Test Vehicle for Java Card

September 20, 2012
Toru Hashimoto
IT Security Center (ISEC)
Information-technology Promotion Agency, JAPAN (IPA)
Contents

1. Introduction of Japan’s Scheme
2. Test Vehicle
3. Attack Methods for IC chips
4. Java Card and GlobalPlatform
5. Test Vehicle for Java Card
6. Future Plan
Japan’s Common Criteria Scheme

• JISEC: Japan IT Security Evaluation and Certification Scheme
• IPA: The Certification Body of JISEC
• JISEC has been established in 2001, certifying software-related products only.
Beginning of Hardware Certification

• We have established hardware security evaluation program within JISEC scheme under METI’s leadership.
• It has just begun very recently: The first ITSEFs to evaluate hardware have been approved this year!

METI: Ministry of Economy, Trade and Industry
Checking Skills of ITSEFs

• One problem: How to check the ability of candidate ITSEFs for hardware evaluation?
• Various skills are needed for penetration testing hardware product.

• Test Vehicle is a solution.
Contents

1. Introduction of Japan’s Scheme

2. Test Vehicle

3. Attack Methods for IC chips

4. Java Card and GlobalPlatform

5. Test Vehicle for Java Card

6. Future Plan
What is the Test Vehicle?

- Test Vehicle is a security hardware product in the form of smartcard with some deliberately embedded vulnerabilities.
- A candidate ITSEF demonstrates their ability of penetration testing by attacking it.
- Difficulty for breaking the test vehicle is tuned so that only the skilled candidate ITSEFs should be able to attack successfully.
Previous Work

- IPA funded to develop Test Vehicle of native smart card in 2011.
- These attack methods are covered:
  - Physical Attacks
  - Perturbation Attacks
  - Side Channel Attacks
  - Fault Injection Attacks
  - Software Attacks
1. Introduction of Japan’s Scheme
2. Test Vehicle
3. Attack Methods for IC chips
4. Java Card and GlobalPlatform
5. Test Vehicle for Java Card
6. Future Plan
Attack Methods

• Invasive Attacks
  – Bus Probing
  – ROM Reading

• Semi-invasive Attacks
  – Perturbation Attacks
  – Fault Injection Attacks

• Non-Invasive Attacks
  – Power Analysis
  – Electromagnetic Analysis
Perturbation Attacks

- **Methods**
  - Glitch
  - Laser

- **Effect**
  - Instruction skip
  - Register value change

```java
enter PIN;
if (PIN is incorrect) {
    goto error;
}
proceed...
```
Power Analysis

- Measure power consumption during operation
  - Recover the secret value like a cryptographic key
  - Analyze the operation running inside the chip

![Graph showing power consumption data]
Contents

1. Introduction of Japan’s Scheme
2. Test Vehicle
3. Attack Methods for IC chips
4. Java Card and GlobalPlatform
5. Test Vehicle for Java Card
6. Future Plan
• Open standards architecture for dynamic multi-application card schemes
GlobalPlatform

- Runtime Environment
- Card Manager
- Security Domains
- GlobalPlatform API
- Card Content
GlobalPlatform Security

- On-Card Components’ Security Requirements
- Cryptographic Support
  - Integrity and Authentication
  - Secure Messaging
- Installation of Applications is permitted only with at least an appropriate secure-channel established.
Java Card

- Based on Java Technology
- Can have Java-based applications, named applets
- Can have multiple applets
Security Mechanisms of Java Card

• Type Safety
  – Taking an integer value and reinterpret as a value of different type (type confusion) is forbidden.

• Byte-code Verifier
  – Performed offcard or oncard

• Defensive Virtual Machine
  – Executing illegal byte code is blocked.

• Firewall
  – Data in an applet is protected from other applets.
Type Safety

• Any reference can be dereferenced only as a reference of the original type.

• What if a byte array is accessed as a short array?

<table>
<thead>
<tr>
<th>Read as byte[4]</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>00</td>
<td>01</td>
<td>02</td>
<td>03</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Read as short[4]</th>
<th>0</th>
<th>2</th>
<th>4</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0001</td>
<td>0203</td>
<td>XXXX</td>
<td>XXXX</td>
</tr>
</tbody>
</table>

• Accessing beyond the array bound!

• This is called ‘type confusion’.
Type Safety

- Illegal class cast is prohibited: This is enforced by compiler and runtime environment.

```java
class A {}
class B extends A {}
class C {}
A a;
B b;
C c;
```

<table>
<thead>
<tr>
<th>cast attempt</th>
<th>result</th>
</tr>
</thead>
<tbody>
<tr>
<td>(A)b</td>
<td>O.K. No problem.</td>
</tr>
<tr>
<td>(B)a</td>
<td>ClassCastException is thrown if a is not an object of class B.</td>
</tr>
<tr>
<td>(A)c</td>
<td>Compile Error</td>
</tr>
</tbody>
</table>
Java Card System Security

- Java Card is protected by various security techniques
  - Combined with GlobalPlatform prohibits installation of applets unless authenticated.
  - Byte Code Verifier and Defensive Virtual Machine (if implemented) enforce type safety.
  - Java Card Firewall prohibits accessing unauthorized access to another applet’s data.

- How ITSEFs can evaluate that a Java Card product is really implemented securely?
1. Introduction of Japan’s Scheme
2. Test Vehicle
3. Attack Methods for IC chips
4. Java Card and GlobalPlatform
5. Test Vehicle for Java Card
6. Future Plan
Java Card

- Specifications of GlobalPlatform and Java Card enforce security in theory.
- However, Java Card security could be breakable if implementation is done carelessly, as well as a native smart card is.
Test Vehicle for Java Card

• There are Java Card specific attack methods that are not covered by the native Test Vehicle.

• Therefore, we have developed Test Vehicle for Java Card so as to make it possible to assess the evaluators’ ability of penetration testing of Java Card.

• Test Vehicle defines some attack scenarios regarding partial attack techniques and also combined attacks.
Development

- Test Vehicle for Java Card is sponsored by IPA and developed by Trusted Labs.
Attacking GlobalPlatform

- Installing an applet is allowed only with opening a secure channel.

- How does GlobalPlatform Card Manager determine if secure channel is opened?

- If this decision logic consists of only a single conditional branch, it could be bypassed by perturbation attacks.
Type Confusion

- Causing type confusion somehow to access memory beyond its own applet’s boundary.
- The following methods could be effective if implementation is flawed:
  - Modify CAP file and load an ill-formed applet
  - Bypass On-Card verifier somehow
  - Abuse Transaction Mechanism
Firewall Attack

- Find a way to access another applet’s data, for example:
  - Realize type confusion, i.e. convert an integer value to an object reference.
  - Invoke a private method of another applet.
Full Attack Path

- A full attack against a Java Card is a combination of partial attacks, for example:
  - Find flaws of the implementation.
  - Develop a malicious applet that causes type confusion.
  - Install the malicious applet by attacking GlobalPlatform.
1. Introduction of Japan’s Scheme
2. Test Vehicle
3. Attack Methods for IC chips
4. Java Card and GlobalPlatform
5. Test Vehicle for Java Card
6. Future Plan
Future Plan

- Fine Tuning the Test Vehicle for Java Card
  - Tune the difficulty so that attacking needs state-of-art skill but breakable within practical time scale.
  - The fine tuning will be completed by the end of 2012.
Thank you for your attention.

IT Security Center
IPA, Japan

JISEC Information
URL:
English: http://www.ipa.go.jp/security/jisec/jisec_e/