2110413 Computer Security

Krerk Piromsopa, Ph.D.
Department of Computer Engineering
Chulalongkorn University

- Security & Privacy: the definitions
- Security Components
- Supporting Concepts
- Authentication

Security and Privacy

"Security is the first cause of misfortune."
Old German Proverb

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

Security or Privacy?

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

Solution to Privacy

License Agreement

Sony Ericsson

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.

- 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 ?

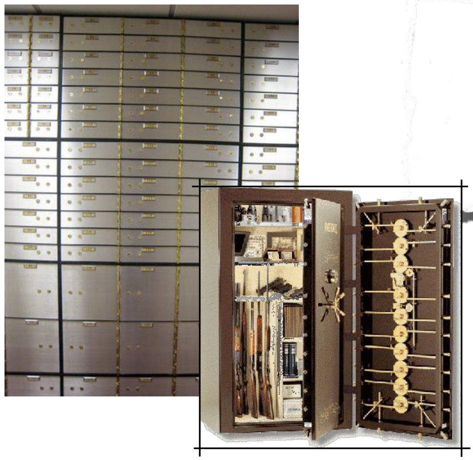
What do we need to create a secure system?

Security in Action: ATM

Windows Product Activation

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

Security in Action: Safe box



Look around yourself to find more examples.

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

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

- 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"

The first A: Authentication

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?

- 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 passphase
- One-time pad
- Challenge and Response
  - How much is 1+1 ?

Good password

- Uniqueness
- Length of password
- Aging
- Password History
- Invalid attempts
- Time between attempts
- Typing
- Guideline
  - Substitution
  - Avoid Patterns
- One-time password

Time between attempts

Prog 1.	**Prog 2.**	**Prog 3.**
1. Input [login name] 2. Fetch [saved password] 3. If no entry then exit 4. Input [password] 5. Compare passwords. 6. If valid then start session else exit End if	1. Input [login name] 2. Input [password] 3. Fetch [saved password] 4. If no entry then exit 5. Compare passwords. 6. If valid then start session else exit End if	1.Input [login name] 2.Input [password] 3.Fetch [saved password] 4.If no entry then [saved password] Null 5.Compare passwords. 6.If valid then start session else exit End if

Patterns & Substitution

- Guessable pattern
  - qwerty
  - q1w2e3r4t5y
  - password1
  - password2
- Substitution
  - act10n
  - 0wn3r
  - 4U&m3
  - p3nc1l
-

How to hack password(s)?

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

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?

Challenge and Response

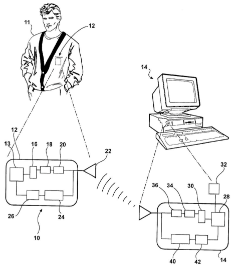
- Alice > Bob : N
- Bob > Alice: $\{N,B\}_k$
- Prevent replay attacks

What do you have?

- Tokens
  - ID
  - Seal
- Smart Tokens
- Biometrics
  - Fingerprints
  - Hand/Palm geometry
  - Handwriting
  - Face Recognition
  - Dental biometrics
  - Retinal
  - Vein

What do you trust?

- Third party authentication
- Proximity/Trusted Zone



Protocol

- Password & Smart Token
- Zero-Knowledge Password Proof

ZKPP

Where is Waldo?

Into action

Assume that password is {1, 2, 5, 7}.
Server creates four strings and sends them to user:

```
       1 2 3 4 5 6 7 8 9
S[1]: T H I S I S 1 S T
S[2]: R A N D O M 2 N D
S[3]: E X A M P L E 3 1
S[4]: 4 T H N U M B E R
Password: [BATP]
```

In this case, the password would be encoded as any combination of “TAPB” (e.g. “PATB” or “BATP”). This way, server can authenticate the password without directly sending the password.

Implication

- A share key is required for each authentication.
- EKE, DH-EKE, SPEKE, SRP
- Any NP problem can be used for ZKPP.

Implementation Issues

- Management Cost
- Communication Channel
- Human Factor
- Accuracy
- Transferability
- Centralize vs. Distributed
- Single Sign-On

Assignment 1

Types of characters (English)	**Number (*k*)**
Lower-case alphabetic	26
Numeric and lower-case alphabetic	36
Upper and lower-case alphabetic	52
Numeric, lower-case alphabetic, with symbols and punctuation	68
All displayable characters	94

1. How long does it take to crack an 8-character UNIX password?
   Please justify your answer.
   Note that you may assume anything.
   (i.e. dictionary attack, brute force attack, speed and number of machines using)

2. From your calculation in exercise 1, what do you think is the minimal length of a password to be considered secure enough?

The End