Breaking Korea Transit Card with Side-Channel Attack -Unauthorized Recharging-

Black Hat Asia 2017

Tae Won Kim, Tae Hyun Kim, and Seokhie Hong
1. Attack Goal & Scenario
2. Target Device Details
   - Introduction of Target Device
   - Authentication Protocol Analysis
   - Cryptosystem
3. Key Recovery Attack
   - Attack environment & Measurement Set-Up
   - Attack Overview
   - Attack Results
4. Recharging Simulation
5. Conclusion
1. Attack Goal & Scenario

2. Target Device Details
   – Introduction of Target Device
   – Authentication Protocol Analysis
   – Cryptosystem

3. Key Recovery Attack
   – Attack environment & Measurement Set-Up
   – Attack Overview
   – Attack Results

4. Recharging Simulation

5. Conclusion
Recharging on Transit Card

USER

Vending & Reload Device

Payment
Recharging on Transit Card
Our Ultimate Goal

Free recharging as much as attacker want
Attack Scenario toward Goal

Phase 1. Extract authentication key for recharging using side-channel analysis attack
Attack Scenario toward Goal

Phase 1. Extract authentication key for recharging using side-channel analysis attack

Phase 2. Design free recharging tool with restored key
Phase 1. Extract authentication key for recharging using side-channel analysis attack

Phase 2. Design free recharging tool with restored key
1. Attack Goal & Scenario

2. Target Device Details
   - Introduction of Target Device
   - Authentication Protocol Analysis
   - Cryptosystem

3. Key Recovery Attack
   - Attack environment & Measurement Set-Up
   - Attack Overview
   - Attack Results

4. Recharging Simulation

5. Conclusion
Target device

• Transit card
  – Pre-paid transit card for the freeway in Korea
  – Over 800 million cards were issued and used
  – Cafeteria and convenience store in the freeway service area
  – Movie theater, Airport car park etc...

• Contact Smartcard
  – Equipped with cryptographic engine in hardware level
  – Countermeasure employed against side-channel attacks
  – Support ISO/IEC 7816 standard and KS X 6924 Korea standard
## Authentication protocol for recharging

<table>
<thead>
<tr>
<th>Transit Card</th>
<th>Card reader</th>
<th>Secure Access Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>Random Number – 1 gen</td>
<td>Request recharging</td>
<td></td>
</tr>
<tr>
<td>Session key – 1 gen ( E( \text{Random Number-1, Card Key} ) )</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Signature – 1 gen ( E( \text{Card information, Session key-1} ) )</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Roles:
- **Transit Card**
- **Card reader**
- **Secure Access Module**

### Information:
- **Public information**
- **Secret information**
- **Crypto algorithm**
## Authentication protocol for recharging

### Transit Card

- **Random Number – 1 gen**
- **Session key – 1 gen**
  \[ E(\text{Random Number-1, Card Key}) \]
- **Signature – 1 gen**
  \[ E(\text{Card information, Session key-1}) \]

### Card reader

- **Request recharging**

### Secure Access Module

- **Card Key gen**
  \[ E(\text{Card information, Master Key}) \]
- **Session key – 1 gen**
  \[ E(\text{Random Number – 1, Card Key}) \]
- **Verify Signature – 1**
## Authentication protocol for recharging

<table>
<thead>
<tr>
<th>Transit Card</th>
<th>Card reader</th>
<th>Secure Access Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>Random Number – 1 gen</td>
<td>Request recharging</td>
<td></td>
</tr>
<tr>
<td>Session key – 1 gen</td>
<td>E( Random Number-1 , Card Key )</td>
<td></td>
</tr>
<tr>
<td>Signature – 1 gen</td>
<td>E ( Card information , Session key-1 )</td>
<td></td>
</tr>
<tr>
<td>Card Key gen</td>
<td>E( Card information , Master Key )</td>
<td></td>
</tr>
<tr>
<td>Session key – 1 gen</td>
<td>E( Random Number – 1 , Card Key )</td>
<td></td>
</tr>
<tr>
<td>Verify Signature – 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Random Number – 2 gen</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Session key – 2 gen</td>
<td>E( Ran Number-2 , Session Key-1 )</td>
<td></td>
</tr>
<tr>
<td>Signature – 2 gen</td>
<td>E ( Card info , Session key-2 )</td>
<td></td>
</tr>
</tbody>
</table>
Authentication protocol for recharging

