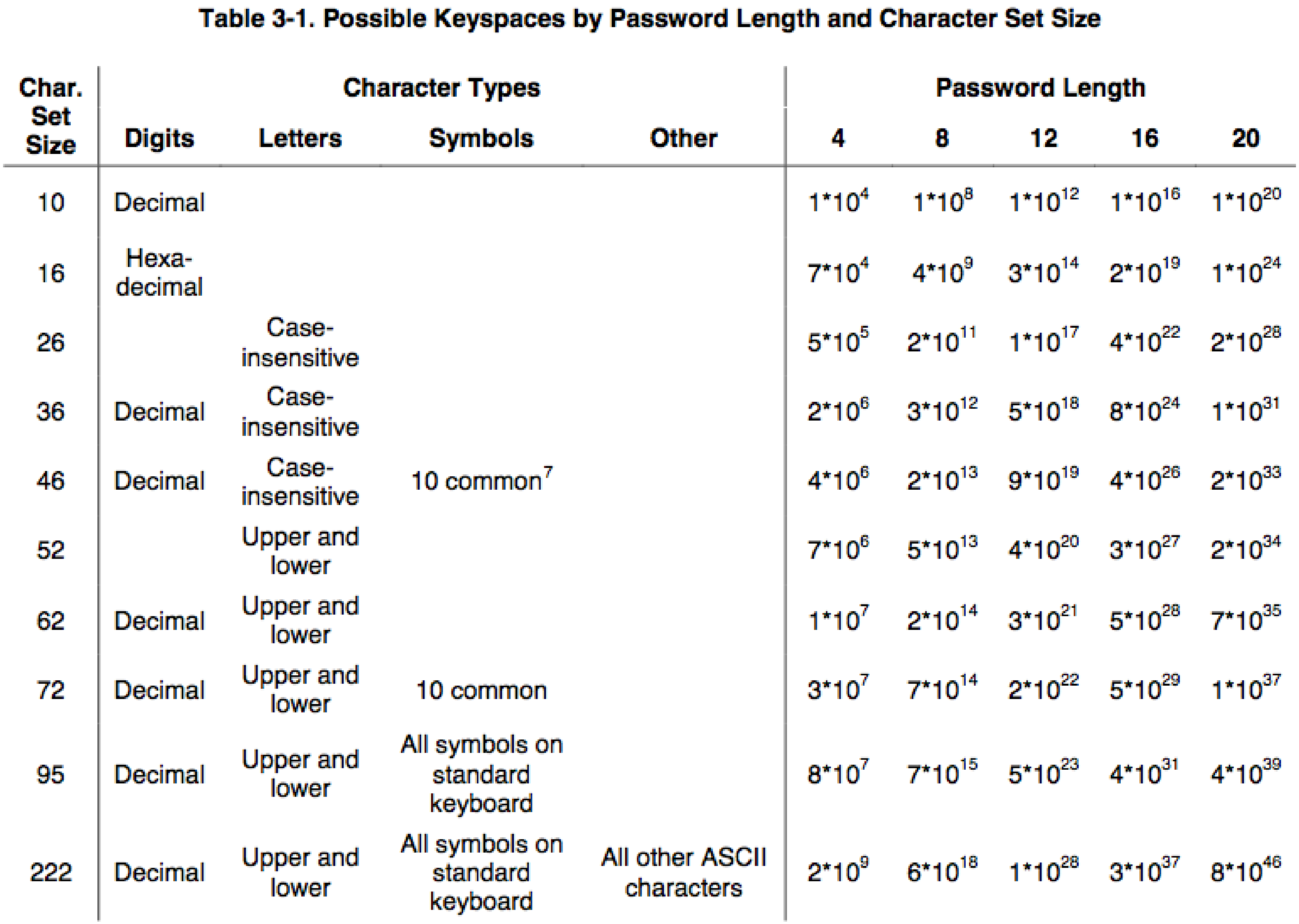


Table 3-1. Possible Keyspaces by Password Length and Character Set Size

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

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

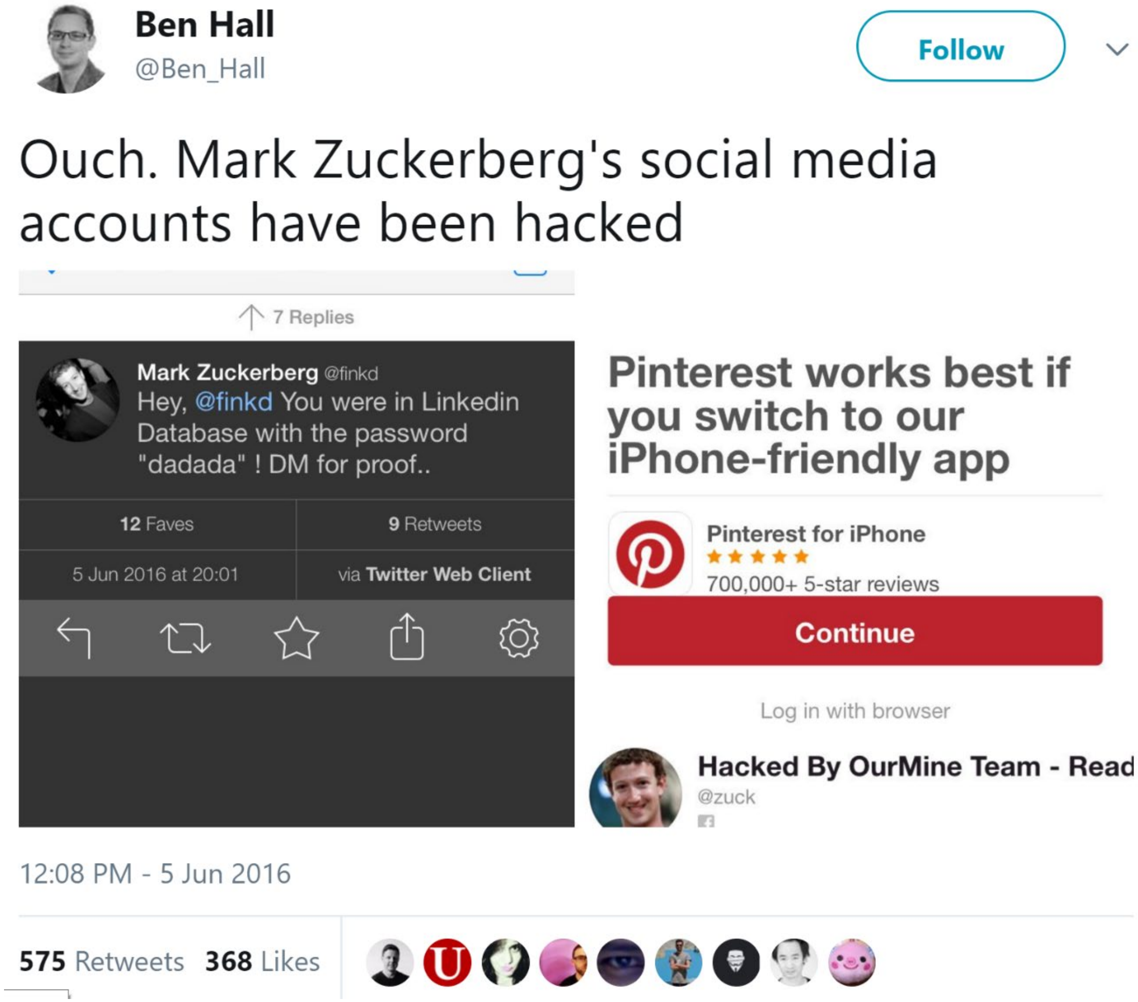
Question: Download a password dictionary.
Is your password listed in the dictionary?

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 Faves | **9** Retweets
5 Jun 2016 at 20:01 | via **Twitter Web Client**

Pinterest works best if you switch to our iPhone-friendly app

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: ******

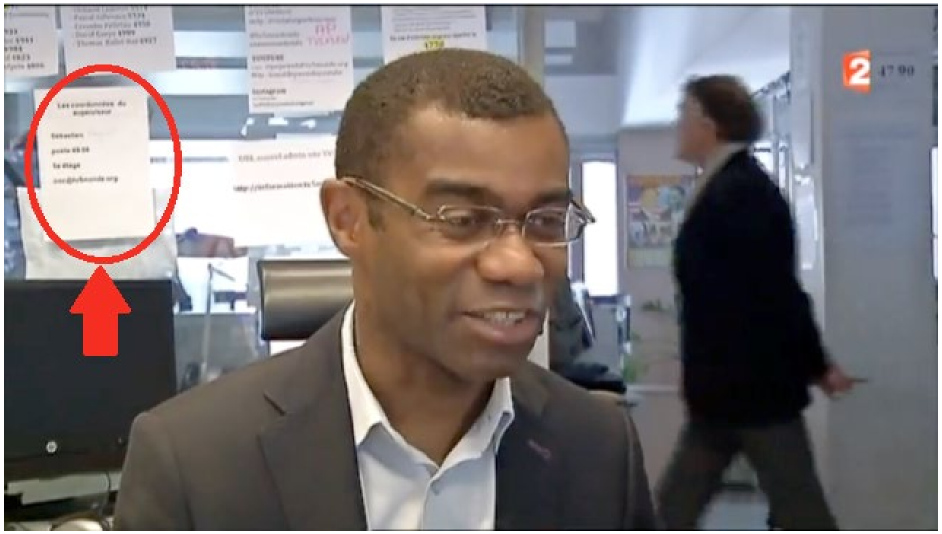
2.2.3 Stealing the Password

Shoulder Surfing, Sniffing

- ***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



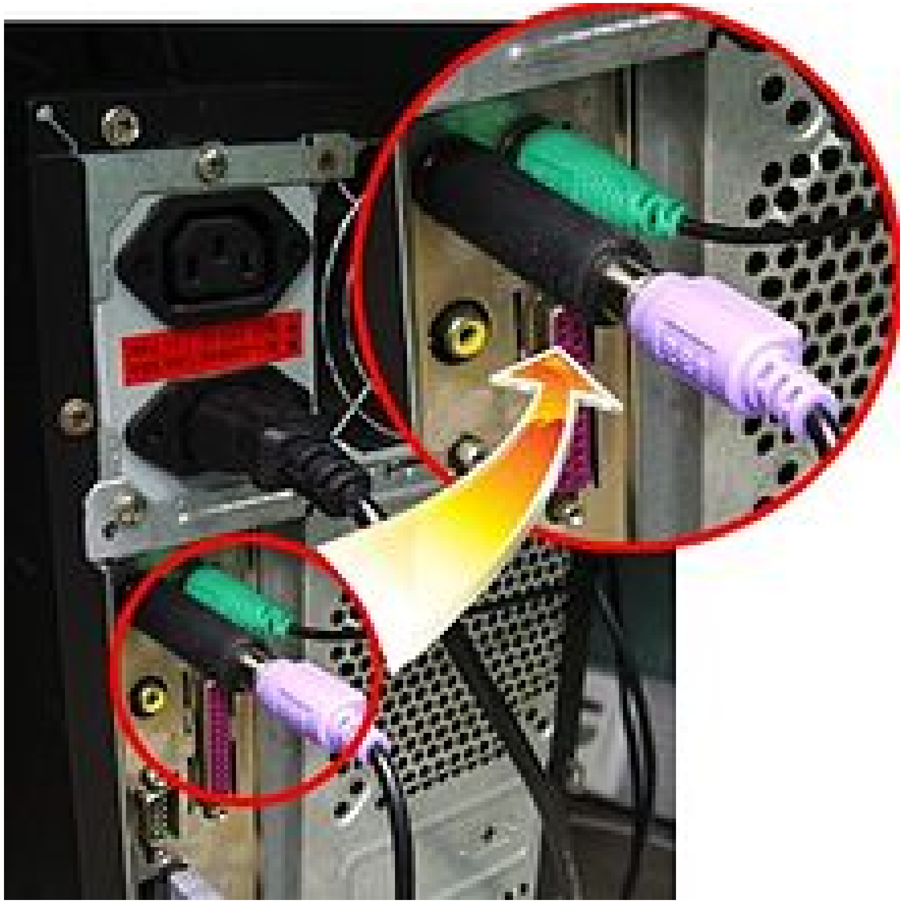
http://securityaffairs.co/wordpress/35856/cyber-crime/tv5monde-investigation-details.html
http://www.bbc.com/news/world-europe-32248779

