

Information Security for Privacy Protection

Atsuko Miyaji

JAIST



Abstract

- How and Why our privacy has been leaked out?
- What is a solution to protect our privacy?
→ Information Security
- Recent research interest on information security to enhance our privacy.

2



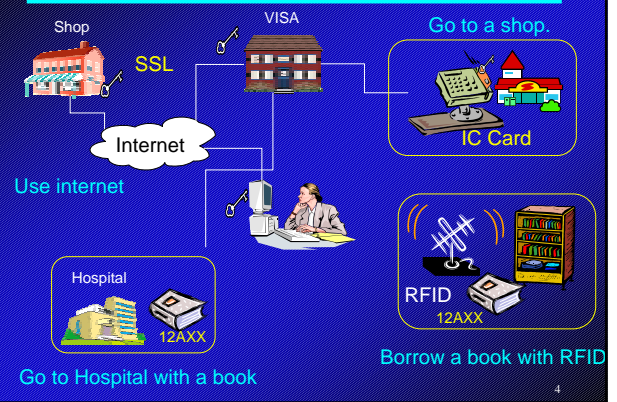
Outline

- Our life has been digitalized.
- Our privacy has been leaked out.
- Subjects of Information Security.
- Recent research of information security
 - Protect your system even if your key has been stolen
 - Protect your key against electronic consumption
 - Protect your privacy against collusion

3



Our life has been digitalized

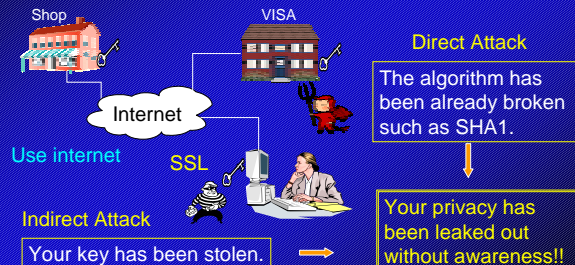


4



Our privacy has been leaked out

It seems secure by encryption.
→ Theoretical security analysis is necessary.
Fault tolerance system is required: it stands if a key is stolen.

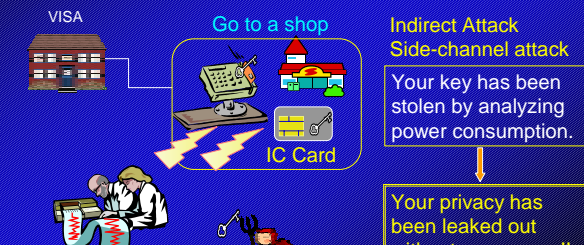


5



Our privacy has been leaked out

It seems secure: IC card, secure number theory, never stolen the card, and face-to-face communication without Internet.
→ Realistic security analysis is necessary: implementation



6

Our privacy has been leaked out

It seems secure through secure channel.
 ⇒ Anonymity is necessary for protocol.

Shop VISA Alice needs insurance. Alice insurance. Internet Alice Ski No insurance Indirect Attack Your various privacy has been gathered and combined. Hospital Alice Cancer Mild 12AXX Your privacy has been leaked out without awareness!!

Our privacy has been leaked out

Privacy information has expanded: location, taste, opinion, idea...
 ⇒ Unlink-ability is necessary for protocol.

She is here! Hospital 12AXX Serial No linkable Borrow a book with an RFID 12AXX RFID Go to Hospital with the book Your simple privacy such as location, idea, taste, etc has been leaked out without awareness!!

What shall we do?

We need information security !

- Secure network modeling
 - analysis the security related with network or software.
 - mobile agent
 - network virus
 - RFID security
- Secure electronic protocol
 - provide enhanced secure electronic protocol: anonymity, unlink-ability, lost-key security
- Cryptographic basic research
 - analysis security & efficiency
 - Side-channel attack
 - Public-key encryption
 - Secret-key encryption

- Group signature
- E-money
- E-auction
- Fault-tolerance

Fault tolerant system-key-evolving system

Minimize the damage when a secret key is lost or broken.

- A secret key is divided into two devices, user and base.
- Key evolution over time is achieved by user and base.
- User and base are exposed repeatedly
- Any user key except those exposed user keys remains secure.

Security Integration

Shop VISA SCA-resistance IC Card Internet Alice Ski No insurance Anonymity Group signature X+**> Cancer Hospital 12AXX Unlinkability Secure RFID 12AXX RFID Provable secure enc., Key evolving enc

Concluding Remarks

- We have seen how our privacy has been leaked out without awareness.
- We have shown that information security protect our privacy.
- We will give a way that user can control her/his privacy level: sometimes link-ability is fine.
- We will provide the minimum integration that enhance various system security.