Security Components

Chapter 2

Security Components

- ★ Security & Privacy: the definitions
- ★ Security Components
- ★ Supporting Concepts
- ★ Conclusion

Security and Privacy

> “Security is the first cause of misfortune.”
> Old German Proverb

- ★ Though often mentioned together,
  Security & Privacy is not the same thing.
- ★ However, they both need the control over information.

- ★ Security
  - ○ Who can do what when?
- ★ Privacy
  - ○ The freedom to control access to our personal information

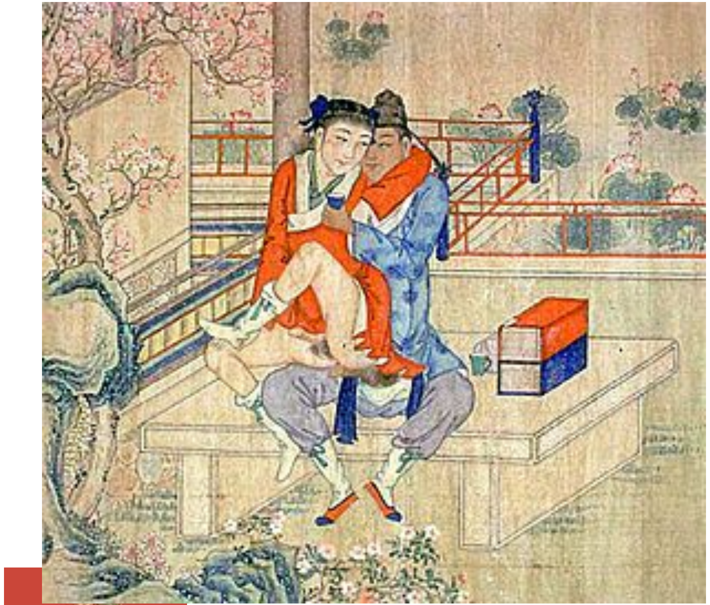
Security and Privacy (ctd.)

- ★ This is Security or Privacy

Security

- ★ a hacker is able to **compromise a computer** system and find out that **a person is a homosexual** or is infected with a disease.

may
or
may not
be **Privacy**



picture from https://en.wikipedia.org/wiki/Homosexuality_in_China

Privacy

★ Privacy is depending on intent.

★ If a homosexual person is willing to go public, it is not a privacy issue.

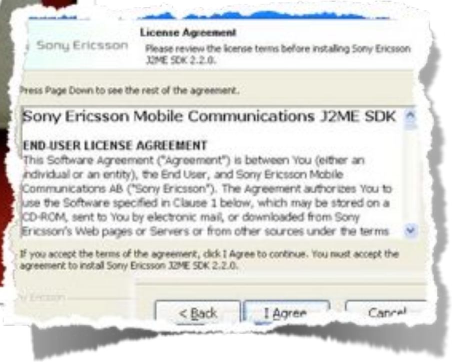
★ In reality, we always trade privacy for services.

★ As long as the provider conforms to the privacy policy, this should be fine.

★ An person may deny to share his/her age with others. However, he/she may share this information with a physical doctor for a better treatment.

Solution to Privacy

- ★ a naïve solution for a privacy-concerned application is to give a user a choice to release his or her personal information
- ★ Disclaimer, Agreement, Privacy Policy
- ★ HIPAA ?



License Agreement

Please review the license terms before installing Sony Ericsson J2ME SDK 2.2.0.

Press Page Down to see the rest of the agreement.

Sony Ericsson Mobile Communications J2ME SDK

END-USER LICENSE AGREEMENT

This Software Agreement ("Agreement") is between You (either an individual or an entity), the End User, and Sony Ericsson Mobile Communications AB ("Sony Ericsson"). The Agreement authorizes You to use the Software specified in Clause 1 below, which may be stored on a CD-ROM, sent to You by electronic mail, or downloaded from Sony Ericsson's Web pages or Servers or from other sources under the terms

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Sony Ericsson J2ME SDK 2.2.0.

