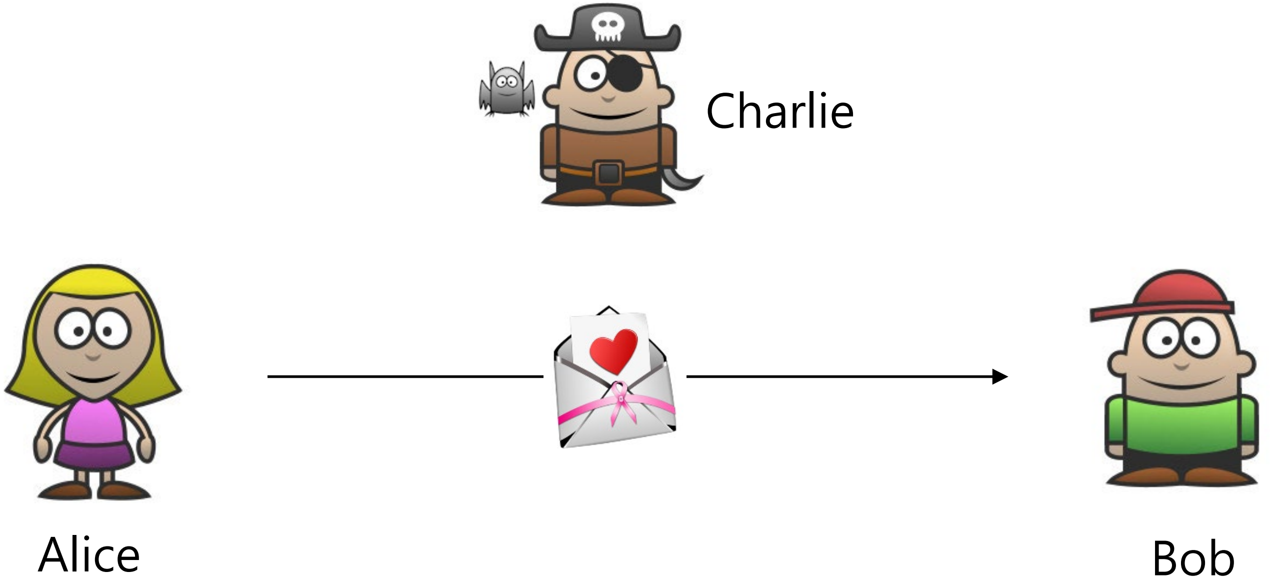
Chapter 15
User Authentication

→

정보보안

Authentication

- Security goals
  - Confidentiality: Only Bob should be able to read the message.
  - Integrity: The message should not be modified en route.
    무결성 데이터가 변경되어
  - Non-repudiation: Alice should not be able to deny her writing the message. 부인방지 ex) 전자서명
  - ☆ Authentication: Alice can confirm that the communicating party is indeed Bob. 주장하고 있는 신분이 맞는.



Authentication

- Definition
  - Authentication (from Greek αὐθεντικός, “real or genuine” and from αὐθέντης, “author”) is the act of confirming the truth of an attribute of a datum (data) or entity.
  - It might involve confirming the identity of a person by validating their identity documents, verifying the validity of a website with a digital certificate, tracing the age of an artifact by carbon dating, or ensuring that a product is what its packaging and labeling claim to be.

Keys

Hand signature

Hologram tags

Authentication Factors

- Authentication Factors
  - The ways in which someone may be authenticated fall into three categories, based on what are known as the factors of authentication: something the user *has*, something the user *knows*, and something the user *is*.

    가진것 알고있는것. 본질적인 것을 지문.얼굴인식 등
  - Each authentication factor covers a range of elements used to authenticate or verify a person's identity prior to being granted access, approving a transaction request, signing a document or other work product, granting authority to others, and establishing a chain of authority.

Authentication Factor (Ownership Factor)

- Ownership factors
  - Something the user has. 가지고 있으면 정당하다고 생각
  - E.g., wrist band, ID card, security token.