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

Key-Logger

- A ***key-logger*** 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 ***key-logger***
- By **hardware**:
  Hardware key-logger: see the next slide for an example
- **See** "Hardware-based keyloggers" in
  http://en.wikipedia.org/wiki/Keystroke_logging

Hardware Key-Logger

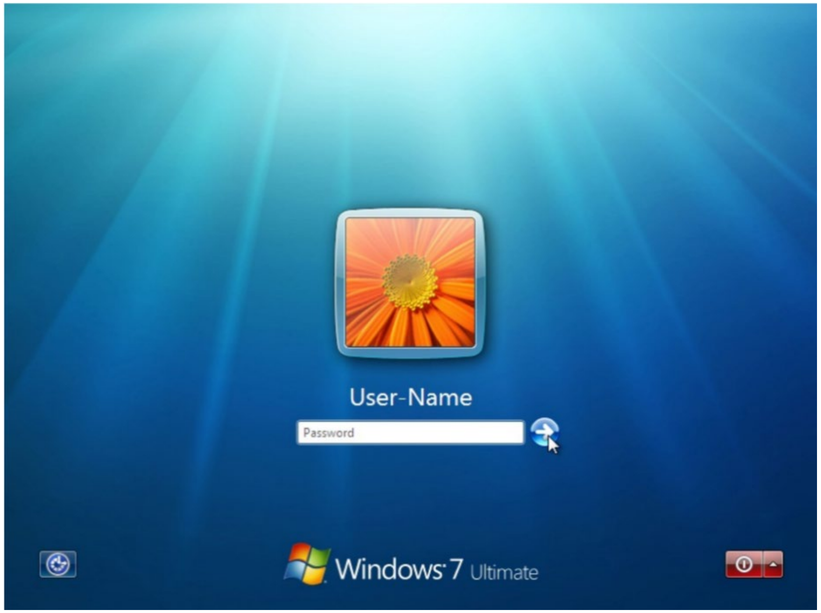


From http://en.wikipedia.org/wiki/Keystroke_logging

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

Login Spoofing

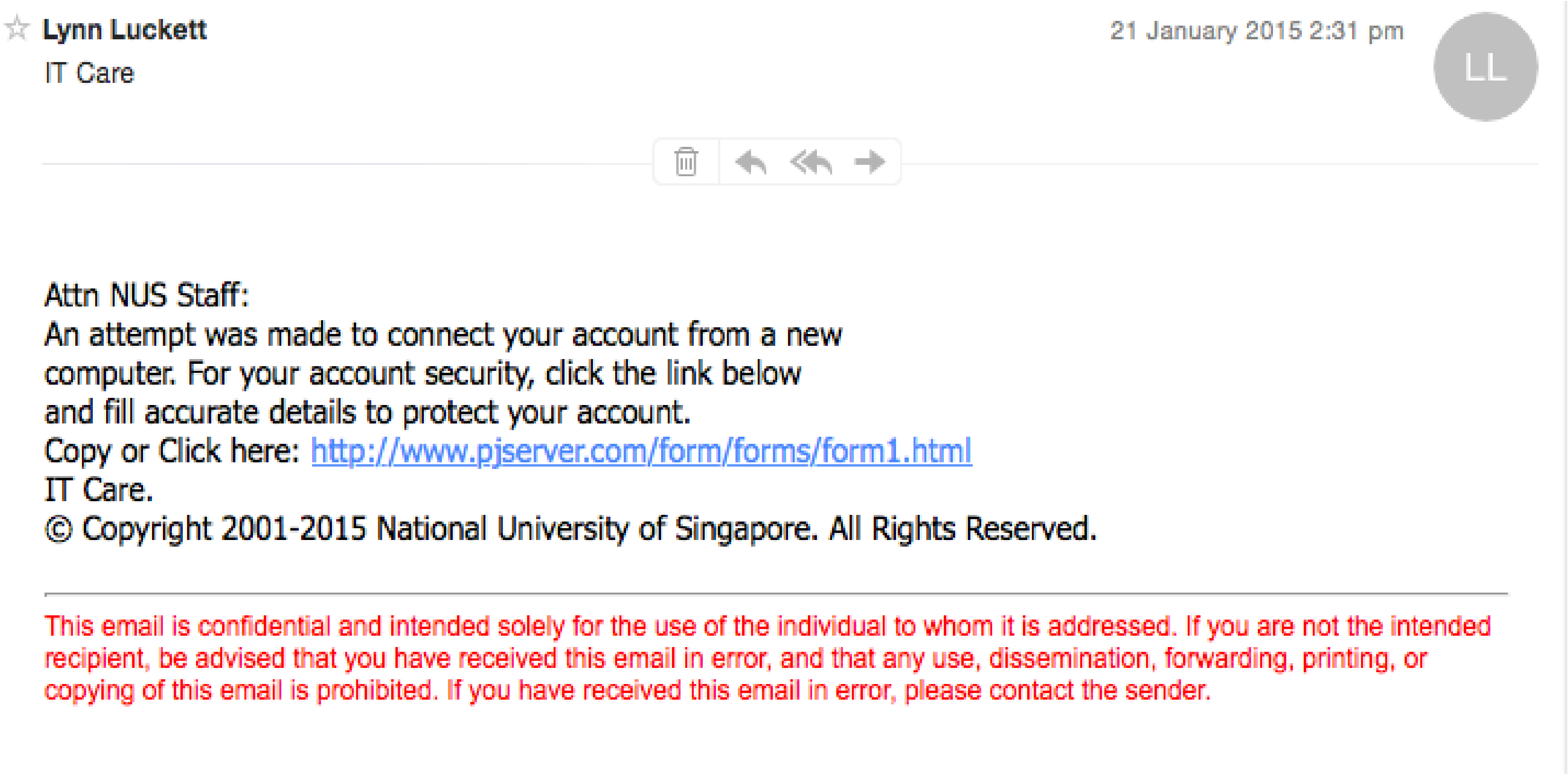
- Attacker displays a “spoofed” (fake) login screen



- 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

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:



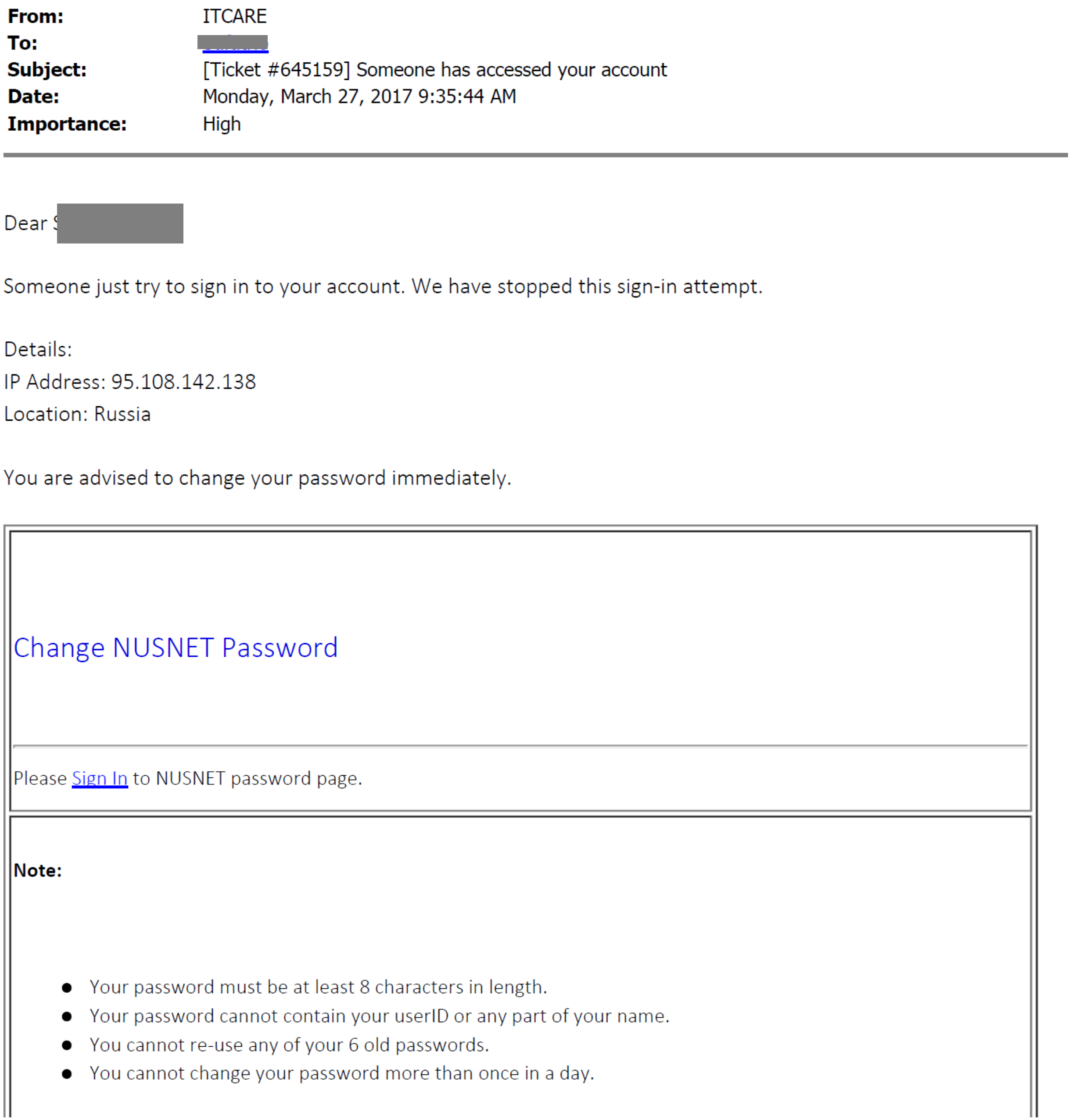
☆ **Lynn Luckett**
IT Care

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.