Fact

Google Privacy said they may access your information to improve Google’s services.

We (Google) **may combine the information** we collect among our services and across your devices for the purposes described above. ….. Depending on your account settings, your activity on other sites and apps **may be associated with your personal information in order to improve Google’s services** and the ads delivered by Google.

Taken from https://policies.google.com/privacy?hl=en-US#intro

Fact

What Facebook's privacy policy allows may surprise you.

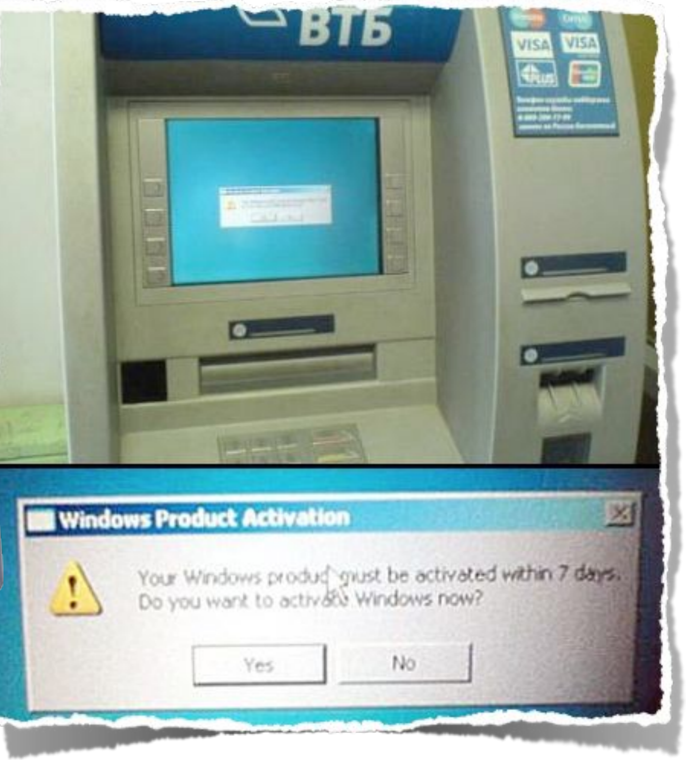
"If you start typing something and change your mind and delete it, Facebook keeps those and analyzes them too," Zeynep Tufekci, a prominent techno-sociologist, said in a 2017 TED talk .

Taken from https://www.chicagotribune.com/business/ct-facebook-privacy-policy-20180325-story.html

Security Components

Security in Action: ATM

- ★ Is this a secure system?
- ★ If yes, what does it have?



Windows Product Activation

Your Windows product must be activated within 7 days.
Do you want to activate Windows now?

Yes No

Security in Action: Security Deposit Box (Safe box)

- ★ To access a security deposit box, there are several steps.
- ★ Is it a secure system?
- ★ If yes, what does it have?

Look around yourself to find more examples.

- ★ Is it secure?
  - ○ Your home?
  - ○ You computer?

Security Components

- Authentication
  - “Who are you? Are you really the person whom you claim to be?”
- Authorization
  - “Do you have the authority to do what you are trying to do?”
- Accounting (Auditing)
  - “What did you do?”

the **AAA** of Security

Analogy

★ The AAA is usually compared to three headed dogs (Kerberos). (One head for each component)

★ The Athena project from MIT named it Authentication Project “Kerberos”.

Cerberus or Kerberos (Greek Κέρβερος, Kerberos, "demon of the pit") was the hound of Hades, a monstrous three-headed dog with a snake for a tail (sometimes said to have 50 or 100 heads) called a hellhound.

Supporting Concepts

- AAA is not enough?
- Integrity
  - Integrity (n) “the quality or state of being complete or undivided”
- Software Engineering & Threat Modeling
  - “Threat modeling is a method of addressing and documenting the security risks associated with an application.”
- Validation of Input
  - “All input is evil until proven otherwise”

Conclusion

- 3 Security Components
  - Authentication
  - Authorization
  - Auditing
- 2 Supporting Concepts
  - Integrity
  - Input Validations
- Missing a component means a system is not secure.
- Having all components does not mean the system is secure.