놀이동산 밴드

OTP

학생증

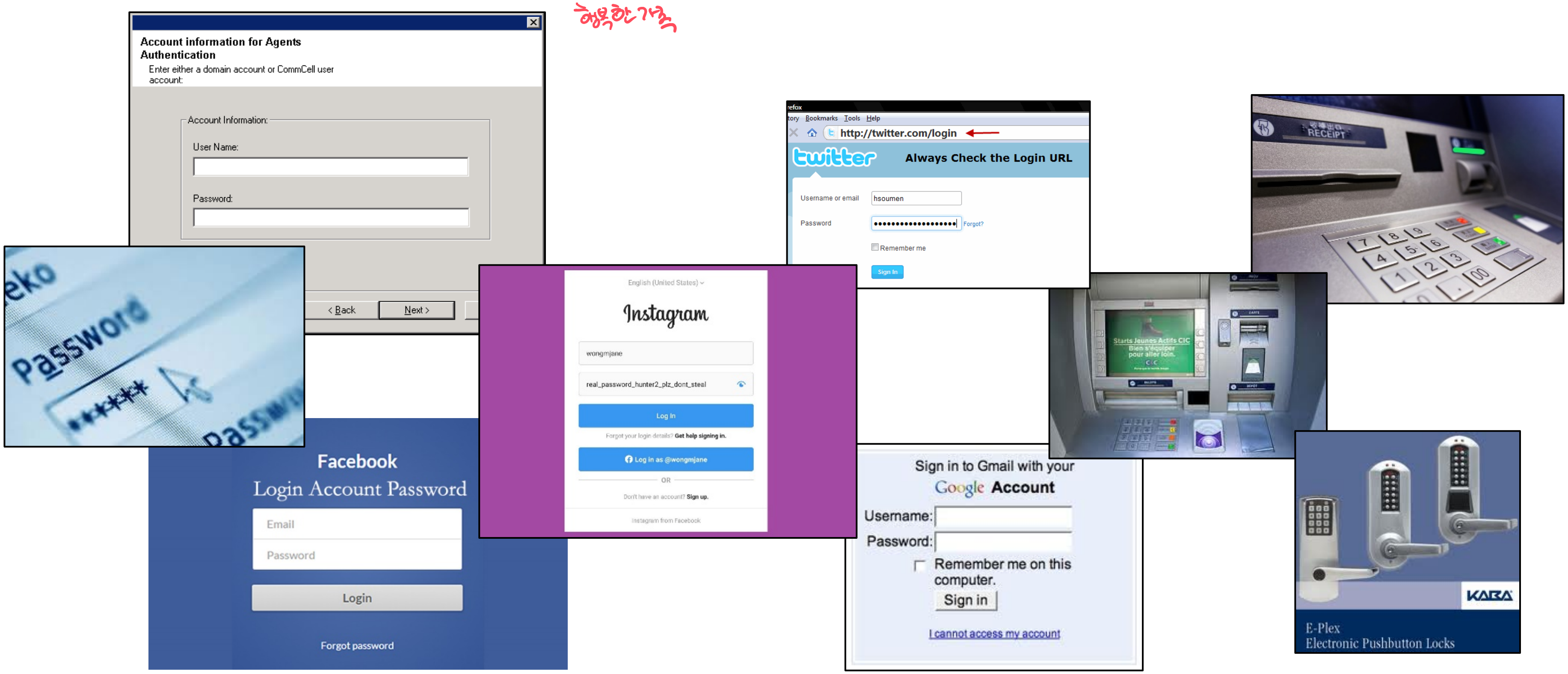
Authentication Factor (Knowledge Factor)

- Knowledge factors
  - Something the user knows.
  - E.g., password, pass phrase, or personal identification number (PIN).

단어.

구

행복한 가족



Account information for Agents Authentication
Enter either a domain account or CommCell user account:
Account Information:
User Name:
Password:
< Back Next >

http://twitter.com/login
Always Check the Login URL
Username or email: hsoumen
Password: ••••••••••••••••••
□ Remember me

English (United States)
Instagram
wongmjane
real_password_hunter2_plz_dont_steal
Log In
Forgot your login details? Get help signing in.
Log in as @wongmjane
OR
Don't have an account? Sign up.
Instagram from Facebook

Facebook
Login Account Password
Email
Password
Login
Forgot password

Sign in to Gmail with your Google Account
Username:
Password:
□ Remember me on this computer.
Sign in
I cannot access my account