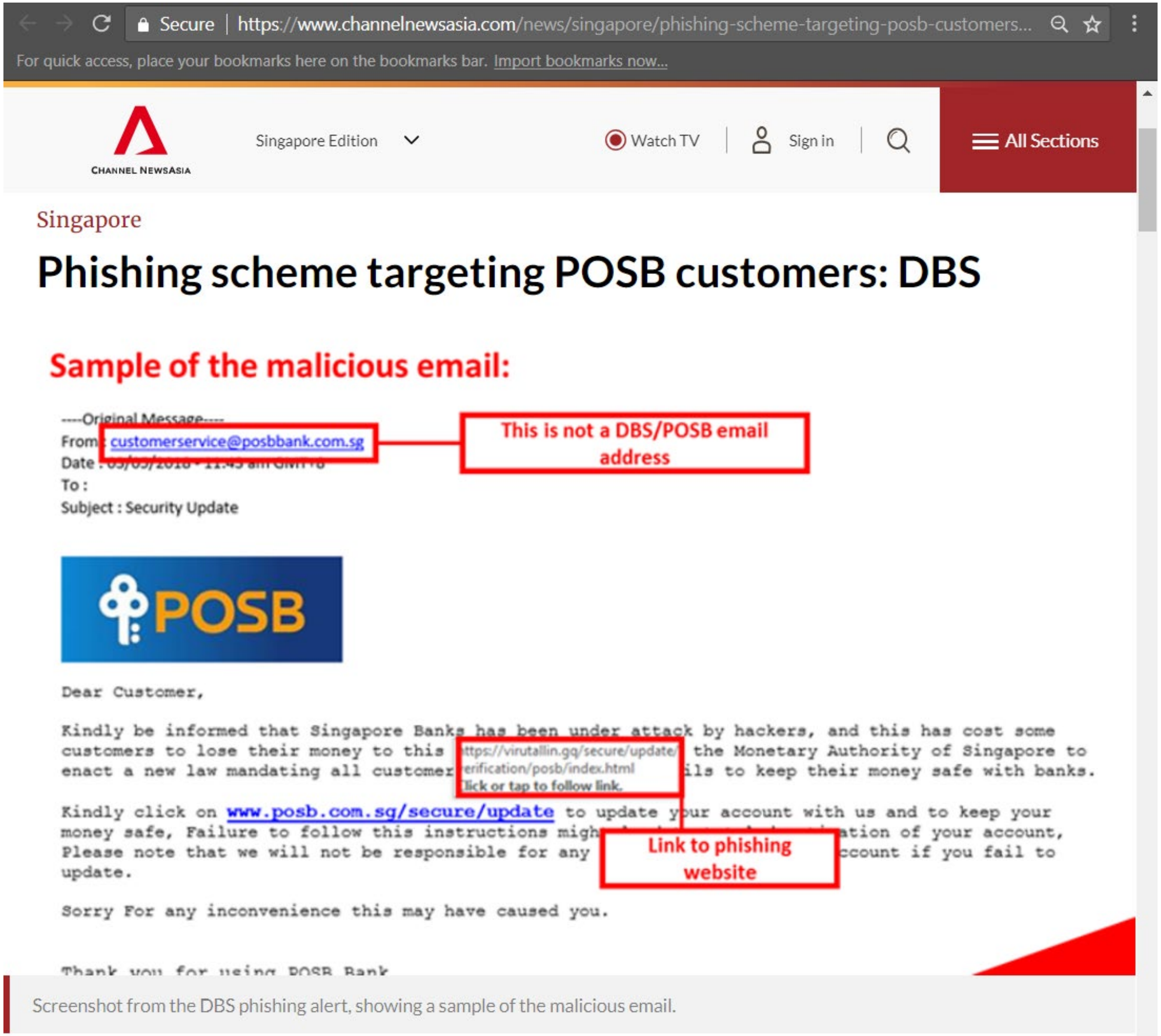
Change NUSNET Password

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


Secure
https://www.channelnewsasia.com/news/singapore/phishing-scheme-targeting-posb-customers...
For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...
CHANNEL NEWSASIA
Singapore Edition
Watch TV
Sign in
All Sections

Singapore

Phishing scheme targeting POSB customers: DBS

Sample of the malicious email:

----Original Message----
From : customerservice@posbbank.com.sg
Date : 05/05/2018 - 11:43 am GMT+8
To :
Subject : Security Update

This is not a DBS/POSB email address

Dear Customer,

Kindly be informed that Singapore Banks has been under attack by hackers, and this has cost some customers to lose their money to this ttps://virutallin.gq/secure/update/ the Monetary Authority of Singapore to enact a new law mandating all customer erification/posb/index.html ils to keep their money safe with banks.
lick or tap to follow link.

Kindly click on www.posb.com.sg/secure/update to update your account with us and to keep your money safe, Failure to follow this instructions migh ation of your account, Please note that we will not be responsible for any ccount if you fail to update.

Link to phishing website

Sorry For any inconvenience this may have caused you.

Thank you for using POSB Bank

Screenshot from the DBS phishing alert, showing a sample of the malicious email.

From: Channel News Asia, 4 May, 2018

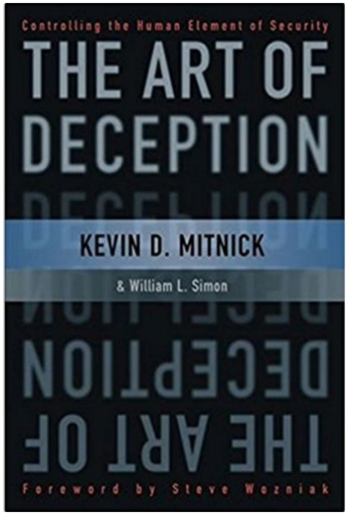
Spear Phishing

- 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

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


Controlling the Human Element of Security
THE ART OF DECEPTION
KEVIN D. MITNICK
& William L. Simon
Foreword by Steve Wozniak

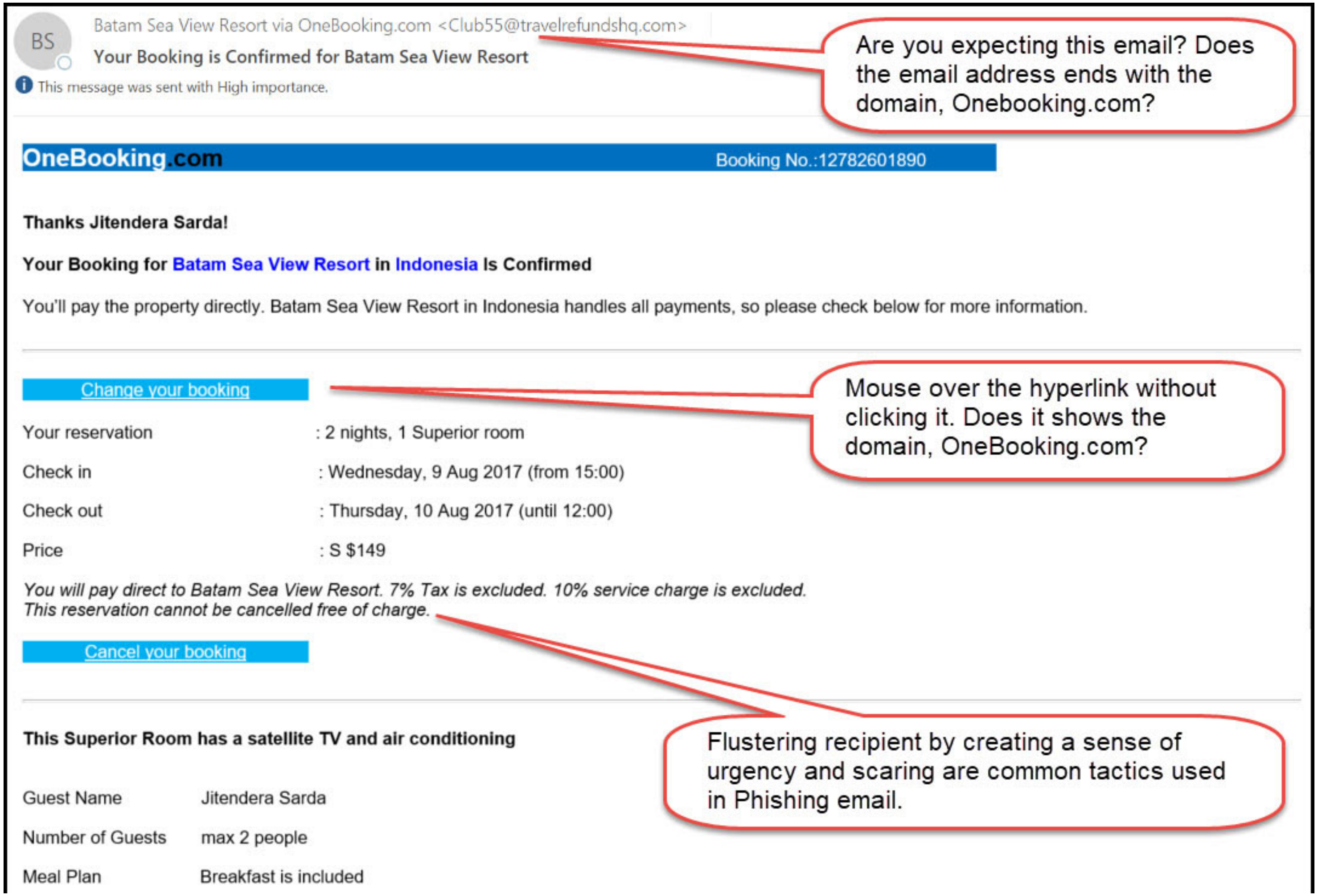
Question (Terminology):

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

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

Preventing Phishing

- User education: phishing drill



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.

Are you expecting this email? Does the email address ends with the domain, Onebooking.com?

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.

Mouse over the hyperlink without clicking it. Does it shows the domain, OneBooking.com?

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.

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

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

From: NUS IT Care

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!?

From: NUS IT Care

Password Caching

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

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 lost 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
  - 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?

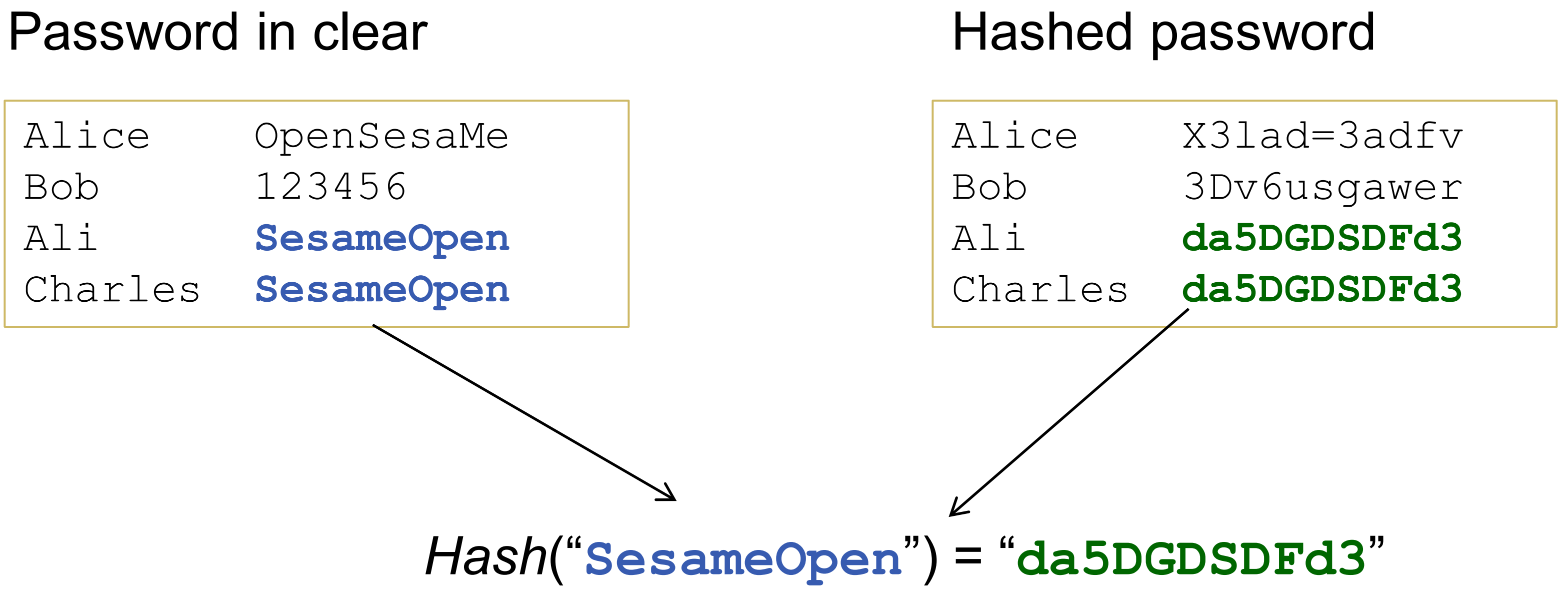
Protecting Password File

- 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 (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**

