Security Aspects on Near Field Communication Mobile Devices

Zhao He

Mobile Security Seminar

February 9th, 2011

Introduction

Technology

Security Threats

Solutions and Analysis

Summary

http://vimeo.com/6588461

Near Field Communication

- NFC in short

  developed by Philips and Sony
- Compatible to RFID

  contactless, proximity range, low bandwidth
- Extension to RFID

  Peer-to-Peer mode

Mensa Card is an RFID card

NFC Mobile Device

+

Rumor says iPhone 5 will feature NFC [1]

[1] http://www.bloomberg.com/news/2011-01-25/apple-plans-service-that-lets-iphone-users-pay-with-handsets.html

NFC Mobile Device (Cont.)

- Google/Samsung Nexus S
  - First Android device to support NFC in both hardware and software
  - Available in the US and UK from December 2010
  - Available in Germany from February 2011 (White shell)

Applications

- Mobile ticketing and payment

  electronic purse, debit/credit card

  already widely used in Japan
- Identification

  e.g. biometric passport
- Receive and share information

  Smart Poster
- Paring service

  iTunes enabled CD store

  cf. Bluetooth

  not for data transmission (explain later)

Introduction

Technology

Security Threats

Solutions and Analysis

Summary

Standards

- Basics
  - 13.56 MHz
  - ~10cm
  - 424kbit/s (slower than Bluetooth 2.1Mbit/s)
- NFCIP-1 and NFCIP-2
  - Near Field Communication Interface and Protocol
  - Specified by NFC-Forum

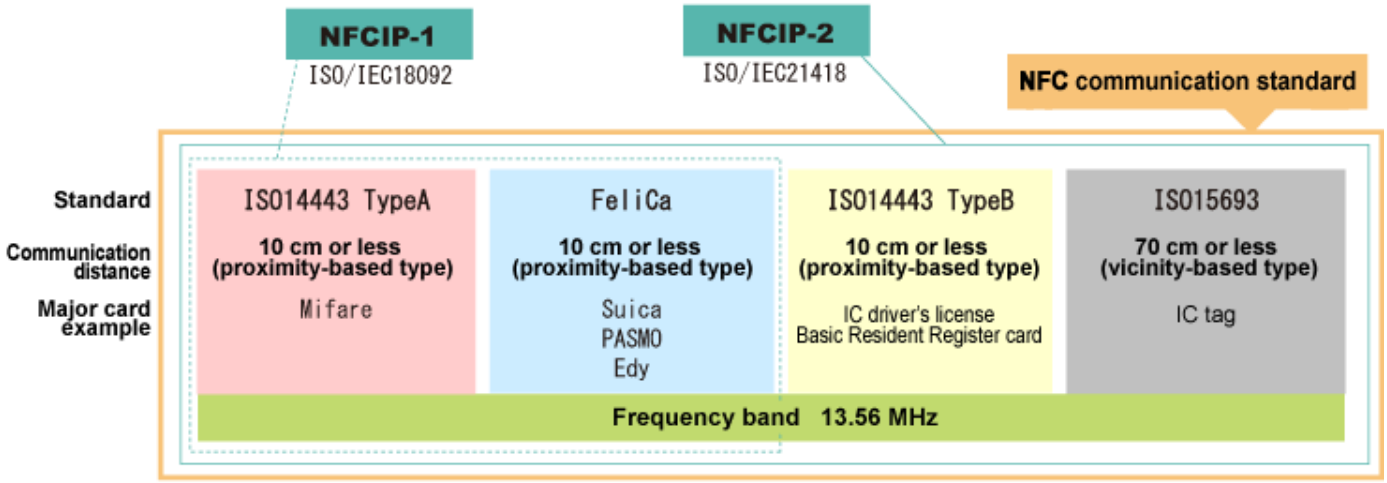
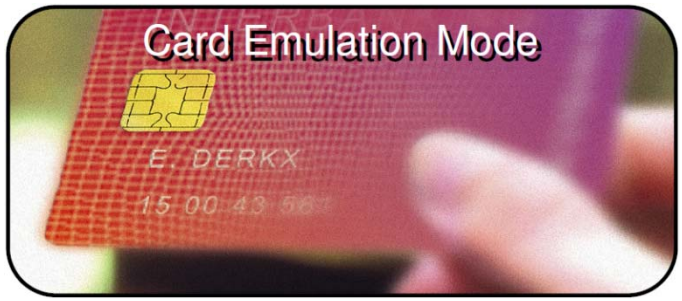
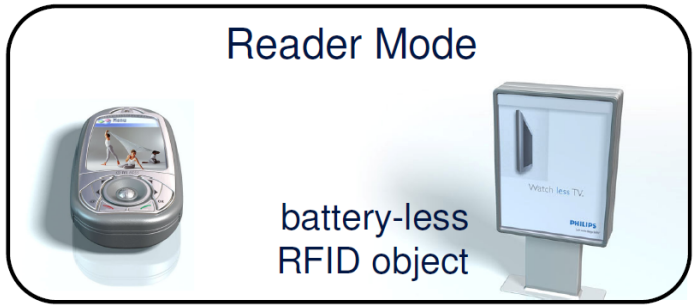