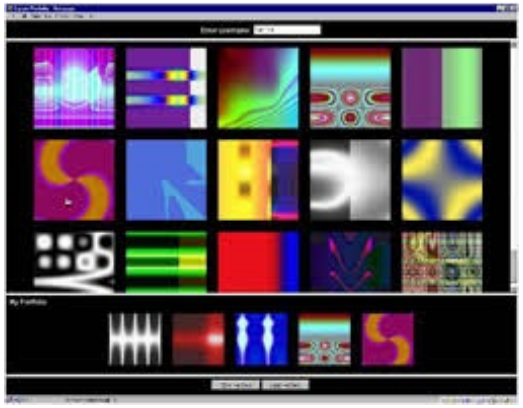
E-Plex
Electronic Pushbutton Locks

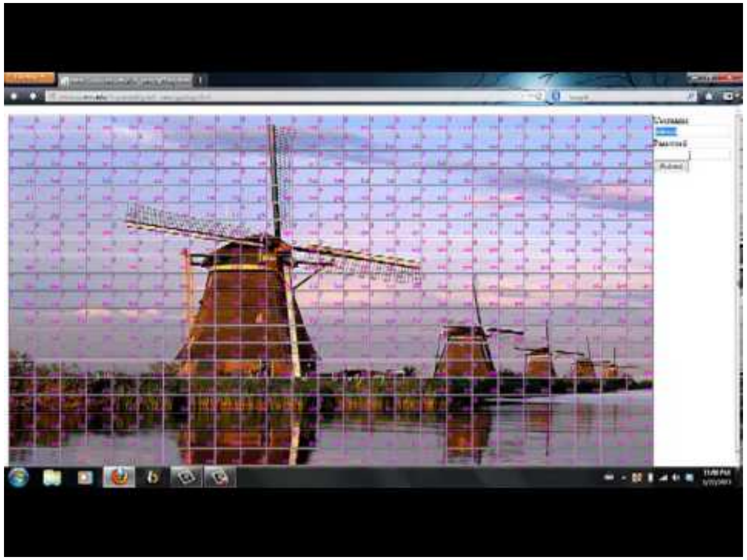
Top 25 Most Common Passwords

Rank	2011	2012	2013	2014	2015	2016	2017	2018	2019
1	password	password	123456	123456	123456	123456	123456	123456	123456
2	123456	123456	password	password	password	password	password	password	123456789
3	12345678	12345678	12345678	12345	12345678	12345	12345678	123456789	qwerty
4	qwerty	abc123	qwerty	12345678	qwerty	12345678	qwerty	12345678	password
5	abc123	qwerty	abc123	qwerty	12345	football	12345	12345	1234567
6	monkey	monkey	123456789	123456789	123456789	qwerty	123456789	111111	12345678
7	1234567	letmein	111111	1234	football	1234567890	letmein	1234567	12345
8	letmein	dragon	1234567	baseball	1234	1234567	1234567	sunshine	iloveyou
9	trustno1	111111	Iloveyou	dragon	1234567	princess	football	qwerty	111111
10	dragon	baseball	Adobe123	football	baseball	1234	iloveyou	iloveyou	123123
11	baseball	iloveyou	123123	1234567	welcome	login	admin	princess	abc123
12	111111	trustno1	Admin	monkey	1234567890	welcome	welcome	admin	qwerty123
13	iloveyou	1234567	1234567890	letmein	abc123	solo	monkey	welcome	1q2w3e4r
14	master	sunshine	Letmein	abc123	111111	abc123	login	666666	admin
15	sunshine	master	Photoshop	111111	1qaz2wsx	admin	abc123	abc123	qwertyuiop
16	ashley	123123	1234	mustang	dragon	121212	starwars	football	654321
17	bailey	welcome	monkey	access	master	flower	123123	123123	555555
18	passw0rd	shadow	shadow	shadow	monkey	passw0rd	dragon	monkey	lovely
19	shadow	ashley	sunshine	master	letmein	dragon	passw0rd	654321	7777777
20	123123	football	12345	michael	login	sunshine	master	!@#$%^&*	welcome
21	654321	jesus	password1	superman	princess	master	hello	charlie	888888
22	superman	michael	princess	696969	qwertyuiop	hottie	freedom	aa123456	princess
23	qazwsx	ninja	azerty	123123	solo	loveme	whatever	donald	dragon
24	michael	mustang	trustno1	batman	passw0rd	zaq1zaq1	qazwsx	password1	password1
25	Football	password1	000000	trustno1	starwars	password1	trustno1	qwerty123	123qwe

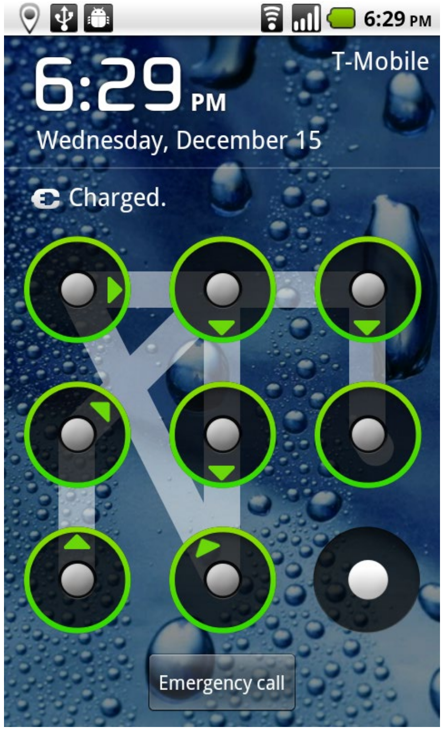
Graphical Password

- Recognition-based techniques
  - Pick several pictures out of many choices and identify them later in authentication
  - Password space $= \binom{N}{K} = \frac{N!}{K!(N-K)!}$, where N is the total number of pictures and K is the number of pictures selected as a password.





Pattern Lock

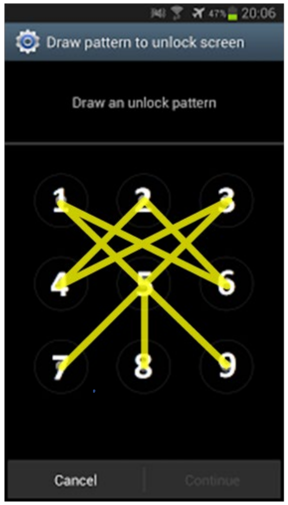

6:29 PM

T-Mobile

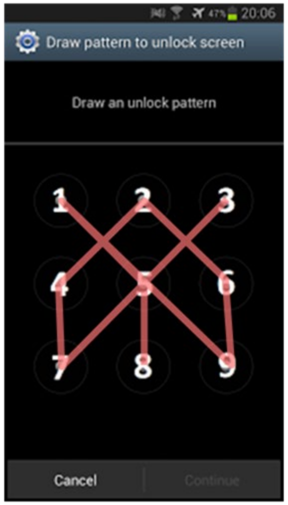
6:29 PM

Wednesday, December 15

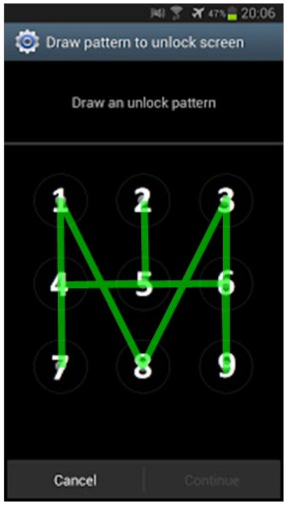
Charged.


