Security of Metro – Subway
Smartcard and farecards

ECE646: Cryptography and Computer Network Security

Hunter, Corzo
Introduction

- Nearly all metro systems around the world use some kind of smartcard for fare collection.
- Smartcards have security features over RFID tokens and paper farecards.
Metro (WMATA) Operation

- Metrorail fares – SmarTrip or paper farecard
- Metrobus – SmartTrip or cash
- Parking – SmartTrip or cash
DC Metro System

- Minimum balance to enter is $1.20.
- You can leave the Metro with negative balance.
- Maximum load is $300.
- Card cost is $5.00 (real cost is $3.40) and minimum balance one can buy is $5.00.
- If a person is more than 4 hours in the system, the rider must talk to a manager when exiting.
Magnetic Stripe Cards

- Paper farecards
- Can hold up to $45.00
- Not likely to be secure
- Being phased out for cost and fraud reasons
- Doesn't appear to be encrypted
- Cloning attack seems possible due to lack of hardware protection
Anatomy of a Magcard Attack

- Need magnetic card reader / writer.
- Read raw data from card.
- Data can be copied to another card using writer (cloning).
Possible Forging

- Read mag card before taking a ride.
- Read mag card after taking a ride.
- Notices changes in the data and correlate.
- Iterate and figure out which bytes stores the value.
- Reverse engineer.
- Modify the value at will.

FREE RIDES
Contactless Smartcards

- ISO 14443 is the standard for contactless Near Field Communication
- Chip is powered by radio waves emanated from card reader.
- Generally credit card sized.
- ISO/IEC 14443 uses following terms for components:
  - PCD: proximity coupling device (the card reader)
  - PICC: proximity integrated circuit card
Smartcards Features

• Available crypto systems in hardware.
• Authentication.
• MIFARE is a trademark of NXP Semiconductors.
• MIFARE is a technology that has been selected for most contact-less smartcard projects worldwide.
Smartcard Attacks

- Cloning/modification attacks.
- Replay attacks.
- Skimming attacks.
- Eavesdropping.
- Relay attacks.
Current SmarTrip

- Known as GOCard type and currently in circulation.
- ISO 14443 Type B
- Also used by Chicago Transport Authority.
- WMATA is introducing MIFARE plus cards into the system.
- Both card types use ISO-14443 communication protocol.
# GOCard vs Plus

<table>
<thead>
<tr>
<th></th>
<th>GOCard</th>
<th>MIFARE Plus</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>ISO 14443 type B</td>
<td>ISO 14443</td>
</tr>
<tr>
<td>Crypto</td>
<td>3DES</td>
<td>128-bit AES</td>
</tr>
<tr>
<td>Memory</td>
<td>2KB</td>
<td>2KB or 4KB</td>
</tr>
<tr>
<td>Op. Frequency</td>
<td>13.5 MHz</td>
<td>13.5 MHz</td>
</tr>
<tr>
<td>Chip Manufacturer</td>
<td>Fujitsu MB89R118</td>
<td>NXP</td>
</tr>
</tbody>
</table>
MIFARE Plus and Smartrip

- Based on smartrip use and operation, WMATA must store at least value, last time scanned, last station code, and maybe other non-disclosed information.

- All the keys in all the cards are different and derived using key diversification.
MIFARE Attacks

- MIFARE classic was partially reverse engineered by Karsten Nohl in 2008.
- Later on, the dutch research group cloned MIFARE classic card and discovered other vector attacks.
- MIFARE classic proprietary CRYPTO-1 was broken.
- The best attack was able to clone card in 10 seconds without the need of a valid card reader.
- Companies are implementing more cryptographic algorithm standards rather than proprietary algorithms.
MIFARE Plus cards support one pre-personalization and 3 security levels. Cards operate in one security level at any given time and can only be switched to a higher level.

- **Security Level 0**: MIFARE Plus cards are pre-personalized with configuration keys, level switching keys, MIFARE Classic CRYPTO1 and AES keys for the memory.

- **Security Level 1**: In this level the cards are 100% functionally backwards compatible with MIFARE Classic 1K and MIFARE Classic 4K cards. Cards work seamlessly in existing MIFARE Classic infrastructure.

- **Security Level 2**: Mandatory AES authentication. MIFARE Classic CRYPTO1 for data.

- **Security Level 3**: Mandatory AES for authentication, communication confidentiality and integrity. Optional proximity detection (MIFARE Plus X only).
Security Levels

- **MIFARE Classic**
  - Level 0
  - Optional AES authentication
  - Program AES level switching keys (mandatory)
  - Program Crypto 1 and AES keys per sector (recommended)

- **MIFARE Plus Level 0**
  - Level 0
  - Multi sector authentication
  - Optional Random ID
  - Proximity Check
  - Anti-tearing for keys & sector trailers

- **MIFARE Plus Level 1**
  - Level 1
  - One mandatory AES authentication
  - Memory access using MIFARE Crypto with session keys
  - Optional AES authentication possible

- **MIFARE Plus Level 2**
  - Level 2

- **MIFARE Plus Level 3**
  - Level 3
  - AES for authentication, data encryption and integrity
  - Functional backwards compatible with MIFARE Classic
Key Diversification

- On the case of the Smartrip, diversification is done based on the Electronic Chip I.D.
- It uses AES-128 encryption scheme.
SmarTrip implemented with MIFARE
MIFARE Plus Security

- MIFARE Plus supports a key diversification scheme to prevent that different cards use the same keys. This ensures that even if one card gets compromised, the rest of the system remains secure.

- The protection of data sessions uses session keys, which are generated from two random values negotiated between card and reader during authentication.
Recommendations

- Enable proximity check which is offered by the MIFARE Plus X architecture to impede relay attacks.
- Update mechanism for master keys.
- Implement anti cloning mechanism.
- Phase out paper farecards.
THANK YOU
WMATA requires that the smartrip cards must support key diversification.

MIFARE Plus X supports this and does this through using CMAC for sub-key generation.
MIFARE Plus X Operation

- The UID is programmed into a locked NV-memory by the manufacturer.
- The PCD typically polling for PICCs in the field. This is done with the REQA. When a PICC is within the operating range of the PCD and receives the REQA, any MIFARE PICC returns the ATQA.

![Diagram of MIFARE Plus X Operation](image)
MIFARE Plus X Operation

- Anti-collision loop and UID.

---

Fig 2. Anticollision Loop as part of the Card Activation Sequence

(1) The CT (= Cascade Tag, Type A) byte indicates that the UID is not received completely yet. It indicates that another anticollision loop on the next higher cascade level is required to get the complete UID.
# Security Level Comparison

<table>
<thead>
<tr>
<th>Features</th>
<th>MIFARE Plus S</th>
<th>MIFARE Plus X</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Export controlled</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Security Level 0</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personalization</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Security Level 1</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fully MIFARE classic compatible</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Optional AES authentication</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Security Level 2</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AES authentication + MIFARE classic crypto</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Security Level 3</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AES authentication</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Data encryption by AES</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Data integrity by AES</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Encrypted update of keys</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Multi sector authentication, read &amp; write</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Full virtual card concept support</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Proximity check</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Extra commands to make transaction faster</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Value blocks supported</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Random ID</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>