Information Security for Privacy Protection

Atsuko Miyaji

JAIST

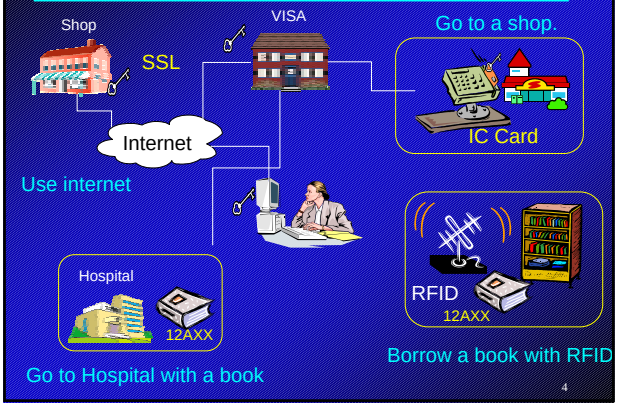
Abstract

- 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.

Outline

- Our life has been degitalized.
- 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

Our life has been degitalized

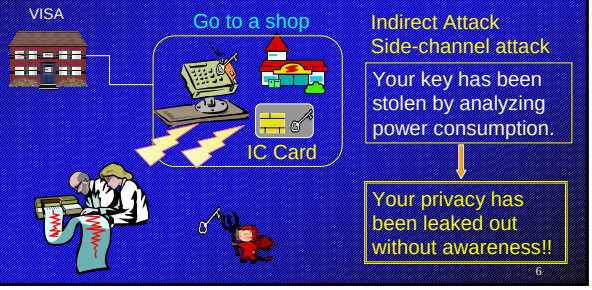


Our privacy has been leaked out

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

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

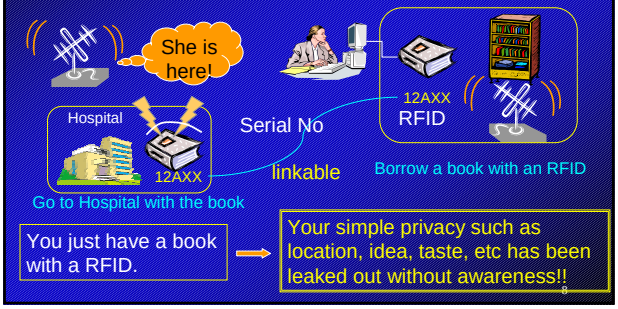


Our privacy has been leaked out

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

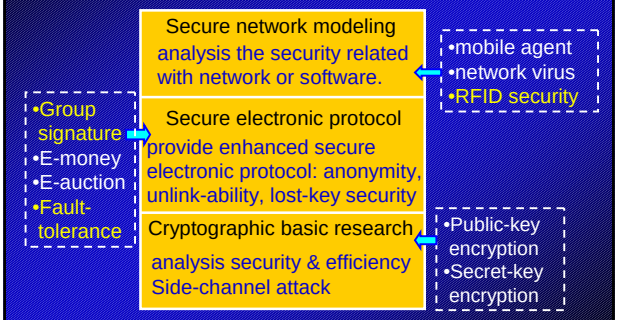
Our privacy has been leaked out

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



What shall we do?

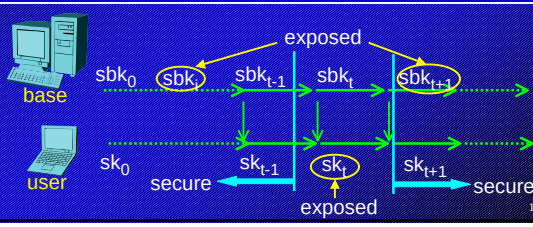
We need information security !



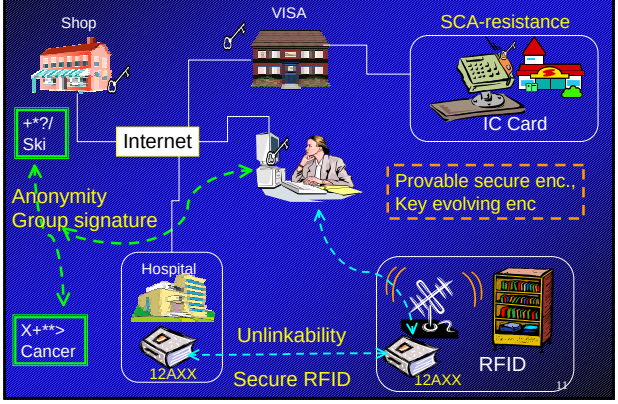
Fault tolerant system-key-evolving system

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



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.