Security on Smart Card and RFIDs

Dr LM Cheng
Department of Computer Engineering and Information Technology

Magnetic Card

- composed of a layer of magnetic material for storing information
- easy to carry
- can be use for authentication
- ISO 7811
Magnetic stripe Content of Financial Cards

Max Capacity ~ 1K bit
**Major Problems - Fraud card activities**

- **Stealing** — A legal card may be stolen and used in ATMs or EPOSs.
- **Altering and re-embossing** a genuine card, that is modifying the visual features of card.
- **Skimming** or altering the original electronic data stored on the magnetic stripe, for example the expire date or the credit limit.
- **Buffering** or re-encoding the original data to the magnetic card. This technique is commonly used in producing card counterfeits of store-value ticket.

- **Copying** of data from a genuine card to another in an on-line fashion — “white plastic fraud”
- **Counterfeiting** — “color plastic fraud” may be prepared by reading another legal card and encoding the same information onto another fraud card in an off-line fashion.
Valid Card
Fraud Card

**Smart Card**

- Integrated Circuit - chip
- originated from France
- invented in 70 and matured in 90
- Magnetic Card replacement
Types of Smart Card

- Memory Card
- MPU IC card
- Crypto-processor card
- Contactless card
Examples

- Memory Card – prepay card
- MCU card – SIM card
- Crypto-processor card – Smart HKID card
- Contactless card - Octopus

Advantages of Smart Card

- Large storage capacity
- more security features
- multiple functions
- flexibility in use - intelligent, lower power consumption, effective packaging
- as access card, electronic purse, debit/credit cards, ID card etc. - particular off-line applications
**Smart Card Software**

- Intelligent Chip Operating System - COS
- Encryption techniques - RSA & DES
- Multiple Application Requirements
  - Bank, library, Digital Signature, ePurse

**Open Platforms**

Open Platforms are developed to support multiple applications, they are:
- Multos (HKID card)
- Java (SIM/G3 mobile phone)
- Window for Smart Card (WfSC)
- Linux
Standardization

ID-1 Card
ISO 7816

Contact Card
ISO 7816

Contactless Card

CICC Close Couple
ISO 10536

PICC
ISO 14443

PICC
ISO 15693

All range
ISO 18000

Memory Card
Processor Card
Dual Interface 13.56 MHz

RFID

Basic Internal Structure of a Most Advanced CPU Smart Card
Basic Internal Structure of a RFID

Possible Attacks on Smart Card

*UV or X-ray inspection:* use high efficiency UV or X-ray to inspect the memory areas to extract important information like PIN, secret key and public key

*EM analysis:* use electron microscope to inspect the internal structure of the mask
confusion: disturb the power supply/frequency during PIN verification by resetting the PIN, or confusing the accurate enter of PIN or allowing access to the protected memory

duplication: illegal copying of card content from one to another using block memory movement
tracking: based on the protocol exchange between the terminal and the card to track the sequence of commands

Statistical Power Attacks:
- Attack on DES & RSA using SPA & DPA
- Use relationship of power with respect to the key data manipulation to unveil the entire key or portion or key
Multiple OS Security
- Access to native code caused the portability of code
- Exception propagation problems for Denial of Services attack
- Multiple applications and applet firewalling against illegal access
- Object-sharing loopholes against role and privilege attack
- Treatment of garbage applets for information leakage attack

General Smart Card Security Features

- Against UV or X-ray inspection:
  - Using implementation to avoid visible of ROM Code

- EM analysis:
  - Address Scrambling of memories

- Against confusion:
  - Low/High voltage sensors
  - Low/High Frequencies sensors
  - High Frequency Protection
- **Against duplication:**
  - Security PROM Hardware Protected
  - Unique Chip Identification Number
  - Move Code Blocking
- **Against Tracking:**
  - Secure authentication and data/key encryption
- **Against DPA:**
  - Random Wait State (Advance)
  - Current Scrambling Generator (Advance)
- **Against Multiple application OS:**
  - Using logistic (management) methods for security control

---

**Is Smart Card Secure?**

- There is no 100% secured/perfect system available
- System design and built for minimal attack risk can be treated as secure
- Secure system are evaluated/classified in different levels using international standards such as TCSEC/DoD (Orange Book-USA), ITSEC (Europe) and CCITSE (ISO15408)
Trusted Computer Security Evaluation Criteria – USA(DoD)

- **D**: Minimal protection
  - No protection
- **C1**: Discretionary Security Protection
  - Use control access
- **C2**: Controlled Access Protection
  - Use accountability/auditing
- **B1**: Labelled Security Protection
  - Use sensitivity (classification) labels
- **B2**: Structured Protection
  - Use formal security policy more resistant to penetrate
- **B3**: Security domain
  - Highly resistant to penetration. Use security administrator, auditing events and system recovery process
- **A1**: Verified protection
  - Highly assure of penetration. Use formal specification and verification approaches.
Information Technology Security Evaluation Criteria (ITSEC) and Common Criteria (CC) – Europe&Canada

- EAL1 - functional tested
- EAL2 - structurally tested
- EAL3 - methodologically tested and checked
- EAL4 - methodologically designed, tested and reviewed
- EAL5 - semiformally designed and tested
- EAL6 - semiformally verified designed and tested
- EAL7 - formally verified designed and tested

Federal Information Processing Standards (FIPS) - evaluation

- FIPS46-2 and 81 for DES
- FIPS 186 for Digital Signature
- FIPS 140-2 for Cryptographic Modules
Security evaluation requirements

- Cryptographic modules
- module interface
- role and services
- finite state machine model
- physical security
- Environmental Failure Protection/Testing (EFT/EFP)
- Software security

- Operation security
- cryptographic key management
- cryptographic algorithm
- EMI/EMC
- self tests