Draw pattern to unlock screen

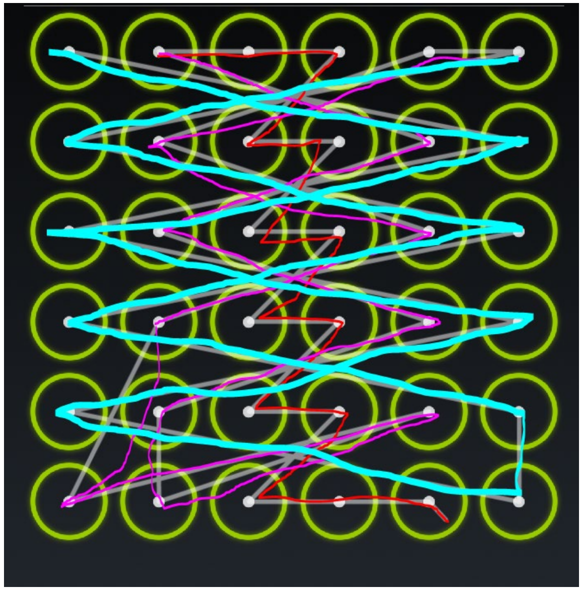
Draw an unlock pattern


Draw pattern to unlock screen

Draw an unlock pattern


Draw pattern to unlock screen

Draw an unlock pattern

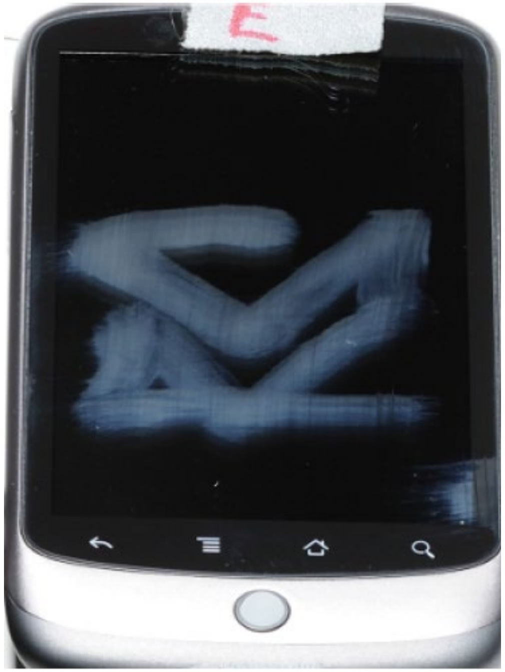


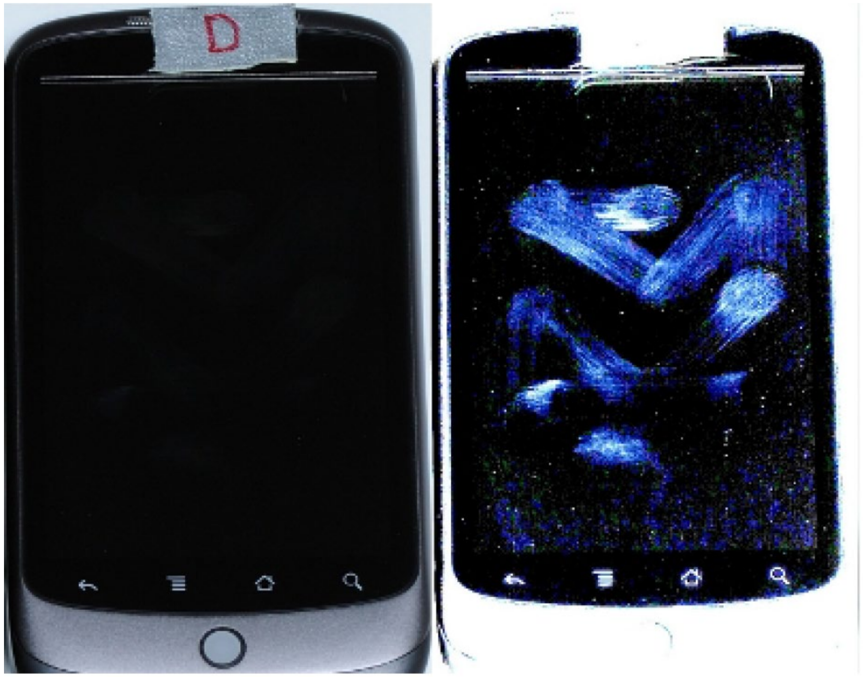
Pattern Lock: Rules & Key Space

- Rules
  - At least four points must be chosen,
  - No point can be used twice,
  - Only straight lines are allowed, and
  - One cannot jump over point not visited before.
- The number of pattern locks

Grid	Pattern locks
3 × 3	389,112
4 × 4	4,350,069,823,024
5 × 5	?