Image from http://www.toppan-tl.co.jp

Operation Modes

- Card Emulation Mode
  - ISO 14443
  - PICC (proximity integrated circuit card)
- **Reader**/Writer Mode
  - ISO 14443
  - PCD (proximity coupling device)
- Peer-to-Peer Mode
  - ISO 18092





Images from [2]

Introduction

Technology

Security Threats

Solutions and Analysis

Summary

Transactions over the RF link

- Eavesdropping

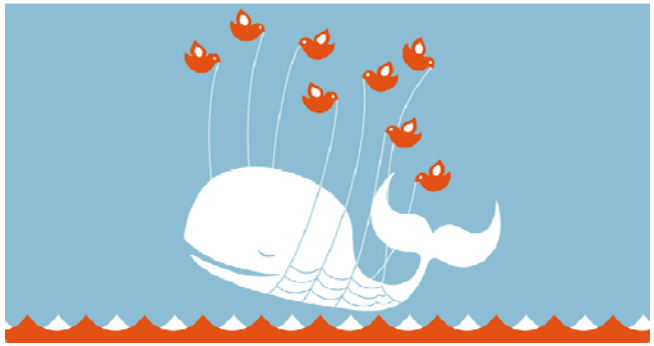
  Retrieve RF signal without the owner's consent

- Data corruption

  RFID jamming causing reader DoS

- Man-in-the-middle attack

  Retrieve signal from sender and send respond to the receiver



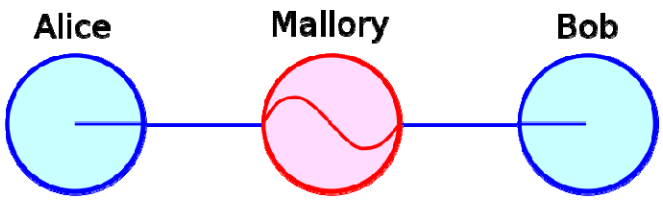
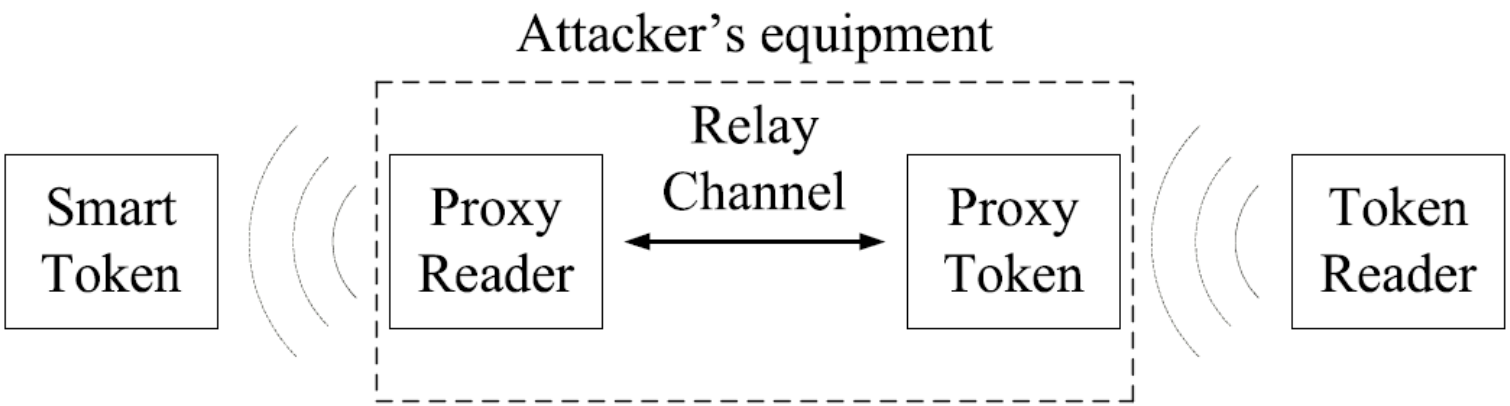


Image one from film *Das Leben der Anderen* copyright Sony Pictures Entertainment Inc.
Image two copyright Yiying Lu. Image three copyright Miraceti