End of Chapter 2

Authentication

Chapter 3

Authentication

- Definition
- Authentication Methods
  - What do you know?
  - What do you have?
  - What do you trust?
- Authentication Protocol
- Zero-Knowledge Password Proof
- Good Password and Bad Password
- Password Hacking
  - Rainbow Table
- Implementation Issues

Definition of Authentication

“It’s easy to know men's faces, not their hearts.”
Chinese Proverb

- ★ In a computer system, authentication is the process of verifying identity of a user.
  In a communication system, authentication is the process of verifying the stated source of a message [dictionary.com].
  - ○ validating the quality or condition of being trustworthy, genuine, or creditable
  - ○ examination of a token or investigation of some property of the subject itself

How to Authenticate?

- Validating authenticity of a document (e.g. transcript, bank note, cheque ....)
- Identifying a person (student, member of a group, ...)
- The source of data (e.g. network packet, email, ...)
- Owner of (house, car, ...)
- How about software or computer systems?

Authentication Methods

- ★ What do you know?
- ★ What do you have?
- ★ Who do you trust?

- ★ Every authentication method has its own strength and weakness, and there is no such thing as a perfect authentication method.

What do you know?

A secret between two is God's secret, a secret between three is everybody's.
Spanish Proverb

- ★ Prearrange questions
- ★ Password or Passphrase
- ★ One-time pad
- ★ Challenge and Response
  - ○ How much is 1+1 ?

In the past, an american soldier has to state a prearrange question with the army for identifying himself in case of emergency.

Challenge and Response

- ★ Knowledge of a method
- ★ Alice > Bob : N
- ★ Bob > Alice: {N,B}k
- ★ Prevent replay attacks

- ★ To avoid replay attack, car remote is now a challenge and response.

What do you have?

- ★ Tokens
  - ○ ID
  - ○ Seal
- ★ Smart Tokens
- ★ Biometrics
  - ○ Fingerprints
  - ○ Hand/Palm geometry
  - ○ Handwriting
  - ○ Face Recognition
  - ○ Dental biometrics
  - ○ Retinal
  - ○ Vein
  - ○ Voice
  - ○ Pattern (walking/typing rhythms)

What do you trust?

- Third party authentication
  - Facebook Login
  - Google Login
  - ChulaSSO
- Proximity/Trusted Zone
  - Dress like a student on the campus

Authentication Protocol

- ★ A combination of methods for authentications
- ★ Use a combination of password and smart tokens
- ★ Example
  - ○ Login with SSH to a gateway
  - ○ Server challenges with a nounce
  - ○ Use crypto card to generate a one-time password
  - ○ Use it to access the system.