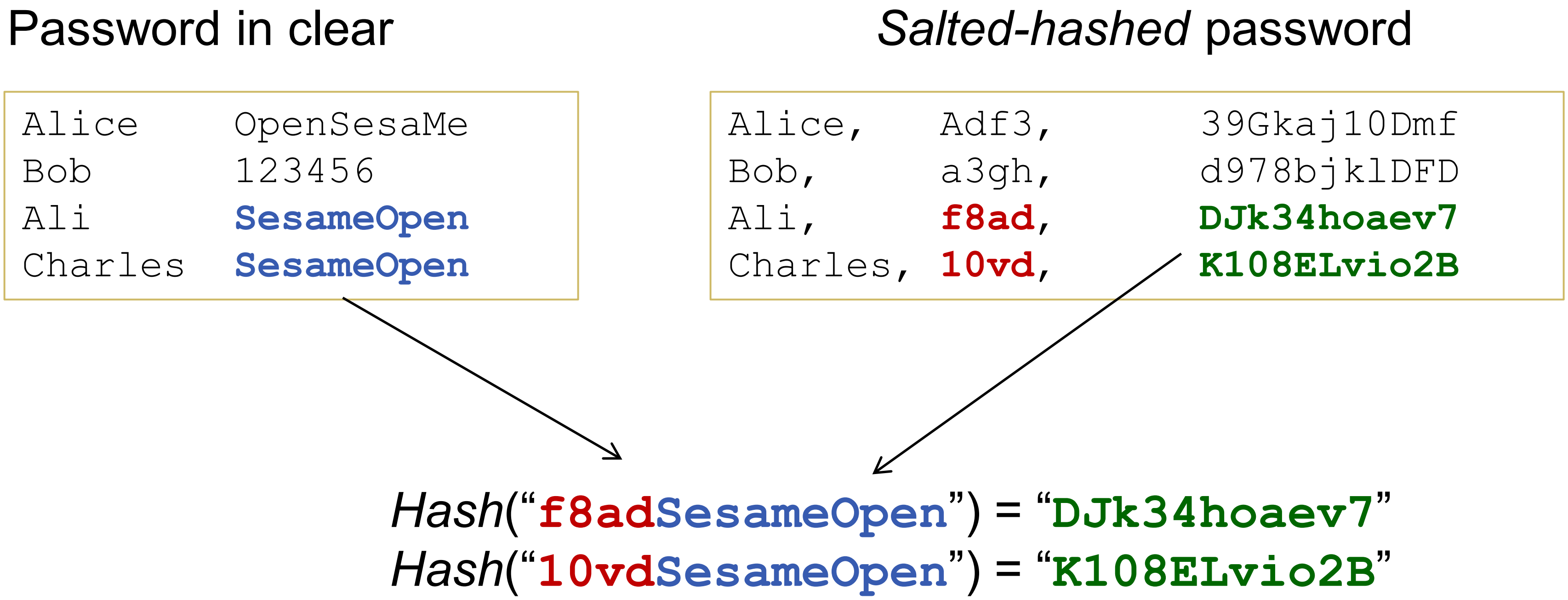
Hashed password

Alice	X31ad=3adfv
Bob	3Dv6usgawer
Ali	**da5DGDSDFd3**
Charles	**da5DGDSDFd3**

Hash(“**SesameOpen**”) = “**da5DGDSDFd3**”

Hashed Password (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? (See tutorial)
- 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**

Hash("**f8adSesameOpen**") = "**DJk34hoaev7**"

Hash("**10vdSesameOpen**") = "**K108ELvio2B**"

2.2.5 Security Questions

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

Optional:
Ariel Rabkin, "*Personal Kowledge 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)

- ***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)

Question: Give example of "bad" security questions

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 ☺

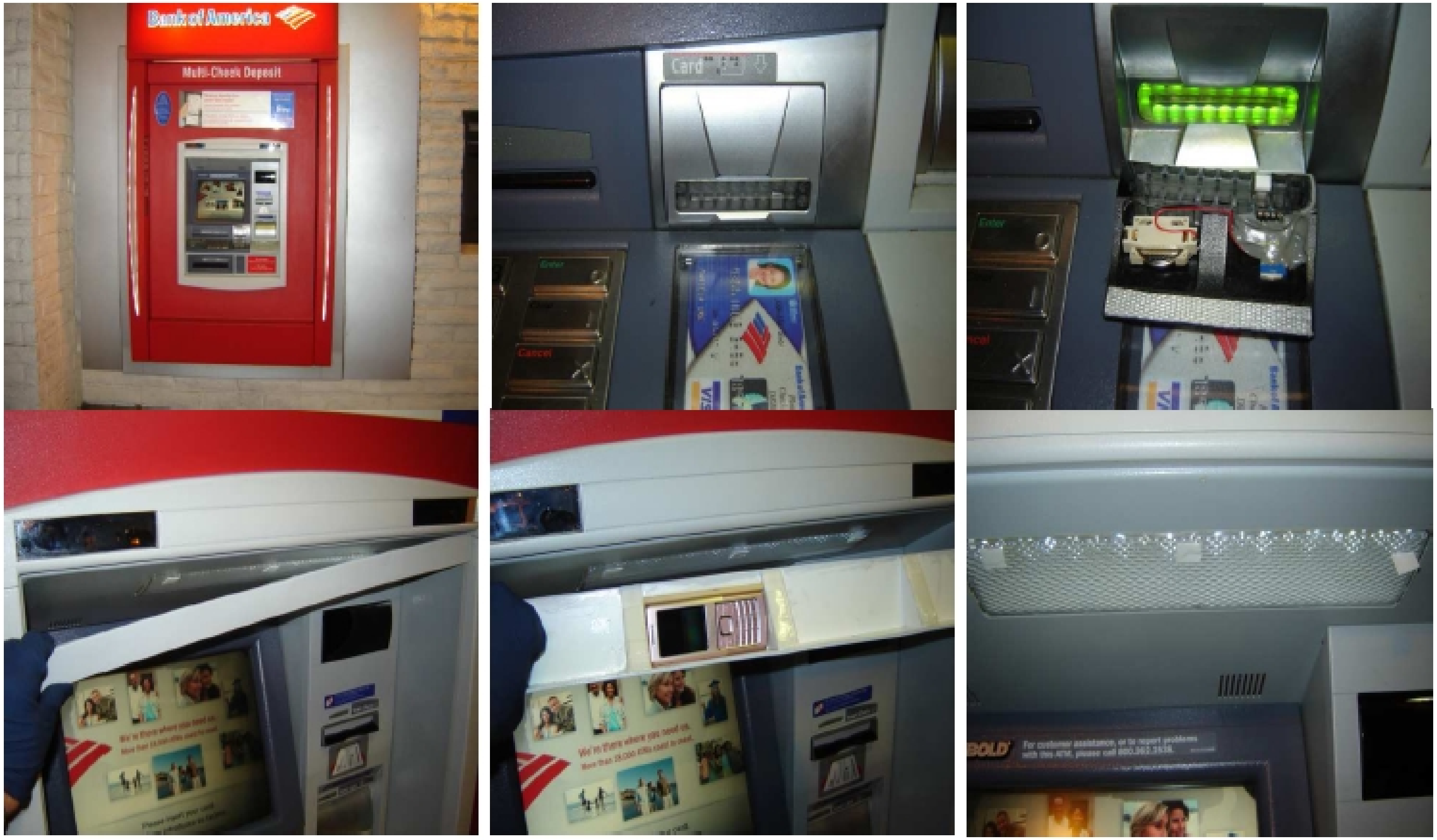
http://colnect.com/en/bank_cards/bank_card/4130-ATM_Card-Bank_of_America-United_States

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
  (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

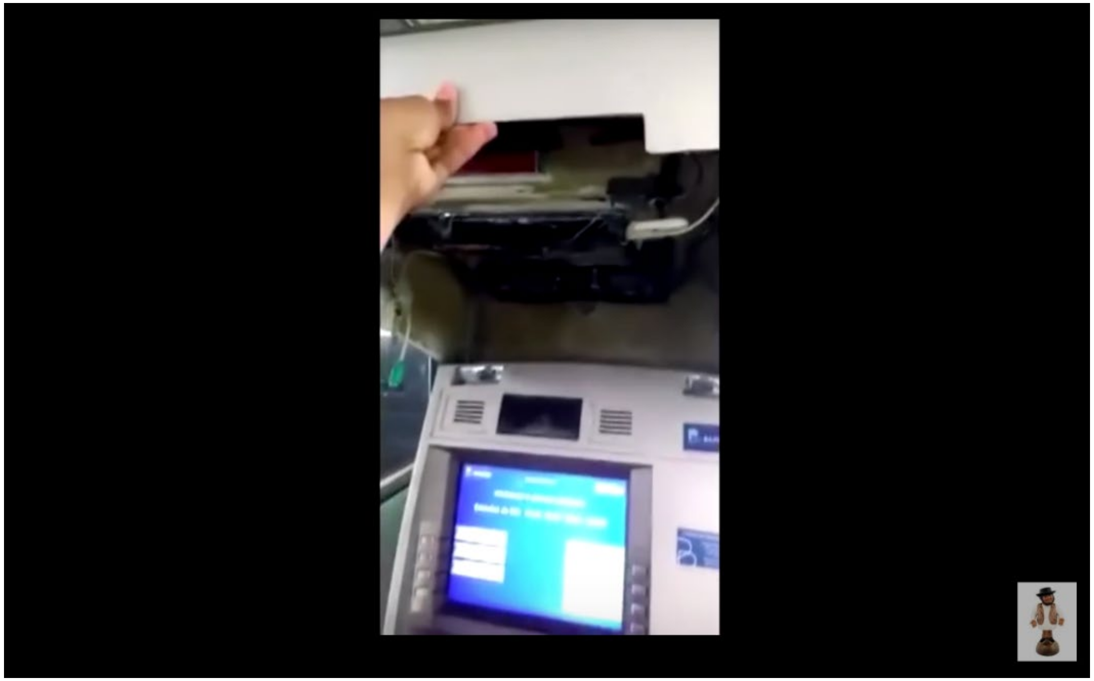


Synopsis:

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

Fun Video to Watch: Very Big ATM Skimmer

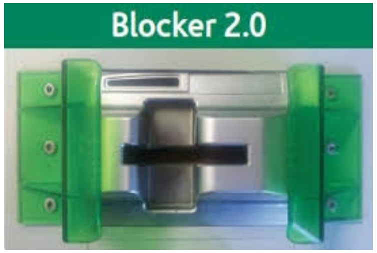


https://www.liveleak.com/view?i=bea_1457038390

Another (really big) ATM skimmer!