Pattern Lock: Smudge Attack





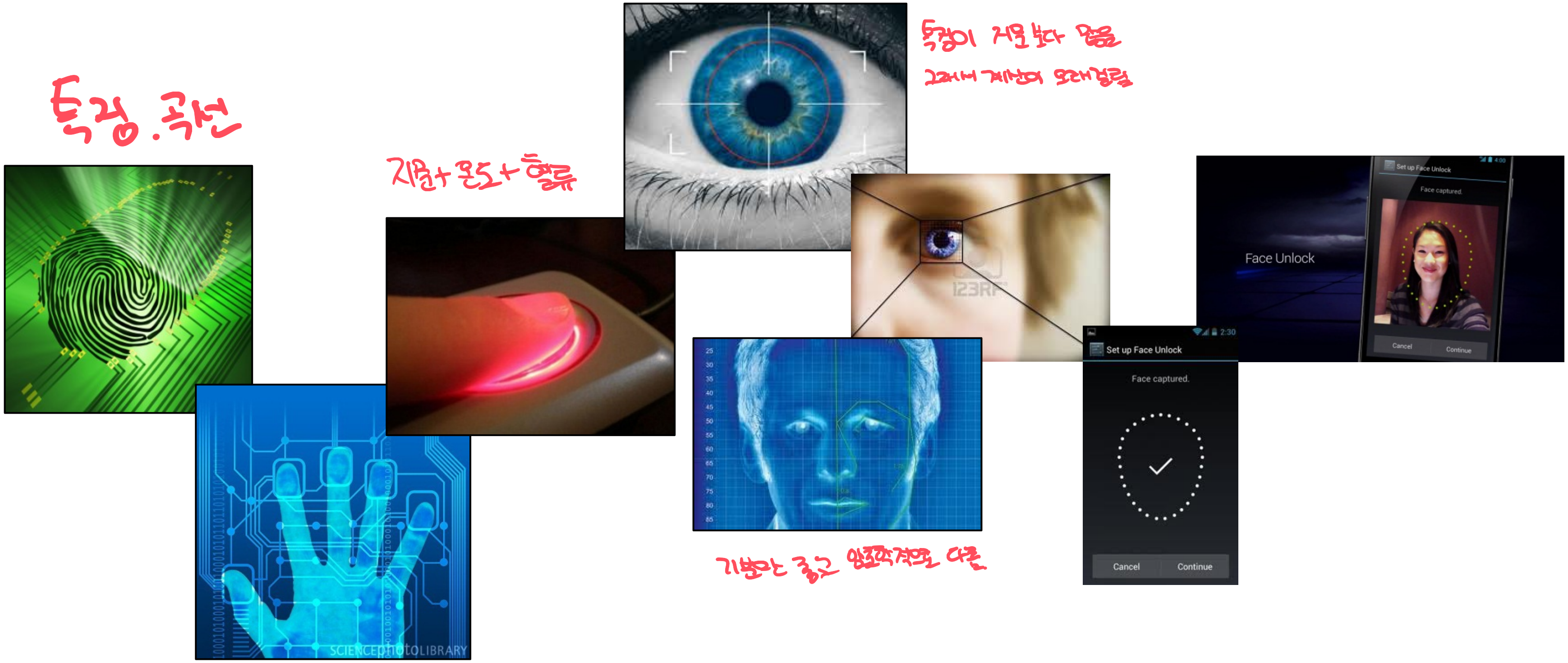
- Smudge attacks on smartphone touch screens (2010)
  - Adam J. Aviv et al.

Authentication Factor (Inherence Factor)

몸에 붙어있는것이 장.단점

- Inherence factors
  - Something the user is (or does). ex) 미션 임파서블
  - E.g., fingerprint, iris/retina, face, voice, or other biometric identifier.