Relay Attack

- Grand Master Chess problem [8]
  - forward move from one grand master to the other



Basic relay attack setup [3]

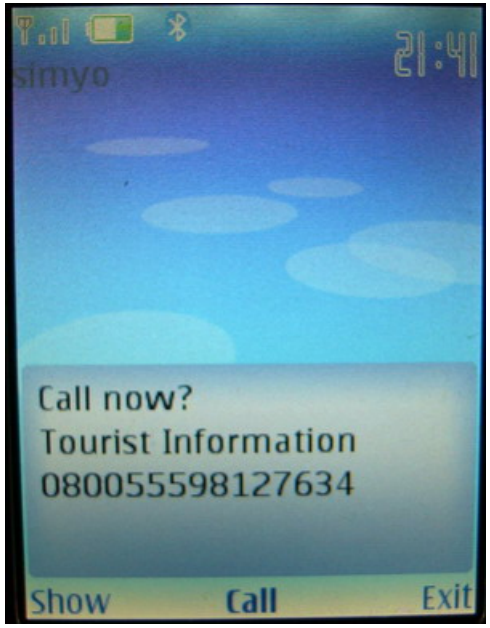
Spoofing

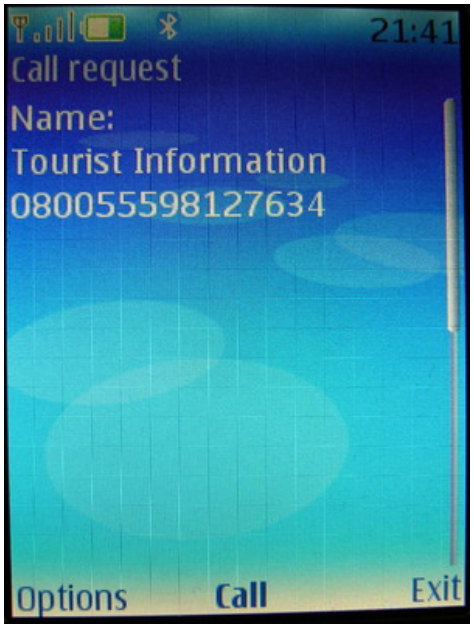
- Cloning RFID tag
  - One can fake the “unique” ID [2]
  - Underlying problem in current biometric passport [4,5]

[2] http://www.openpcd.org

Virus

- Example: SmartPoster
  - URI “`tel:0900942234711`”
  - Title “`Tourist Information\r080055598127634 \r\r\r\r\r\r\r\r`”





Telephony URI Spoofing [6]

