Are Embedded Secure Elements more secure than traditional smart cards?

Marc Witteman (Riscure)
Hans van Tilburg (Visa)

Cartes America 2014
Outline

- Introduction
- eSE concepts
- eSE in practice
- Conclusion
Background
- eSE is a secure microcontroller
- eSE becomes standard component in smart phones
- eSE used to enable secure apps like payment

Research questions
- How secure is an embedded secure element (eSE)?
- What is the impact on certification?

Approach
- Use smart card as reference
- Compare design and implementation
Security Evaluation & Certification

Certification of payment IC cards and USIMs

Application

OS

Chip

ICC evaluation

Platform evaluation

IC evaluation
Security evaluation methods

- **Physical**
  - Microscopic inspection
  - Tapping & Modification

- **Logical**
  - Scanning & fuzzing
  - Data corruption

- **Side Channel**
  - Observation of leakage
  - Key extraction

- **Fault Injection**
  - Environment manipulation
  - Privilege escalation
### Security Evaluation Rating

<table>
<thead>
<tr>
<th>Factor</th>
<th>Identification</th>
<th>Exploitation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elapsed time</td>
<td>0-5</td>
<td>0-8</td>
</tr>
<tr>
<td>Expertise</td>
<td>0-7</td>
<td>0-6</td>
</tr>
<tr>
<td>Knowledge of target</td>
<td>0-9</td>
<td>0-5</td>
</tr>
<tr>
<td>Access to target</td>
<td>0-3</td>
<td>0-6</td>
</tr>
<tr>
<td>Equipment</td>
<td>0-7</td>
<td>0-8</td>
</tr>
<tr>
<td>Open samples</td>
<td>0-6</td>
<td></td>
</tr>
<tr>
<td><strong>Sub total</strong></td>
<td><strong>0-37</strong></td>
<td><strong>0-33</strong></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>0-70</strong></td>
<td></td>
</tr>
</tbody>
</table>

- Rating made for successful attacks
- More points = More difficult
- Smart card certification requires 31 points
Outline

- Introduction
- eSE concepts
- eSE in practice
- Conclusion
eSE concepts

Contactless card emulation

Multi-point configuration
SC vs. eSE – Conceptual comparison

**Smart Card**
- Simple card management
  - Single management entity
- ISO 7816 and/or ISO 14443 interface
- User control of peer and session

**eSE**
- Complex card management
  - Multiple actors,
- SWP, DWP, I²C, USB, proprietary interface
- Host control of peer and session
Outline

- Introduction
- eSE concepts
- eSE in practice
- Conclusion
eSE teardown
eSE anatomy

- Embedded Secure Element
- Silicon spacer
- NFC Controller
- Metal carrier/heat sink
- PIN
### SC vs. eSE – Practical comparison

<table>
<thead>
<tr>
<th>Smart Card</th>
<th>eSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embedded in a plastic card</td>
<td>Packaged as SMD component, Embedded in a smart phone</td>
</tr>
<tr>
<td>Price of a single smart card $1…$20</td>
<td>Price of a smart phone $200…$900</td>
</tr>
<tr>
<td>Attack window limited by short sessions</td>
<td>Attack window unlimited while always-on</td>
</tr>
<tr>
<td>Replaceable hardware, card disabling mitigates attacks</td>
<td>Permanent hardware, eSE disabling unattractive</td>
</tr>
</tbody>
</table>
## Security impact

<table>
<thead>
<tr>
<th>Attack type</th>
<th>Good for eSE</th>
<th>Bad for eSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Semi)invasive</td>
<td>• Packaging is hurdle for attack</td>
<td>• Not tamper evident</td>
</tr>
<tr>
<td></td>
<td>• Samples expensive</td>
<td>• Samples unrestricted</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Less disabling</td>
</tr>
<tr>
<td>Logical</td>
<td></td>
<td>• Attack window unlimited</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Sensitivity to Man-In-The-Middle attack</td>
</tr>
</tbody>
</table>
Outline

• Introduction
• eSE concepts
• eSE in practice
• Conclusion
Evaluation impact

Small for IC evaluation

• Consider different protocols

Big for Platform & ICC evaluation

• eSE no longer stand-alone but integrated in the system
• Logical access unrestricted
• Limited scope of logical testing today
• Different threat environment
Mitigations

Man-In-The-Middle attacks

- Include NFC controller in logical evaluation scope
- Use certified TEE for router config

Remote attacks

- More focus on logical evaluation
- Use network penetration style methods
Conclusion

- Embedded Secure element not more secure than smart cards
- New threats and risks identified
- Evaluation scope & methods need update
Challenge your security

Contact: Marc Witteman
CTO

Riscure B.V.
Frontier Building, Delftechpark 49
2628 XJ Delft
The Netherlands
Phone: +31 15 251 40 90

www.riscure.com

Riscure North America
71 Stevenson Street, Suite 400
San Francisco, CA 94105
USA
Phone: +1 650 646 99 79

inforequest@riscure.com