특징.곡선

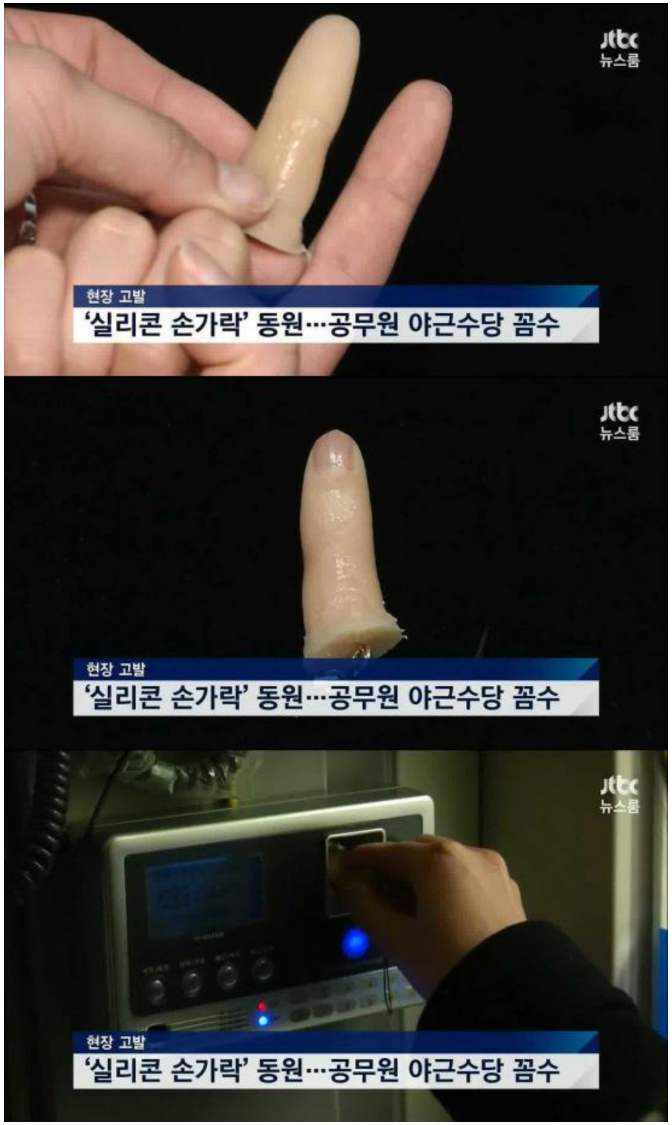


지문+온도+혈류

특징이 지문보다 많음
그래서 계산이 오래걸림

기본은 좋고 암호적적으로 다름

Biometrics: Security


jtbc 뉴스룸
현장 고발
'실리콘 손가락' 동원…공무원 야근수당 꼼수
jtbc 뉴스룸
현장 고발
'실리콘 손가락' 동원…공무원 야근수당 꼼수
jtbc 뉴스룸
현장 고발
'실리콘 손가락' 동원…공무원 야근수당 꼼수

Biometrics: Issues and Concerns

- Privacy and discrimination
  - It is possible that data obtained during biometric enrollment may be used in ways for which the enrolled individual has not consented.
- Danger to owners of secured items
  - In 2005, Malaysian car thieves cut off the finger of a Mercedes-Benz S-Class owner when attempting to steal the car.

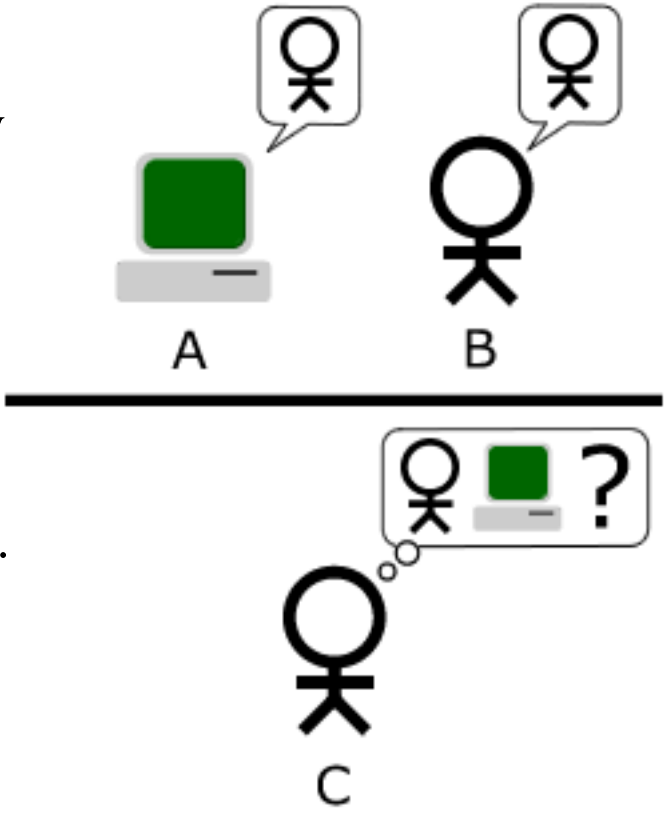
지문이 처음 도입되었던 2005년

Two-Factor Authentication

- Multi-factor authentication 2가지를 섞음 보통.
  - Multi-factor authentication is an approach to authentication which requires the presentation of two or more of the three authentication factors. After presentation, each factor must be validated by the other party for authentication to occur.
- Example: ATM 카드를 넣고. 비번입력
  - An automated teller machine (ATM) typically requires two-factor verification.
  - To prove that users are who they claim to be, the system requires two items: an ATM smartcard (application of the ownership factor) and the personal identification number (PIN) (application of the knowledge factor).
  - In the case of a lost ATM card, the user's accounts are still safe; anyone who finds the card cannot withdraw money as they do not know the PIN. The same is true if the attacker has only knowledge of the PIN and does not have the card.