Introduction

Technology

Security Threats

Solutions and Analysis

Summary

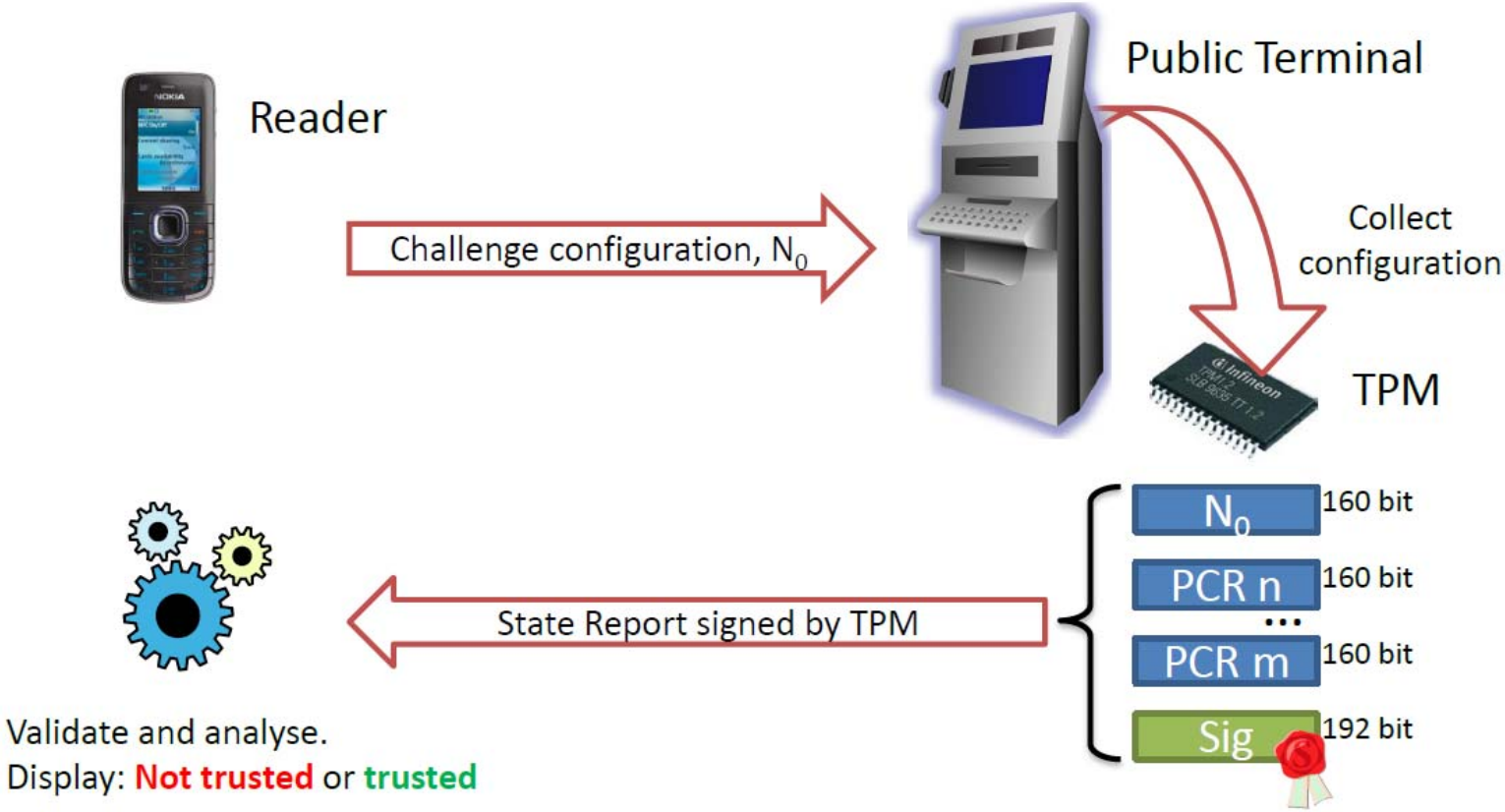
On the RF Infrastructure

- Eavesdropping
  - No protection, easy to decode [9]
  - Attacker can receive RF signal up to 10m
- Data corruption
  - No protection against RFID jamming
  - Secure channel (e.g. public-key)
- Man-in-the-middle attack
  - Possible but very difficult
  - Attacker has to align the RF field to both sender and receiver
- Relay attack
  - Time constraints [3]
  - attack time < normal response time. Fail

Trusted Platform Module

- Secure channel between user and public terminals
  - NFC-enabled TPM on vending machines
- Public key infrastructure
  - Elliptic curve cryptography (ECC), as suggested in [9]
  - Sign internal configuration with user's message
  - User checks signature with an attestation
- Against spoofing
  - Can't reproduce the same TMP without cracking ECC
- Against man-in-the-middle attack
  - NFC module is integrated into TPM
  - User and terminal located in proximity

Trusted Platform Module (Cont.)



NFC remote attestation protocol [7]

Introduction

Technology

Security Threats

Solutions and Analysis

Summary

Summary

- NFC does not provides security itself
  - RFID Infrastructure (ISO 14443) is vulnerable
  - Developing standards
- Solutions
  - Avoid contactless if possible (biometric passport)
  - Use a public key based data exchange channel
- Pros and Cons
  - Good for: ticketing, device paring
  - Be aware of: electronic payment, identification

References

[1] G. Madlmayr, J. Langer, C. Kantner, and Josef Scharinger. **NFC Devices: Security and Privacy**. In *Proceedings of ARES 2008*.

[2] R. Gomes. **Introduction to NFC**. *16th IST Mobile & Wireless Communications Summit*. Budapest, Hungary, July 2007.

[3] G. Hancke, K. Mayes and K. Markantonakis. **Confidence in Smart Token Proximity: Relay Attacks Revisited**. *Elsevier Computers & Security*, June 2009.

[4] A. Juels, D. Molnar, and D. Wagner. **Security and Privacy Issues in E-passports**. In *Proceedings of SECURECOMM 2005*.

[5] J.-H. Hoepman et al. **Crossing Borders: Security and Privacy Issues of the European E-Passport**. In *IWSEC 2006*.

[6] C. Mulliner. **Vulnerability Analysis and Attacks on NFC-enabled Mobile Phones**. In *Proceedings of IWSS at ARES 2009.*

[7] M. Hutter, R.Toegl. **A Trusted Platform Module for Near Field Communication.** In *Proceeding of ICSNC 2010*.

[8] J.H. Conway. **On Numbers and Games**. Academic Press, 1976.

[9] E. Haselsteiner and K. Breitfuss. **Security in near field communications (NFC)**. In *Workshop on RFID security*, 2006.

http://vimeo.com/4561032