Preventive Measures

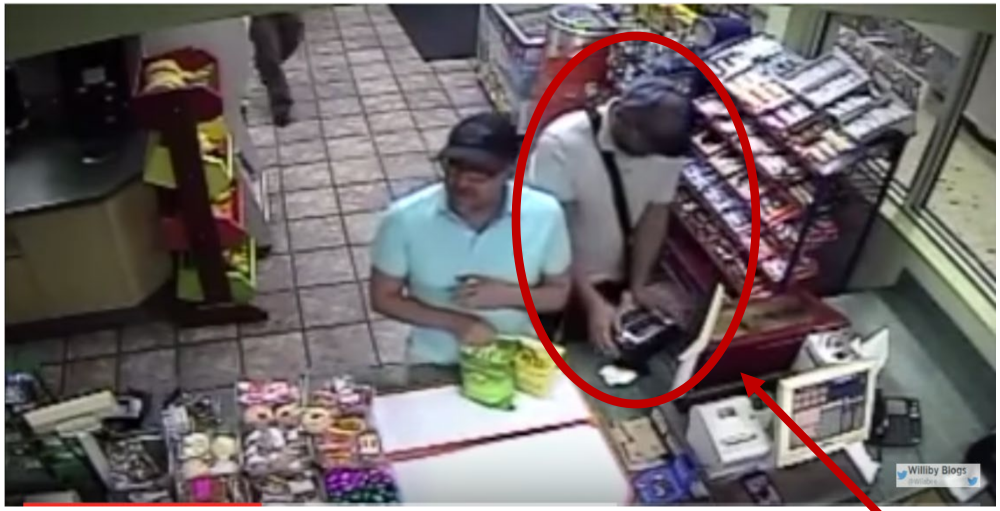
- Install **anti-skimmer device**: a device that prevents external card reader to be attached onto the ATM



- **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

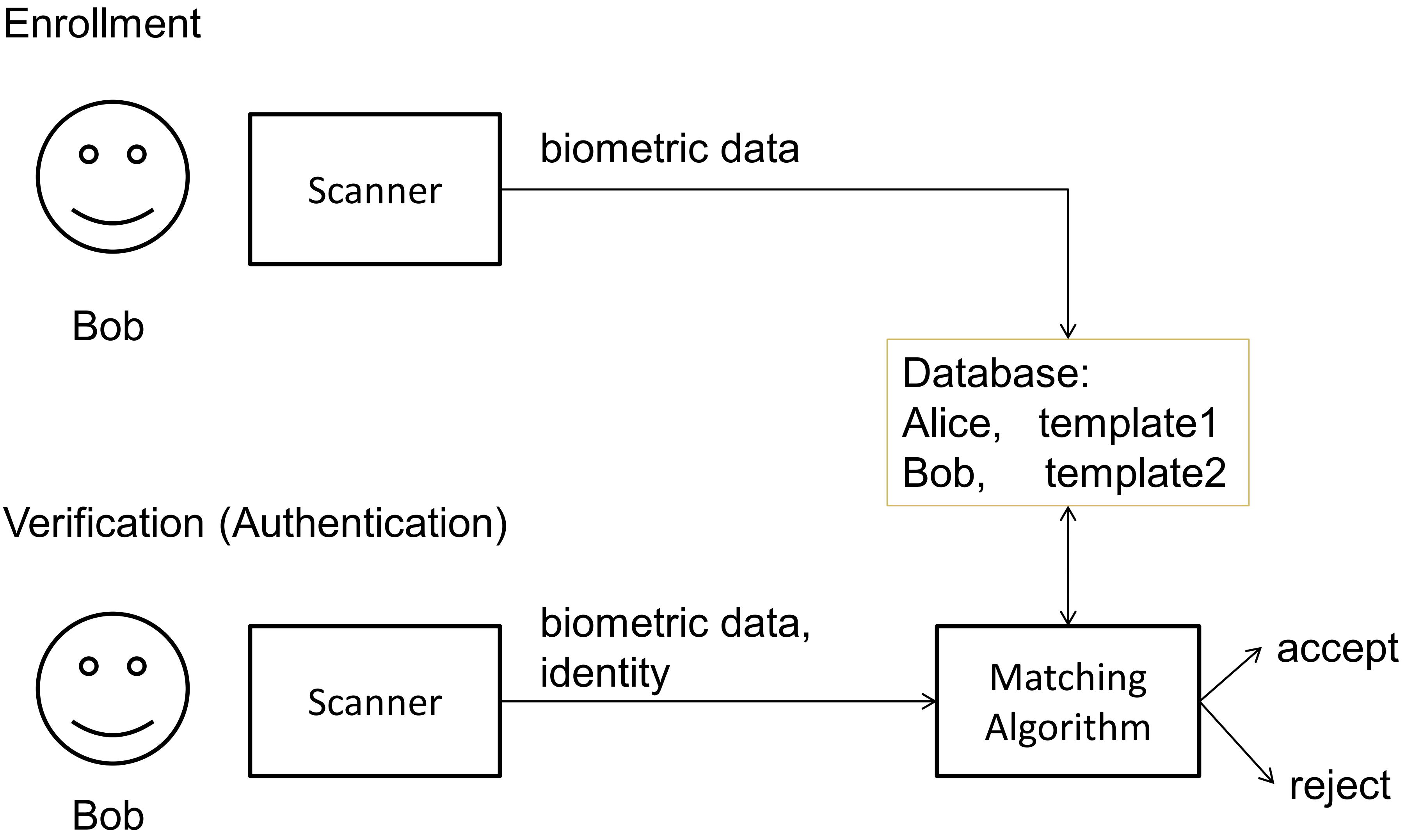
Reading:

[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

Bob

Scanner

biometric data

Database:
Alice, template1
Bob, template2

Verification (Authentication)

Bob

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

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)

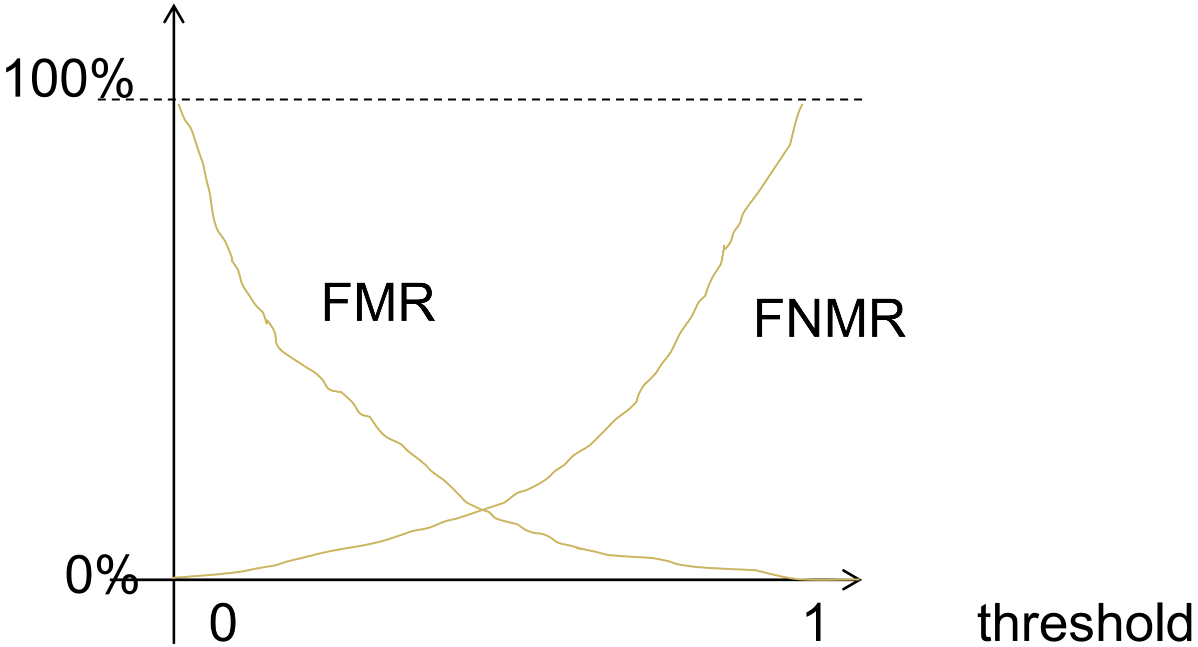
$$\textbf{FMR} = \frac{\text{number of successful false matches } (B)}{\text{number of attempted false matches } (B+D)}$$

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

	accepted/ match	rejected/ non-match
genuine attempt	***A***	***C***
false attempt	***B***	***D***

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

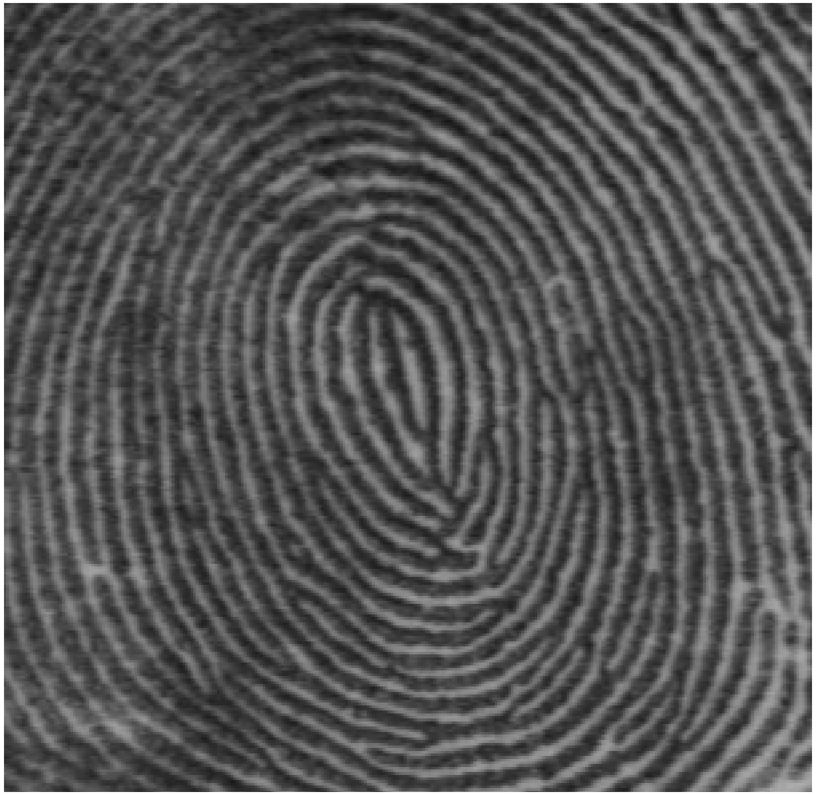
Failure-to-enroll rate (FER):