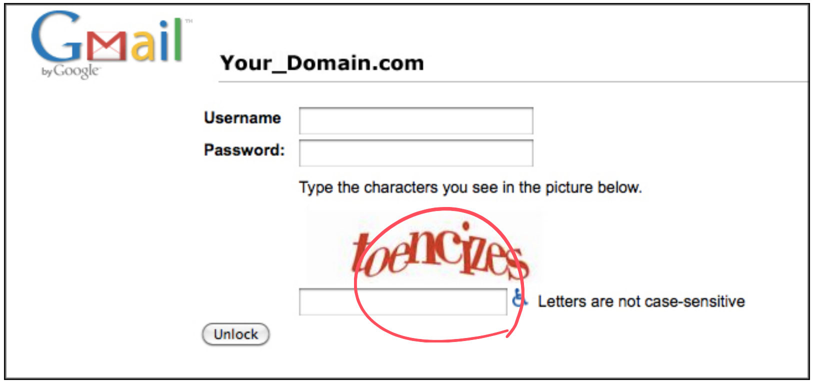
Turing Test

- Background 사람인지 , 프로그래밍인지
  - The Turing test is a test of a machine's ability to exhibit intelligent behavior equivalent to, or indistinguishable from, that of a human.
  - In the original illustrative example, a human judge engages in natural language conversations with a human and a machine designed to generate performance indistinguishable from that of a human being.
  - The test was introduced by Alan Turing in his 1950 paper "Computing Machinery and Intelligence." In the years since 1950, the test has proven to be both highly influential and widely criticized, and it is an essential concept in the philosophy of artificial intelligence.



Human Authentication

- CAPTCHA
  - CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is a type of challenge-response test used in computing as an attempt to ensure that the response is generated by a human.
  - The test is designed to be easy for a computer to generate, but difficult for a computer to solve, so that if a correct solution is received, it can be presumed to have been entered by a human.



Your_Domain.com

Username

Password:

Type the characters you see in the picture below.

Letters are not case-sensitive

사람인지만 확인 CAPTCHA↑ 사람이냐, 아니냐.

No CAPTCHA reCAPTCHA

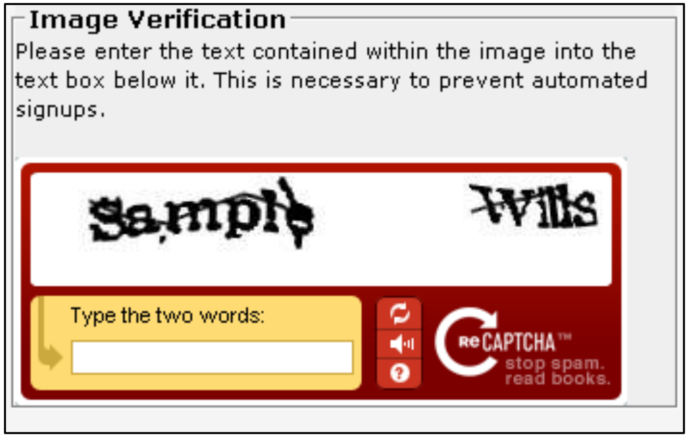
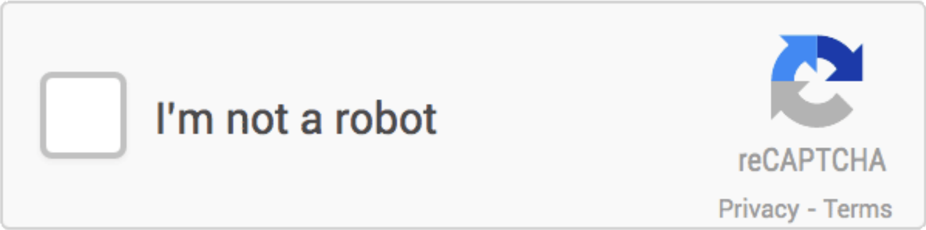


Image Verification

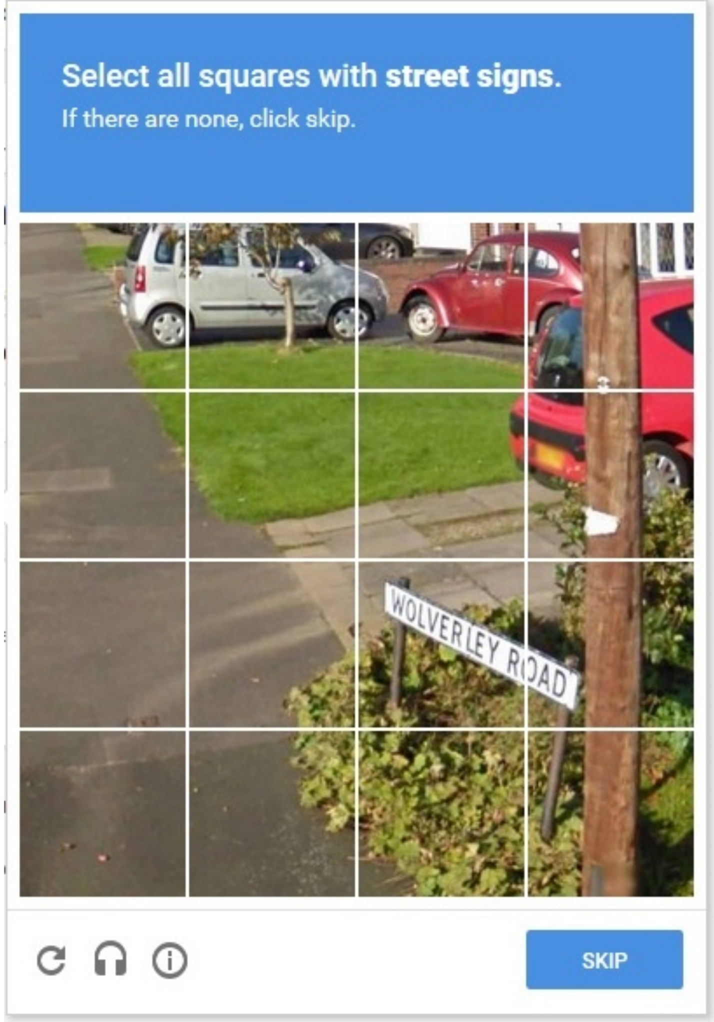
Please enter the text contained within the image into the text box below it. This is necessary to prevent automated signups.