Transit Card

- Random Number – 1 gen
- Session key – 1 gen
  \[ E(\text{Random Number -1}, \text{Card Key}) \]
- Signature – 1 gen
  \[ E(\text{Card information}, \text{Session key-1}) \]

Card reader

- Request recharging
- Random Number – 1, Card Information, Signature – 1

Secure Access Module

- Card Key gen
  \[ E(\text{Card information}, \text{Master Key}) \]
- Session key – 1 gen
  \[ E(\text{Random Number -1}, \text{Card Key}) \]
- Verify Signature – 1
- Random Number – 2 gen
- Session key – 2 gen
  \[ E(\text{Random Number -2}, \text{Session Key-1}) \]
- Signature – 2 gen
  \[ E(\text{Card info}, \text{Session key-2}) \]
- Verify Signature – 2
- Recharging
## Authentication protocol for recharging

<table>
<thead>
<tr>
<th><strong>Transit Card</strong></th>
<th><strong>Card reader</strong></th>
<th><strong>Secure Access Module</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Random Number – 1 gen</td>
<td>Request recharging</td>
<td>Card Key gen</td>
</tr>
<tr>
<td>Session key – 1 gen</td>
<td></td>
<td>E( Card information, Master Key )</td>
</tr>
<tr>
<td>E( Random Number-1, Card Key )</td>
<td></td>
<td>Session key – 1 gen</td>
</tr>
<tr>
<td>Signature – 1 gen</td>
<td></td>
<td>E( Random Number – 1, Card Key )</td>
</tr>
<tr>
<td>E( Card information, Session key-1 )</td>
<td></td>
<td>Verify Signature – 1</td>
</tr>
<tr>
<td>Session key – 2 gen</td>
<td></td>
<td>Random Number – 2 gen</td>
</tr>
<tr>
<td>E( Ran Number-2, Session Key-1 )</td>
<td></td>
<td>Session key – 2 gen</td>
</tr>
<tr>
<td></td>
<td></td>
<td>E( Ran Number-2, Session Key-1 )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Signature – 2 gen</td>
</tr>
<tr>
<td></td>
<td></td>
<td>E( Card info, Session key-2 )</td>
</tr>
<tr>
<td>Session key – 2 gen</td>
<td></td>
<td>Signature -2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Send card a valid signature !!</td>
</tr>
</tbody>
</table>
## Authentication protocol for recharging

<table>
<thead>
<tr>
<th>Transit Card</th>
<th>Card reader</th>
<th>Secure Access Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>Random Number – 1 gen</td>
<td>Request recharging</td>
<td>Card Key gen</td>
</tr>
<tr>
<td>Session key – 1 gen (E\left( \text{Random Number-1}, \text{Card Key} \right))</td>
<td>(E\left( \text{Card Information}, \text{Signature – 1} \right))</td>
<td>(E\left( \text{Card information}, \text{Master Key} \right))</td>
</tr>
<tr>
<td>Signature – 1 gen (E\left( \text{Card information}, \text{Session key-1} \right))</td>
<td>(E\left( \text{Random Number – 1, Card Information, Signature – 1} \right))</td>
<td>Session key – 1 gen (E\left( \text{Random Number – 1, Card Key} \right))</td>
</tr>
</tbody>
</table>

### Secure Access Module

- **Card Key gen**
  \(E\left( \text{Card information}, \text{Master Key} \right)\)
- **Session key – 1 gen**
  \(E\left( \text{Random Number – 1, Card Key} \right)\)
- **Verify Signature – 1**
- **Random Number – 2 gen**
- **Session key – 2 gen**
  \(E\left( \text{Random Number-2, Session Key-1} \right)\)
- **Signature – 2 gen**
  \(E\left( \text{Card info, Session key-2} \right)\)

### Target

- **Random Number – 1, Card Information, Signature – 1**

### Send card a valid signature !!

- **Session key – 2 gen**
  \(E\left( \text{Random Number-2, Session Key-1} \right)\)
- **Verify Signature - 2**
- **Recharging**
**Authentication protocol for recharging**