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

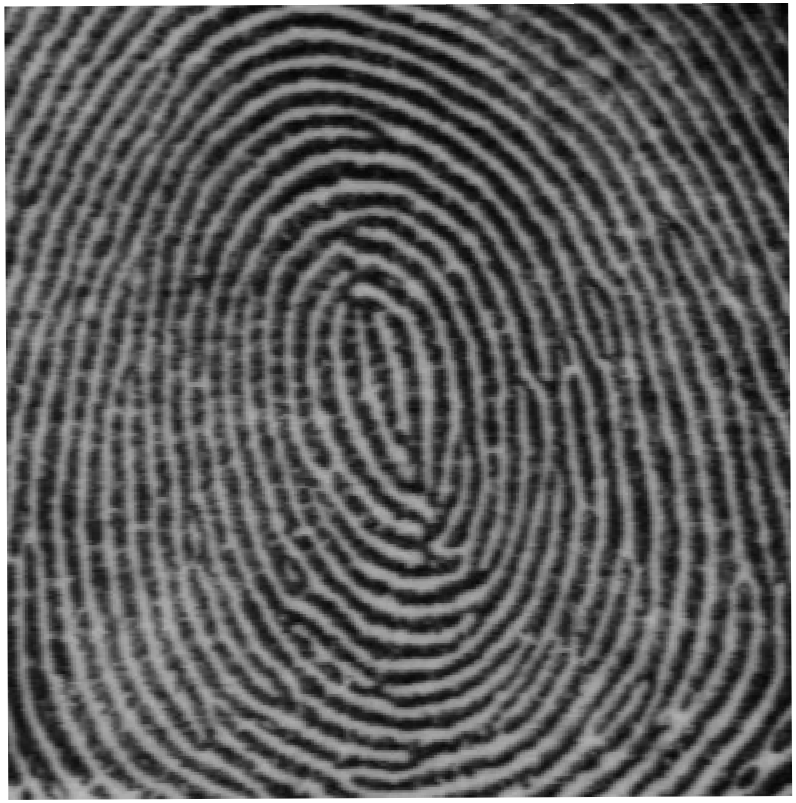
Failure-to-capture rate (FTC):

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

Examples on Fingerprint

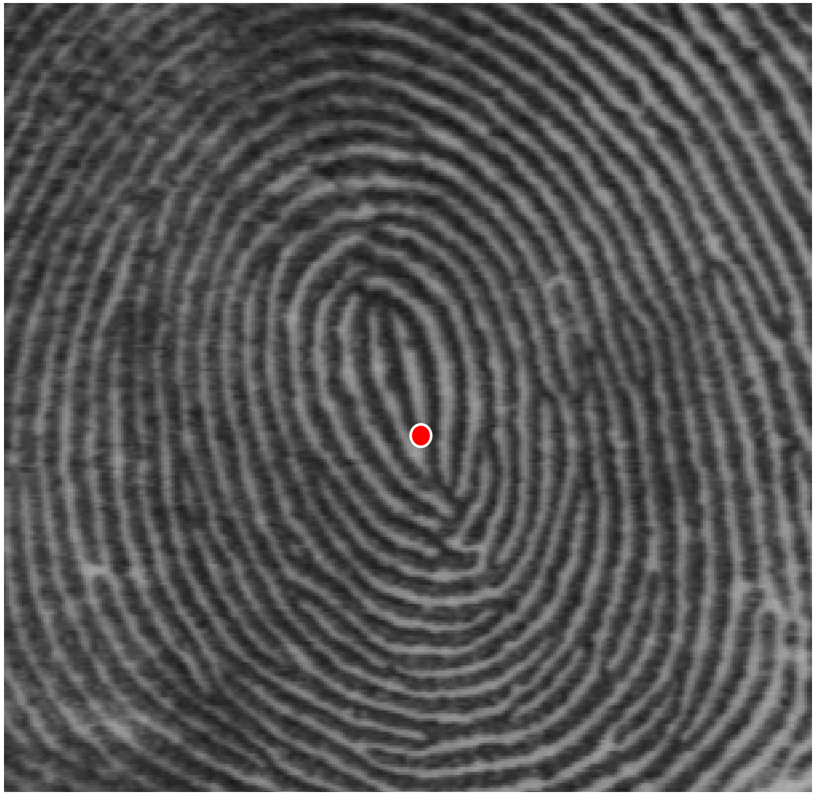


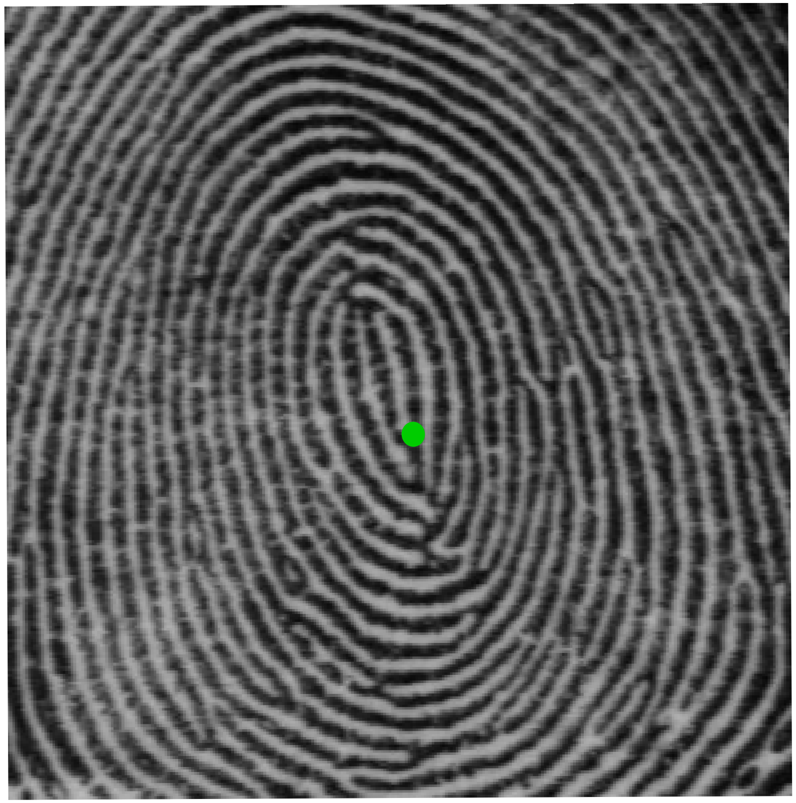
First scan of a finger



Another scan
of the same finger

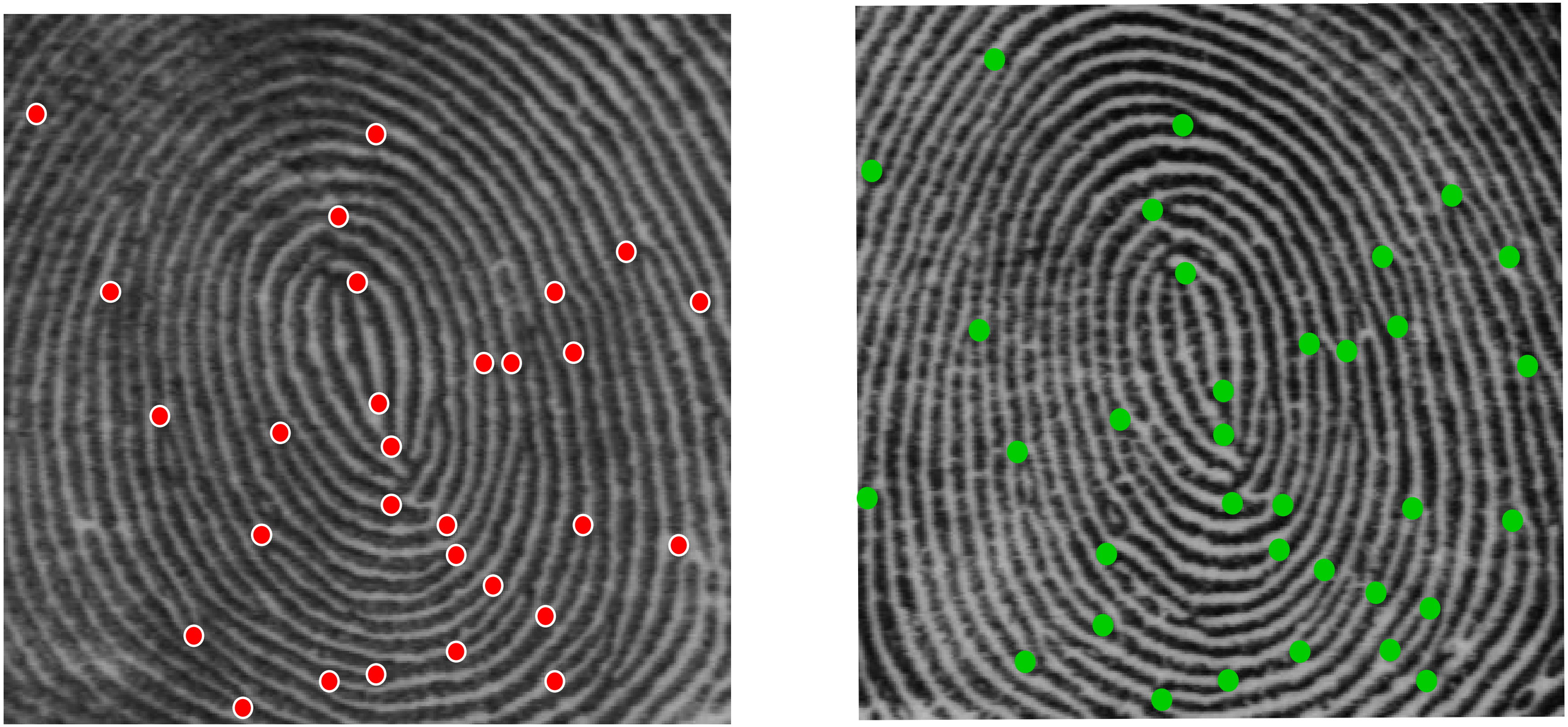
Fingerprint: Background





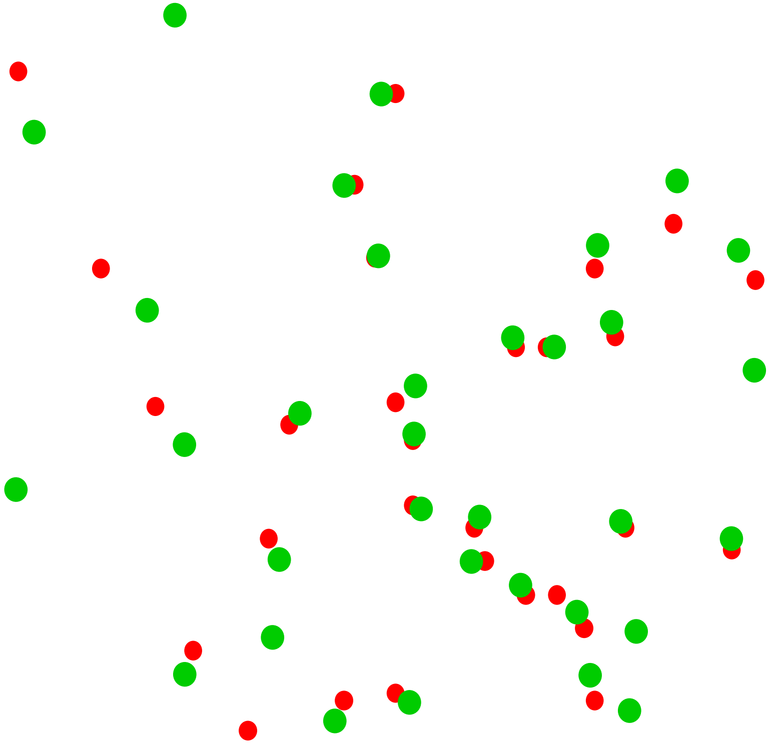
A feature point

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*!



