

Title	Information Security for Privacy Protection
Author(s)	Miyaji, Atsuko
Citation	
Issue Date	2005-03-11
Type	Presentation
Text version	publisher
URL	<a href="http://hdl.handle.net/10119/8274">http://hdl.handle.net/10119/8274</a>
Rights	
Description	JAIST 21世紀COEシンポジウム2005「検証進化可能電子社会」 = JAIST 21st Century COE Symposium 2005 “Verifiable and Evolvable e-Society”, 開催 : 2005年3月10日~11日, 開催場所 : 石川ハイテク交流センター, Technical session 3 <Security>

# 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



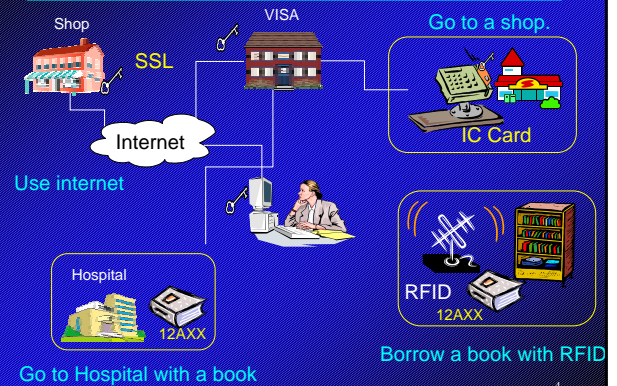
## Outline

- 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

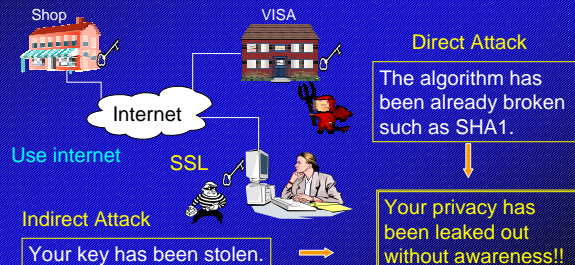


4



## 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: Alice Ski, No insurance

Internet: SSL

VISA: Alice needs insurance.

Hospital: Alice Cancer Mild, 12AXX

Indirect Attack: Your various privacy has been gathered and combined.

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

Go to Hospital with the book

You just have a book with a RFID.

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.

base:  $sbk_0, sbk_t, sbk_{t+1}$  (exposed)

user:  $sk_0, sk_{t-1}, sk_t, sk_{t+1}$  (secure)

## Security Integration

Shop: SCA-resistance, IC Card

Internet: Provable secure enc., Key evolving enc

Hospital: Unlinkability, Secure RFID, 12AXX

RFID: 12AXX

Group signature:  $+^{**?}/Ski$

Anonymity

X $^{**>}$  Cancer

## 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.