Zero-Knowledge-Password Proof

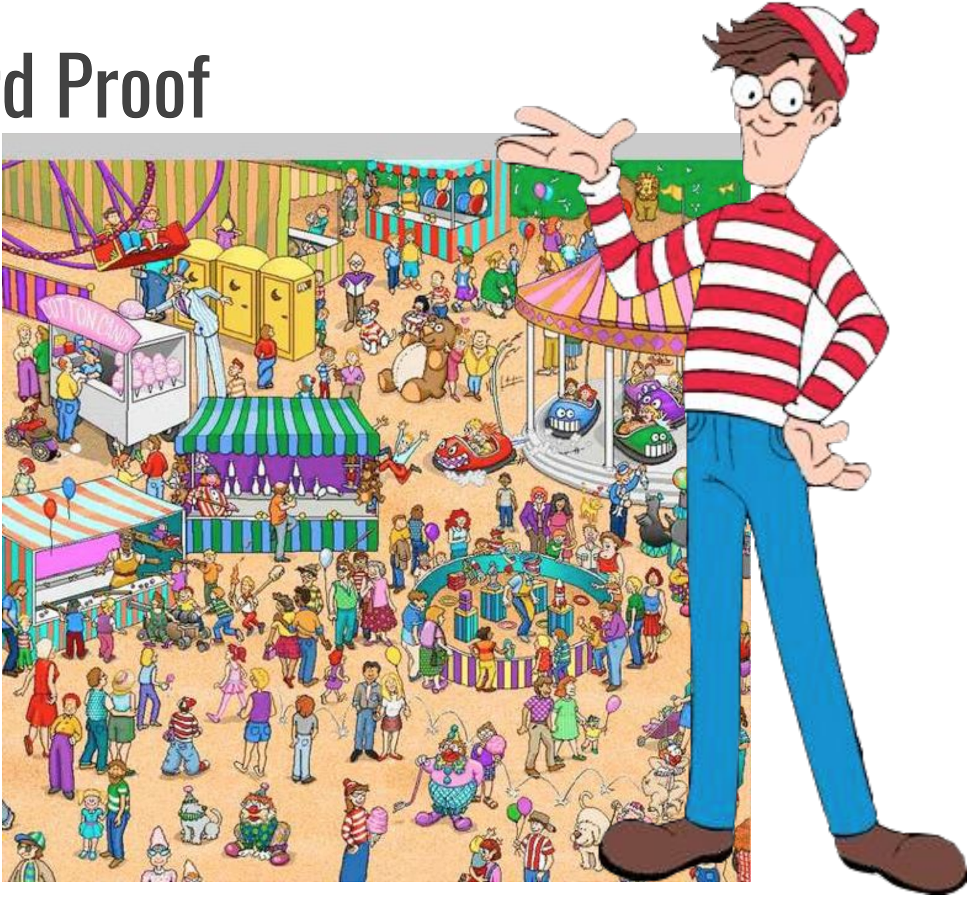
★ An authentication protocol.

★ Proof the knowledge of password without saying it out loud.

★ Where is Waldo?

★ Both parties share a same picture. Use a coordinate of Waldo to validate the knowledge.

★ Modern authentications are based on ZKPP.



Zero-Knowledge-Password Proof (ctd.)

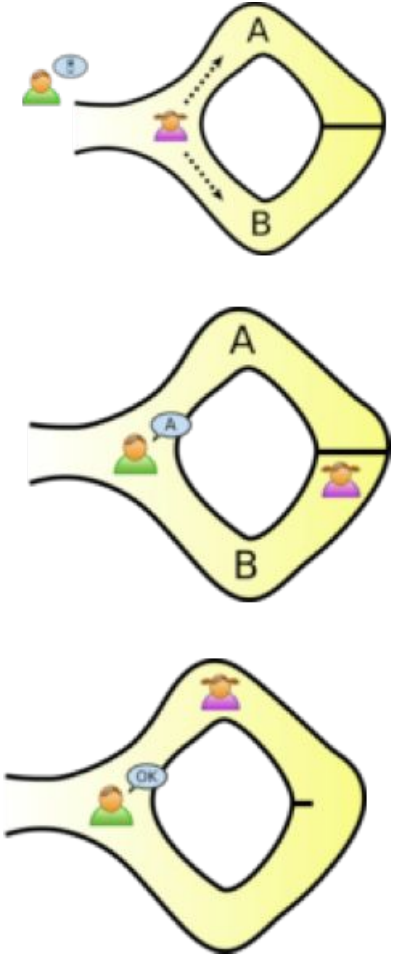
★ Proof that the little girl got a key to the gate at the end of the tunnel.

★ Let the girl walk into the tunnel.

★ Ask her to get out at a random direction.

★ Repeat the steps several time.

★ If that girl always come out at the right direction, she got a key.



