Smart Cards & Cryptography and IT Security

Ahmad Boorghany
boorghany@ce.sharif.edu

Spring 2014
Outline

- Why smart cards?
- Smart card types
- Chip types in smart cards
  - Memory Cards
  - Microprocessor Cards
- PKCS#11
- Java Cards
Why Smart Cards?
Why Smart Cards?

- E-Commerce
- Bank Issued Smart Cards
- SIM Cards and Telecommunication
- Loyalty and Stored Value
- Healthcare Informatics
- Enterprise and Network Security
- Physical Access
Smart Card Types

- Contact Cards

Images Courtesy of Wikipedia (link)
Smart Card Types

- **Contact Cards**

![Diagram of a contact card](Image Courtesy of Wikipedia (link))

- Chip Adhesive
- Metal Contacts
- Active Chip Side
- Chip
- Encapsulation Substrate
- Bond Wire
- Hotmelt
- Card Body

Image Courtesy of Wikipedia (link)
Smart Card Types

- Contactless Cards

Image Courtesy of Wikipedia (link)
Smart Card Types

- **Other Types:**
  - SIM Sized!

Image Courtesy of SIMPLE Mobile (link)
Smart Card Types

Other Types:
- SIM Sized!
- Dual Interface Cards
- Hybrid Cards
- NFC (Near Field Comm.)

Image Courtesy of aliexpress.com (link)
Image Courtesy of MER Group (link)
Image Courtesy of CASIO (link)
Smart Card Types

- Other Types:
  - SIM Sized!
  - Dual Interface Cards
  - Hybrid Cards
  - NFC (Near Field Comm.)
  - Multi-component Cards
### Chip Types

- **Memory Card**
  - Mifare Classic (of NXP)
  - SLE5528 (of Infineon)

![Image of Chip Types](link)
Chip Types

- Memory Card
  - Mifare Classic (of NXP)
  - SLE5528 (of Infineon)

Image Courtesy of FuzzySecurity (link)
Mifare Classic is Cracked

- Encryption algorithm reverse-engineered.

Image Courtesy of Karsten Nohl (link)
Mifare Classic is Cracked

- Encryption algorithm reverse-engineered.

Image Courtesy of Karsten Nohl (link)
Mifare Classic is Cracked

- Encryption algorithm reverse-engineered.
- Design weaknesses
- 48-bit key can be brute-forced.

Image Courtesy of Karsten Nohl (link)
Chip Types

- Microprocessor Cards
  - A full-fledged microcontroller
  - Programmable for any application
  - Smart Card OS
    - Windows for Smart Cards!
  - Examples:
    - PKI Functionalities
    - Supporting PKCS#11/MS-CAPI
    - Java Cards
    - MultiOS
Microprocessor Cards

- CPU
  3 ~ 32 MHz
- RAM
  1 ~ 8 KB
- ROM
- EEPROM
  20 ~ 200 KB
- Co-processor
- Flash Memory

Image Courtesy of Gorferay (link)
PKCS#11

- A standard from RSA in PKCS series
- **Interface** to cryptographic modules:
  - Smart Cards, Tokens, HSM, TPM, ...
- Widely supported by 3\textsuperscript{rd}-party applications:
  - (Local/Remote) Login
  - Thunderbird
  - Firefox
  - OpenSSL (+other software using this)
- Microsoft competitor: MS-CAPI
PKCS#11

- Concepts/Features:
  - Session
  - Objects: Data, Keys (Symmetric, Asymmetric)
  - Mechanisms:
    - CKM_AES_CBC
    - CKM_MD5_HMAC
    - CKM_RSA_PKCS_KEY_PAIR_GEN
  - Attributes:
    - CKA_LABEL
    - CKA_NEVER_EXTRACTABLE
PKCS#11 Demo
Java Cards

- Traditional Programming for Smart Cards:
  - Various and Confidential Chips Instructions
  - Specific for a Type of Smart Card
  - Programmed Once while Manufacturing

- Java Card: A specification from Oracle

- A (very) simplified Java language for smart cards

- Alternatives:
  - MultOS
  - Basic Cards
  - .NET Cards
Java Card Benefits

- High-level Language: Easy to program
- Compiled & Stored in EEPROM
- Multi Application

Image Courtesy of Erik Poll (link)
Java Card Benefits

- High-level Language
- Compiled & Stored in EEPROM
- Multi Application
- App. Firewall
- Post Issuance
- Vendor Indep.
- Open Standard

Image Courtesy of Erik Poll (link)
Java Card Language

- Subset of Java
  - No Threads, Doubles, Strings, Multi-dimensional arrays
  - Very restricted API
  - Optional support of *int* and garbage collection
  - 16-bit arithmetic

- With some extras:
  - APDU and RMI API
  - Persistent & Transient data (in RAM & EEPROM, resp.)
  - Crypto API
  - Transaction Mechanism
16-bit Arithmetic

- Nightmare of *(short)*s!

```java
short s; byte b;
s = b+s+1;
   // not ok, compiler complains
s = (short)(b+s+1);
   // not ok, converter complains
s = (short)(b+(short)(s+1))  // ok
```

Code Image Courtesy of Erik Poll ([link](link))
private int balance;
private int[] log;
//@ invariant (* log[n] is previous balance *);
...

// Update log
n++;
log[n] = balance;
//@ Update balance
balance = balance - amount;

what if a card tear occurs here?
Transactions

```java
private int balance;
private int[] log;
//@ invariant (* log[n] is previous balance *);
...

JCSSystem.beginTransaction();
    // Update log
    n++;
    log[n] = balance;
    // Update balance
    balance = balance - amount;
JCSSystem.commitTransaction();
```

Code Image Courtesy of Erik Poll [link]
Java Card Demo

(Look at the next slide first!)
- Application Programming Data Units
- ISO/IEC 7816-4 standard for high-level communication with smart cards.
- Similar to network frames and packets
Thanks for your attention.