CC for Smart Cards and Mobile Security

Wouter Slegers
<table>
<thead>
<tr>
<th></th>
<th>Smartcard* (1999-now)</th>
<th>last 5 years</th>
<th>last 1.5 years</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>All</strong></td>
<td>52%</td>
<td>46%</td>
<td>41%</td>
</tr>
<tr>
<td>≧EAL4+**</td>
<td>79%</td>
<td>89%</td>
<td>86%</td>
</tr>
<tr>
<td><strong>VAN.5</strong>*</td>
<td>98%</td>
<td>92%</td>
<td>92%</td>
</tr>
</tbody>
</table>

* excludes smartcards in the “Other devices” (i.e. EU Tachograph), “Products for Digital Signatures” (i.e. EU digital signature cards), “Trusted Computing” (i.e. TPMs format smartcards) etc

** Only impactful augmentations: ALC_FLR.x excluded

*** not all entries specify AVA_VAN levels
Joint Interpretation Library

Application of Attack Potential to Smartcards

Joint Interpretation Library

Attack Methods for Smartcards and Similar Devices

Joint Interpretation Library

Security requirements for post-delivery code loading

Joint Interpretation Library

Minimum Site Security Requirements

Joint Interpretation Library

Collection of Developer Evidence

SOG-IS Crypto Working Group

SOG-IS Crypto Evaluation Scheme
Agreed Cryptographic Mechanisms
Attacks and ratings
Separating weak from strong
Separating \textit{weak} from strong
Separating weak from strong
JHAS: Attack methods and Attack Potential

Application of Attack Potential to Smartcards

Attack Methods for Smartcards and Similar Devices
Deconstructing a ‘Secure’ Processor

Black Hat – Washington D.C.

Christopher Tarnovsky
Flylogic, Inc.
chris@flylogic.net – http://www.flylogic.net
### Beyond limit of the attacker (31 points)?

<table>
<thead>
<tr>
<th></th>
<th>Identification</th>
<th>Exploitation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td><strong>Points</strong></td>
<td><strong>Name</strong></td>
</tr>
<tr>
<td><strong>Time</strong></td>
<td><em>6+ months</em></td>
<td><em>5 – ∞</em></td>
</tr>
<tr>
<td><strong>Expertise</strong></td>
<td>Expert</td>
<td>5</td>
</tr>
<tr>
<td><strong>Knowledge</strong></td>
<td>Public - Sensitive</td>
<td>0 - 7</td>
</tr>
<tr>
<td><strong>Access</strong></td>
<td>&lt; 1000</td>
<td>0 – 3</td>
</tr>
<tr>
<td><strong>Equipment</strong></td>
<td>Specialized-bespoke</td>
<td>3 – 5</td>
</tr>
<tr>
<td><strong>Open samples</strong></td>
<td>None</td>
<td>0</td>
</tr>
<tr>
<td><strong>Sub total</strong></td>
<td><em>13 – ∞</em></td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Joint Interpretation Library

Minimum Site Security Requirements
SOG-IS Crypto Working Group

SOG-IS Crypto Evaluation Scheme
Agreed Cryptographic Mechanisms
Joint Interpretation Library

Composite product evaluation for Smart Cards and similar devices

Object: Define concept and methodology applicable to composite product evaluation.

Version 1.4
August 2015

JavaCard
Crypto Library
Hardware
Hardware:
- PP-0035/0084
- Promises:
  - Protection from outside*
  - Crypto does not leak*
  - Possibility to make secure software*
IC+Crypto lib:
• PP-0035/0084
  • + Packages
• Promises:
  • Protection from outside*
  • Crypto does not leak*
  • Possibility to make secure software*
JavaCard:

- HW+Crypto Library+JavaCard
- Java Card PP (Open/Closed configuration)

Promises:
- Applets are protected from each other*
- Applets are protected from outside*
- Standard crypto is available
Full smart card:

- ePassport ("MRTD": Machine Readable Travel Document)
- Digital Signature cards ("SSCD": Secure Signature Creation Device)
- Digital Tachograph
- Travel systems (Mifare)
- Payment cards
Composition advantages:
• Efficient re-use of certifications
• Different developers / labs / certification bodies possible

Costs
• Dependencies between projects
JavaCard

Hardware

Crypto Library

Applet

Applet

Applet

1.5y

1.5y
No key needed to access the mezzanine level
Beyond **time** limit of the attacker (>3 months)?

<table>
<thead>
<tr>
<th></th>
<th>Identification</th>
<th>Exploitation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td><strong>Points</strong></td>
<td><strong>Name</strong></td>
</tr>
<tr>
<td><strong>Time</strong></td>
<td><strong>not practical</strong></td>
<td><strong>&lt;1 day - &lt;1 week</strong></td>
</tr>
<tr>
<td><strong>Expertise</strong></td>
<td>Expert</td>
<td>Expert</td>
</tr>
<tr>
<td><strong>Knowledge</strong></td>
<td>Public - Sensitive</td>
<td>Public</td>
</tr>
<tr>
<td><strong>Access</strong></td>
<td>&lt; 1000</td>
<td>&lt;10 - &lt;100</td>
</tr>
<tr>
<td><strong>Equipment</strong></td>
<td>Specialized-bespoke</td>
<td>Specialized-bespoke</td>
</tr>
<tr>
<td><strong>Open samples</strong></td>
<td>None</td>
<td>0 -</td>
</tr>
<tr>
<td><strong>Sub total</strong></td>
<td><strong>13 – ∞</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td><strong>11 – 20</strong></td>
</tr>
</tbody>
</table>