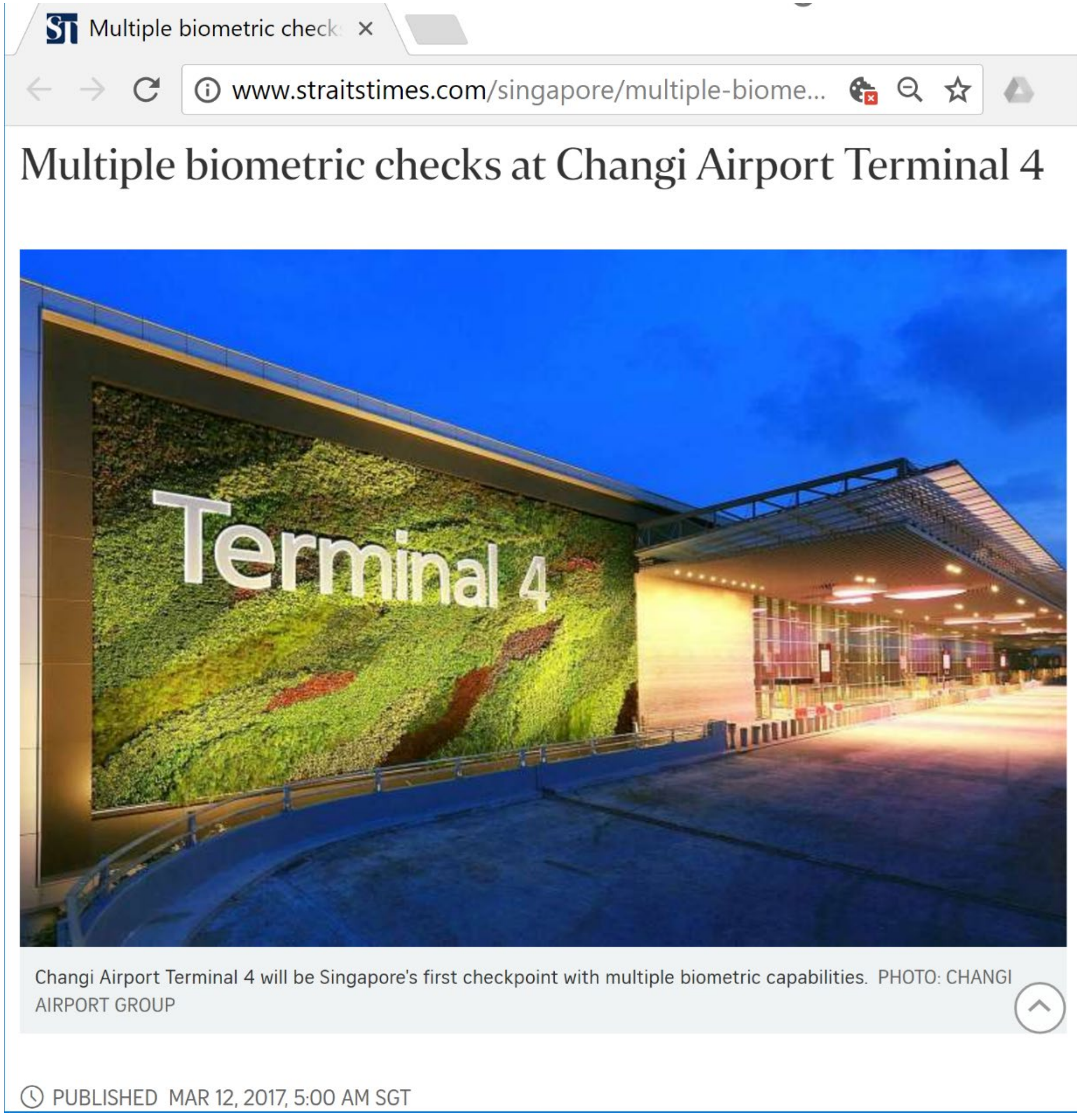
How Good is Fingerprint as a Biometric?

- Performance depends on the quality of the scanner
- 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

Other Forms of Biometrics

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

The Straits Times,
Mar 12, 2017



Multiple biometric check ×

www.straitstimes.com/singapore/multiple-biome...

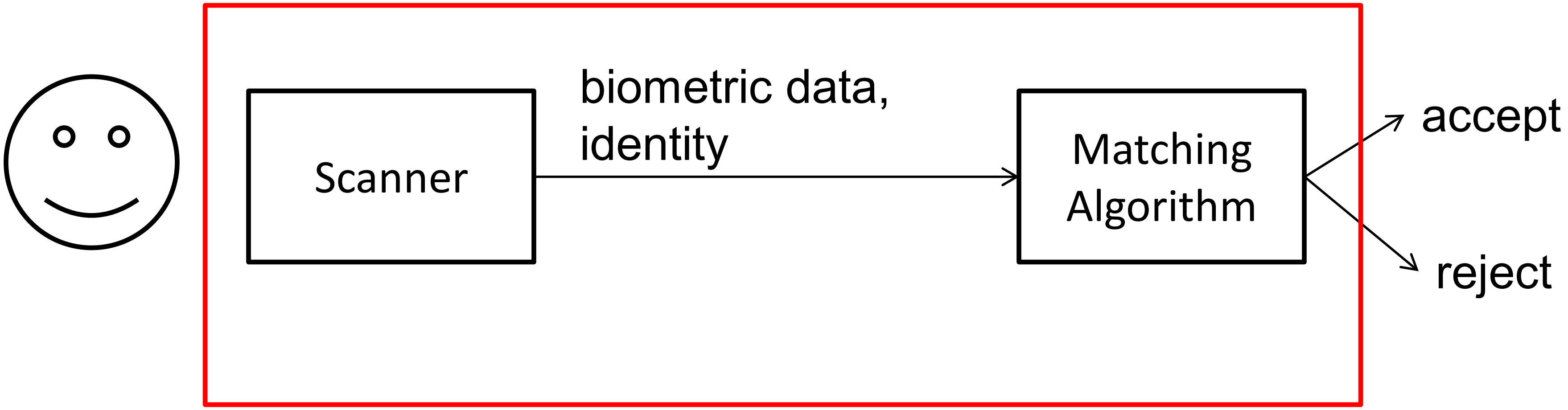
Multiple biometric checks at Changi Airport Terminal 4

Changi Airport Terminal 4 will be Singapore's first checkpoint with multiple biometric capabilities. PHOTO: CHANGI AIRPORT GROUP

PUBLISHED MAR 12, 2017, 5:00 AM SGT

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

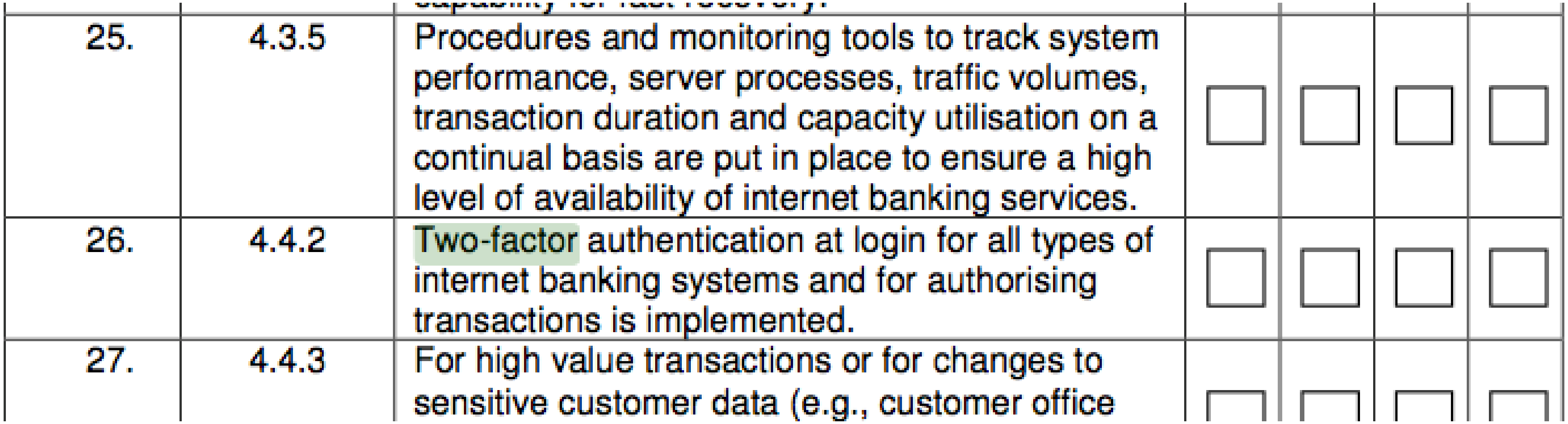
- Require at least two different authentication “factors”
- Commonly-used factors:

1.	What you know:	password, PIN
2.	What you have:	smart card, ATM card, mobile phone, security/OTP token
3.	Who you are:	biometrics

- Other possible factors [Gollmann]:
  1. where you are
  2. what you do
- 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

MAS Compliance Checklist

- 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



		capability for fast recovery.				
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	□	□	□	□

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:

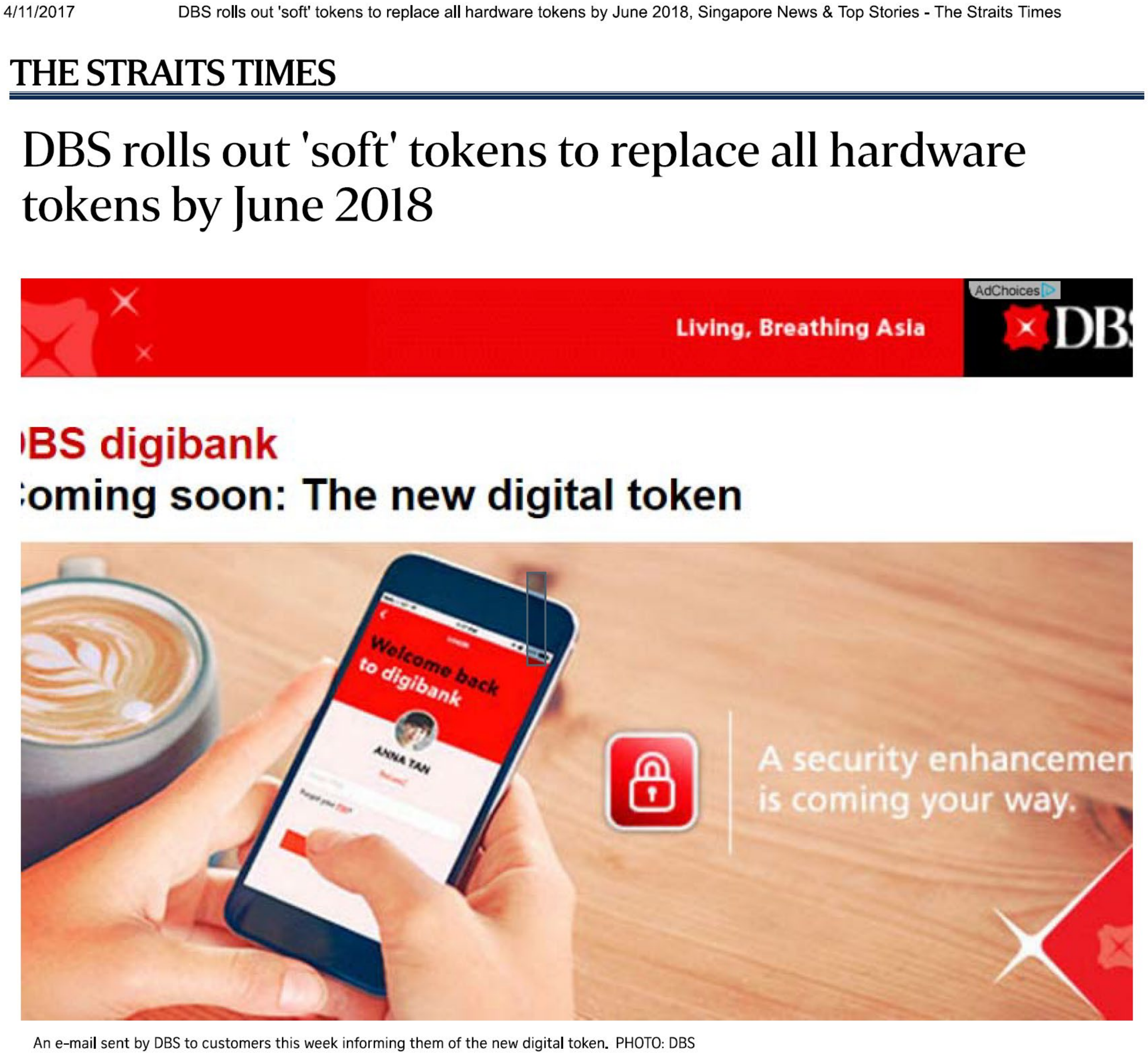
(1) User “presses” the token, which then computes and displays a one-time-password (OTP)

(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!