### Transit Card
- Random Number – 1 gen
- Session key – 1 gen
  \[ E(\text{Random Number-1}, \text{Card Key}) \]
- Signature – 1 gen
  \[ E(\text{Card information}, \text{Session key-1}) \]

### Card reader
- Request recharging
  \[ \text{Target} \]
- Random Number – 1 , Card Information, Signature – 1

### Secure Access Module
- Card Key gen
  \[ E(\text{Card information}, \text{Master Key}) \]
- Session key – 1 gen
  \[ E(\text{Random Number – 1}, \text{Card Key}) \]
- Verify Signature – 1
- Random Number – 2 gen
- Session key – 2 gen
  \[ E(\text{Ran Number-2}, \text{Session Key-1}) \]
- Signature – 2 gen
  \[ E(\text{Card info}, \text{Session key-2}) \]
- Send card a valid signature !!
- Recharging

**Public information**
- Secret information
- Crypto algorithm

---

Transit Card

- Random Number – 1 gen
- Session key – 1 gen
  \[ E(\text{Random Number-1}, \text{Card Key}) \]
- Signature – 1 gen
  \[ E(\text{Card information}, \text{Session key-1}) \]

Card reader

- Request recharging
  \[ \text{Target} \]
- Random Number – 1 , Card Information, Signature – 1

Secure Access Module

- Card Key gen
  \[ E(\text{Card information}, \text{Master Key}) \]
- Session key – 1 gen
  \[ E(\text{Random Number – 1}, \text{Card Key}) \]
- Verify Signature – 1
- Random Number – 2 gen
- Session key – 2 gen
  \[ E(\text{Ran Number-2}, \text{Session Key-1}) \]
- Signature – 2 gen
  \[ E(\text{Card info}, \text{Session key-2}) \]
- Send card a valid signature !!
- Recharging
Crypto Algorithm Analysis

1. **Sign & verify**
   
   
   => performs crypto Algorithm

2. **128-bit Block cipher & operation mode**
   
   - Crypto function => Two Triple-DES
   - Cipher Block Chaining (CBC) mode

3. **Initial Vector**
   
   - $0^{128}$

4. **Signature value**
   
   - Most significant 32-bit of last ciphertext block

5. **Padding rule**
   
   - $80 \ 00 \ 00 \ 00 \ ...$
Outline

1. Attack Goal & Scenario
2. Target Device Details
   - Introduction of Target Device
   - Authentication Protocol Analysis
   - Cryptosystem
3. Key Recovery Attack
   - Attack environment & Measurement Set-Up
   - Attack Overview
   - Attack Results
4. Recharging Simulation
5. Conclusion
**Attack Environment**

- Attack under the secure transit card
  - APDU commands for recharging the card

- Hardware
  - Board
  - Card reader
  - Oscilloscope
  - Spectrum Analyze

- Software
  - For the acquisitions (Customized)
  - Signal preprocessing (Customized)
  - Analysis (Customized)
  - Matlab

---

**Measurement setup**
Phase 1: Locate the position of T-DES

1. I/O signal analysis
2. Visual Inspection
   - Find similar patterns
3. Plaintext CPA
   - Find location of relating plaintext
   - Can deduce location of target operation from plaintext location
**Attack Overview**

**Phase 2 : DPA Attack for key recovery**

1. Pre-processing
   - Compression
   - Alignment

2. First Round attack in the DES
   - 48-bit Key recovery
   - 6-bitwise CPA

3. Correction of error
   - Prevent error propagation
   - Method based on BS-CPA

4. 2-15 Round attack
   - 56-bit full-key recovery
   - 32-bitwise CPA

---

**Phase 1 : Locate the position of T-DES**

1. I/O signal analysis
2. Visual Inspection
   - Find similar patterns
3. Plaintext CPA
   - Find location of relating plaintext
   - Can deduce location of target operation from plaintext location
Attack Overview

Phase 1: Locate the position of T-DES
1. I/O signal analysis
2. Visual Inspection
   - Find similar patterns
3. Plaintext CPA
   - Find location of relating plaintext
   - Can deduce location of target operation from plaintext location