Good Password and Bad Password

- Substitution
  - act10n
  - 0wn3r
  - 4U&m3
  - p3nc1l

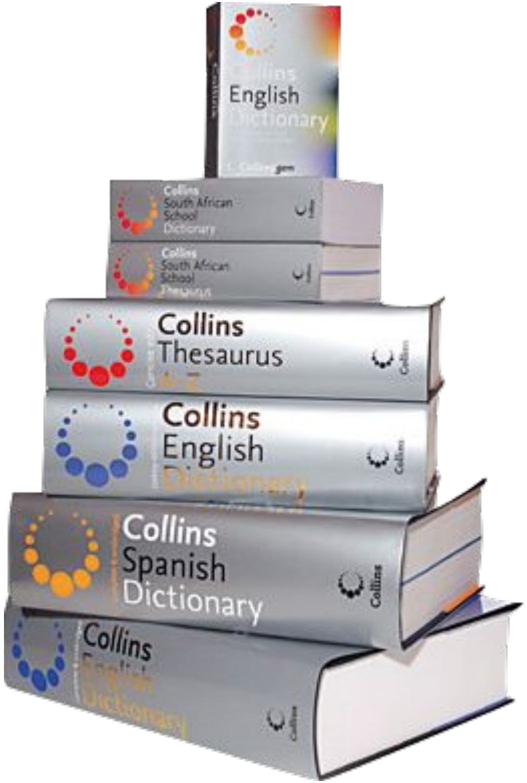
- Guessable pattern
  - Qwerty
  - Q1w2e3r4t5y
  - Password1
  - Password2

How secure is a password?

- Assume that:
    - n is the length of the password (e.g. digits or characters).
    - k is the number of characters in the set of possible characters.
    - C is the constant amount of time requires for testing a password (e.g. seconds).
    - t is the number of times allowed to guess the password before locking the account.
- Given n characters in a password, each character is taken from the k characters in the set,
  How long will it take to test all possibilities?

Password Hacking

- ★ Dictionary attack
- ★ Brute-force attack
- ★ Rainbow table
- ★ Replay attack
- ★ Social Engineering (Phishing)



Watch this

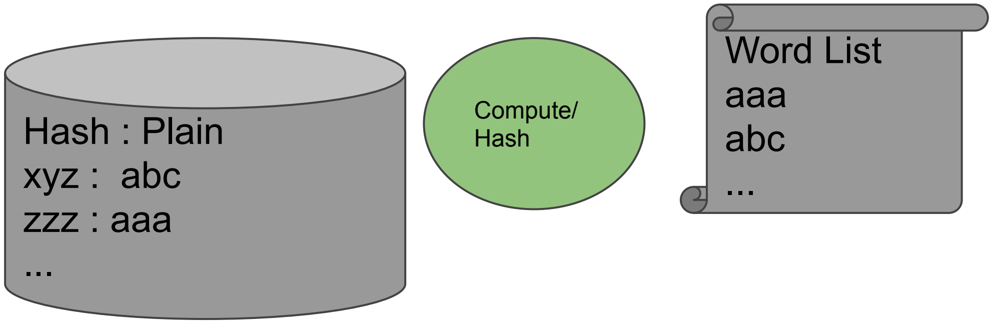
https://www.youtube.com/watch?v=6bNtMPKafk0

https://www.youtube.com/watch?v=f-Dogvyn9ZU

Rainbow Table

- ★ Password is based on one-way hash function. (Theoretically, irreversible).
- ★ Rainbow Table is the use of idle processing power to precompute possible results.
- ★ Change from tring to looking up from the table. (Instant result)

Obtain a hashed value xyz.
Look up for xyz -> **abc**



Hash : Plain
xyz : abc
zzz : aaa
...

Word List
aaa
abc
...

Fact

Rainbow Table
- free download
- Indexed by Google

★ Try search hashed values of simple words in google.

```
$ echo "security" |md5
e46d69abde01f581f79cd4ec029a8469
echo "online" |md5
747a43298e195448246825207a9364b6
```

★ Rainbow Table can be downloaded for free. (http://project-rainbowcrack.com/table.htm)

★ Try it with your password. If it is in the rainbow table, change your password.

Implementation Issues

- ★ Issues not covered in this slide
  - ○ Management Cost
  - ○ Communication Channel
  - ○ Human Factor
  - ○ Accuracy
  - ○ Transferability
  - ○ Centralize vs. Distributed
  - ○ Single Sign-On

End of Chapter 3