THE STRAITS TIMES

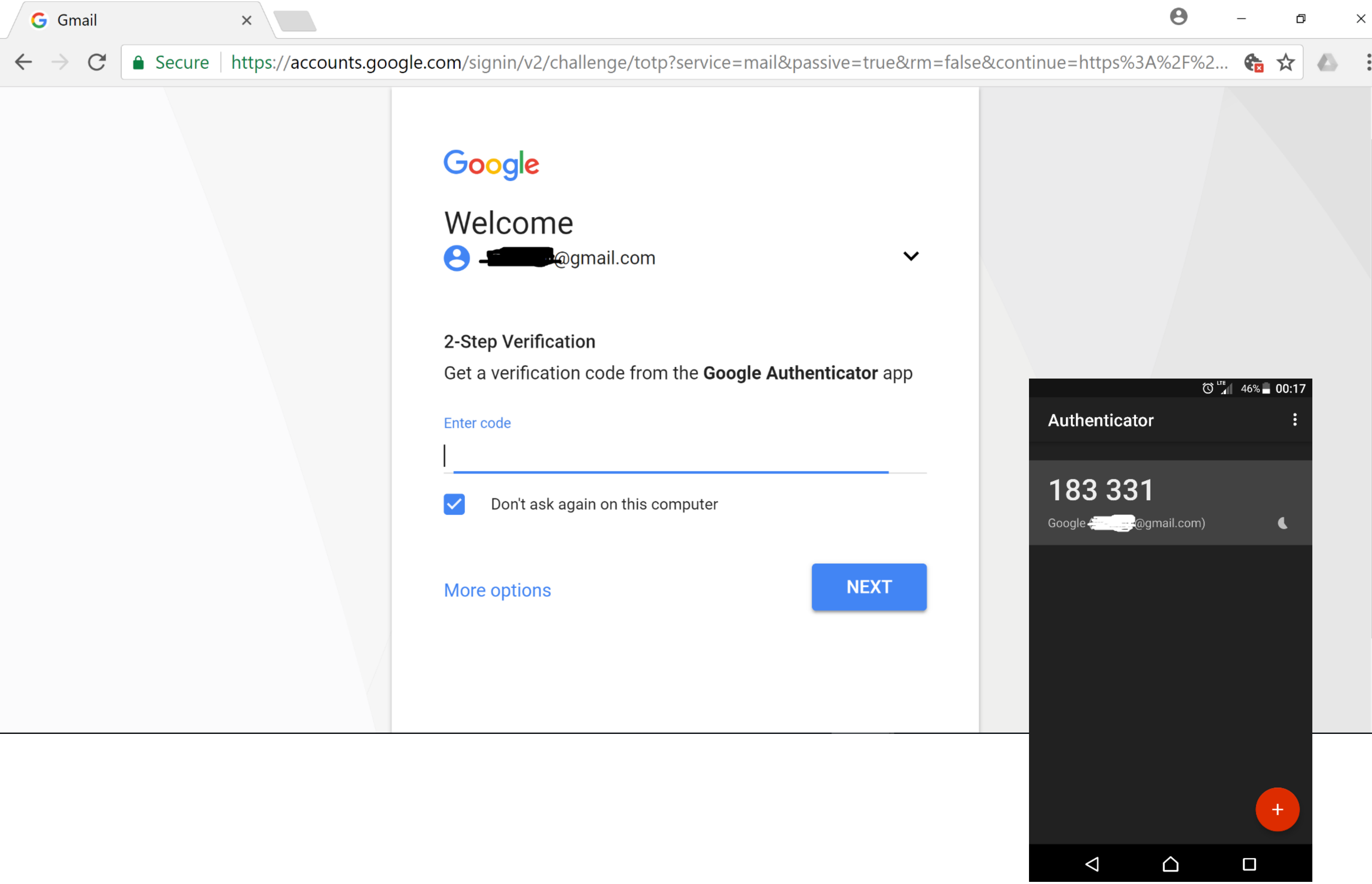
DBS rolls out 'soft' tokens to replace all hardware tokens by June 2018

BS digibank

oming 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



https://accounts.google.com/signin/v2/challenge/totp?service=mail&passive=true&rm=false&continue=https%3A%2F%2...

Google

Welcome

[redacted]@gmail.com

2-Step Verification

Get a verification code from the **Google Authenticator** app

Enter code

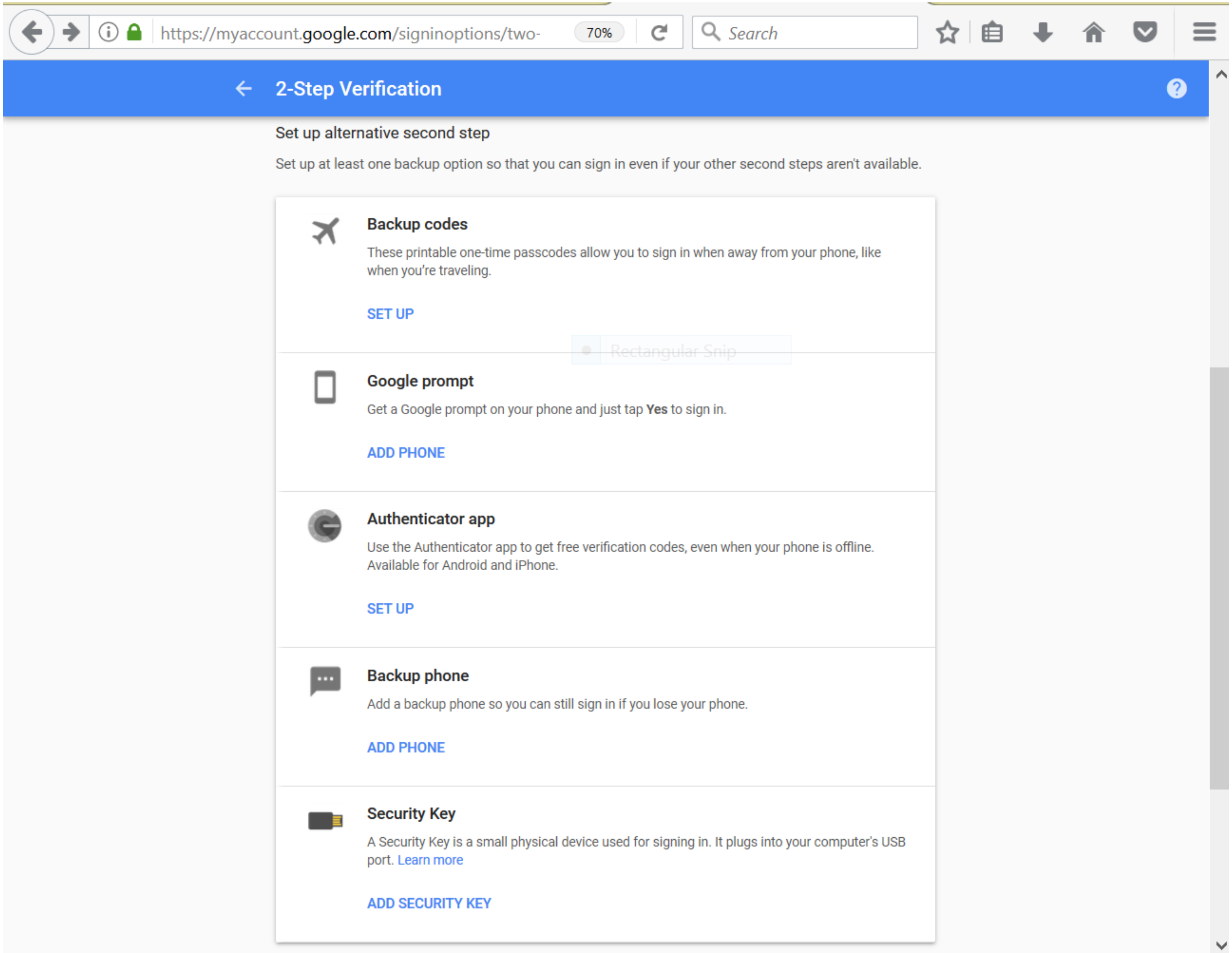
☑ Don't ask again on this computer

Authenticator

183 331

Google ([redacted]@gmail.com)

Another New Trend of OTP Token: Authenticator App Setting



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

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

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

- 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

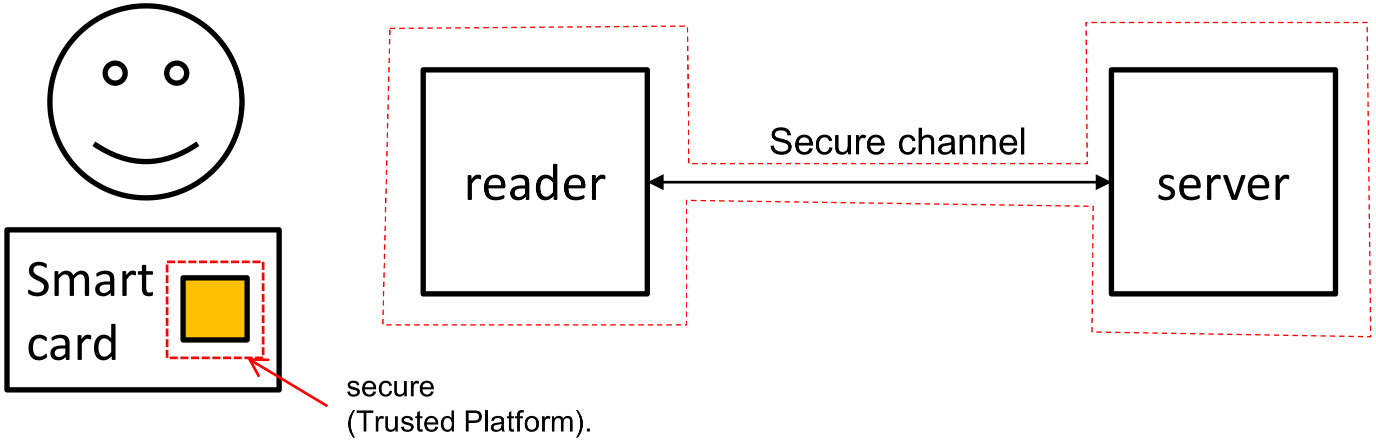
Authentication:

(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 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?

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?