Phase 2: DPA Attack for key recovery
1. Pre-processing
   - Compression
   - Alignment
2. First Round attack in the DES
   - 48-bit Key recovery
   - 6-bitwise CPA
3. Correction of error
   - Prevent error propagation
   - Method based on BS-CPA
4. 2-15 Round attack
   - 56-bit full-key recovery
   - 32-bitwise CPA

Phase 3: Verification of restored the key
- Compare the signature value through card response with the signature value generated by recovered key
- This is only way to confirm the validity
Attack Overview

Phase 1: Locate the position of T-DES
1. I/O signal analysis
2. Visual Inspection
   - Find similar patterns
3. Plaintext CPA
   - Find location of relating plaintext
   - Can deduce location of target operation from plaintext location

Phase 2: DPA Attack for key recovery
1. Pre-processing
   - Compression
   - Alignment
2. First Round attack in the DES
   - 48-bit Key recovery
   - 6-bitwise CPA
3. Correction of error
   - Prevent error propagation
   - Method based on BS-CPA
4. 2-15 Round attack
   - 56-bit full-key recovery
   - 32-bitwise CPA

If fail, return to the beginning
Repeat until the key is found
Tremendous trials and errors!!

Phase 3: Verification of restored the key
- Compare the signature value through card response with the signature value generated by recovered key
- This is only way to confirm the validity
Some Problems for Key Recovery

• Hiding Countermeasure
  – Pre-processing for mitigation
    • Filtering, Alignment
  – Increases the number of traces

• Alignment
  – Align, whenever guess the location of target operation
  – There is no good reference pattern
    • By effect of hiding countermeasure
  – Need elaborated work
    • One or two point of misalignment leads to attack failure

• More requirement of time cost, memory
  – Compression of trace
  – Parallel processing
Visual Inspection

- Search for similar patterns
- Execution of three crypto function
  
  \[
  \Rightarrow 6 \text{ T-DES}
  \]
**Plaintext CPA**

- Perform after alignment
- Result of CPA

=> Indicate location relating to plaintext
Plaintext CPA

- Perform after alignment
- Result of CPA

=> Indicate location relating to plaintext

8-Byte plaintext correlation coefficient peaks

Mean trace
Two possible intervals for target operation

Which one is exact?

=> only can be identified through CPA attack for key recovery

8-Byte plaintext correlation coefficient peaks
Correlation Coefficients for the first Round of DES

- Correlation Coefficients for the first Round of DES
Full Key Recovery

- Correlation coefficients for the Hamming distances between rounds (2-15) of the T-DES
- Correct key guess => Observe 14 peaks
Verification of Restored Entire Key

Response values from the card including signatures

Generated signatures by ourselves

Same
1. Attack Goal & Scenario
2. Target Device Details
   – Introduction of Target Device
   – Authentication Protocol Analysis
   – Cryptosystem
3. Key Recovery Attack
   – Attack environment & Measurement Set-Up
   – Attack Overview
   – Attack Results
4. Recharging Simulation
5. Conclusion
(a) Before recharging, check balance with ATM

(b) Balance : 20,050 (₩)

(c) Recharging Tool

(d) Execution of our recharging program.
   Insert amount of money you wish to recharge => 10,000 (₩)

(e) Completion of recharging

(f) After recharging, Balance : 30,050 (₩)
1. Attack Goal & Scenario
2. Target Device Details
   – Introduction of Target Device
   – Authentication Protocol Analysis
   – Cryptosystem
3. Key Recovery Attack
   – Attack environment & Measurement Set-Up
   – Attack Overview
   – Attack Results
4. Recharging Simulation
5. Conclusion
Conclusion

• Demonstrated that side-channel analysis attack is serious threat in real-world
  – Hacking the Korea transit card in a black-box manner
  – Showing financial damage through unauthorized recharging balance

• Practical attack
  – Trials and errors
    • Approx. six months
  – Current extracting key in same device
    • Approx. 63 hours (trace collection : 58 hours + Attack : 5 hours)

• Further works
  – For black box attack, combination of reverse engineering and side-channel attack
  – Go on attack for any commercial devices!
More details?
Could please see white paper
&
Questions?
ktw@sntworks.kr

Thank you 😊