현재는 captcha가 아님.



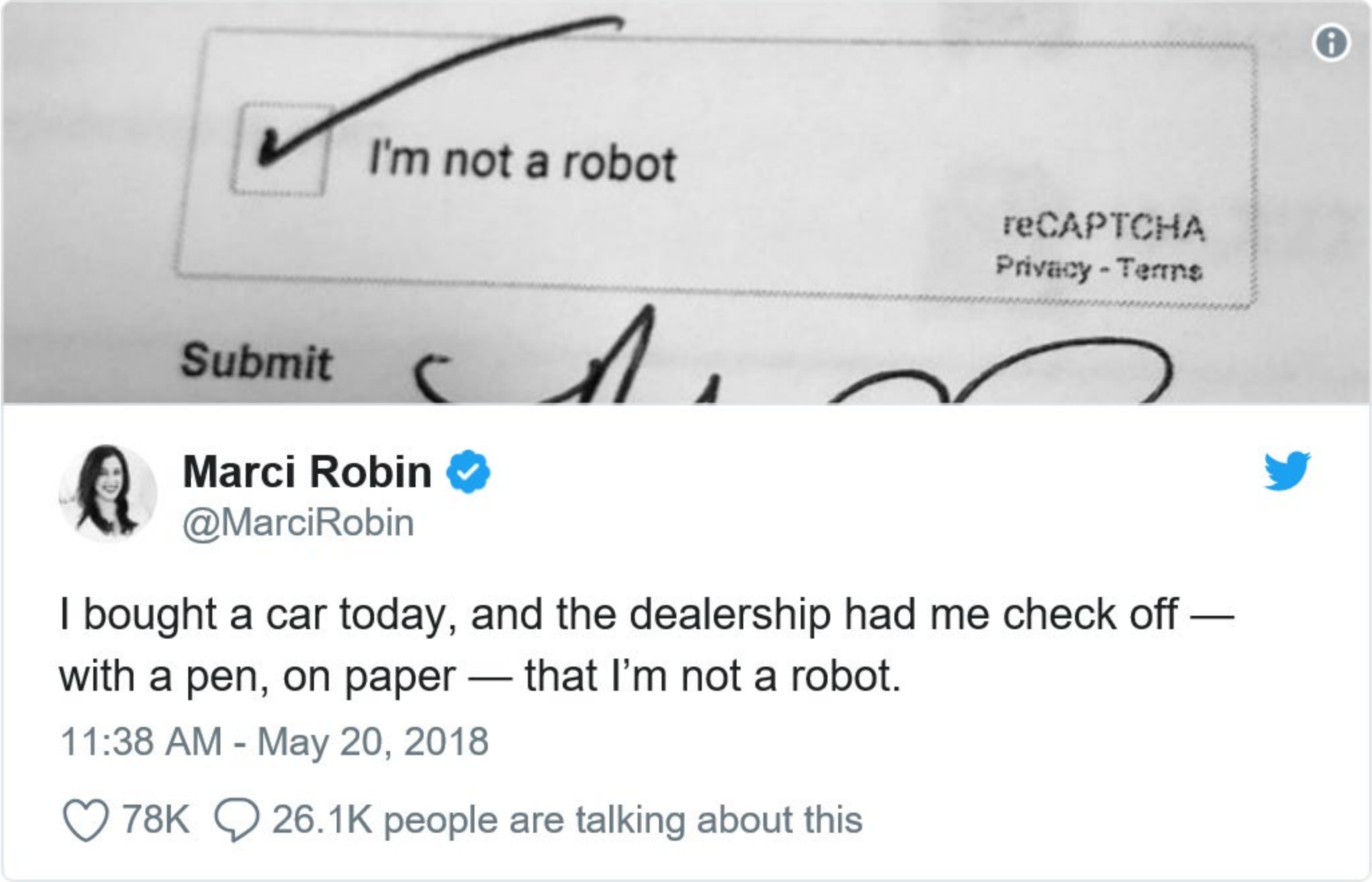
□ I'm not a robot

적당하게 컴퓨터가 안할 행동하면 → 3 안넘어감



Select all squares with street signs.

If there are none, click skip.



Marci Robin
@MarciRobin

I bought a car today, and the dealership had me check off — with a pen, on paper — that I’m not a robot.

11:38 AM - May 20, 2018

♡ 78K 💬 26.1K people are talking about this