ICCC 2012 - Experience
Certification of a loader integrated in a secure microcontroller: strategic stakes

Christiane DROULERS
STMicroelectronics
Secure MCU Division
Agenda

Presentation

• A new generation of Secure MCUs
• Impacts on the CC evaluation approach
• STMicroelectronics approach for the ST33 loader certification
• Conclusion
A new generation of Secure Microcontrollers
A new generation of Secure MCUs: purpose

• The trend is to offer more and more applications on a single chip, increasing Non Volatile Memory size
  • High-end SIM
  • Secure element for NFC (Near Field Communication) products

• Smartcard & Similar Devices vendors (our direct customers) need
  • More supply chain flexibility
  • Shortened time-to-market because of a very dynamic and competitive market

• A high level of security is needed
  • Assets more attractive to attackers, growing risk of exposure to attacks
  • Evolving state-of-the-art of attacks
  • Potential very hostile operational environment
  • Possible co-existence of many different applications on the same chip
A new generation of Secure MCUs: solution

• The new Secure Flash Microcontrollers provide
  • Very dense Non Volative Memory (NVM) capacity up to 1 Mbyte and more
  • A different product lifecycle, allowing more flexibility and a shortened time-to-market for new OSs & applications

• The Common Criteria certification guarantees
  • An evaluation against state-of-the-art attacks
    • High attack potential (AVAN.5) required by the Protection Profile
    • JIL Attack Methods document and Application of attack potential document
  • An evaluation with high development standards (EAL4/5)

• There is only one applicable Protection Profile
  • BSI-PP-0035 “Security IC Platform Protection Profile”
  • Mentions this new kind of MCU (lifecycle) without adapting the Security Problem Definition to late code loading
  • Cannot include specific SFRs because it requires strict conformance, and the loader is an optional element
Impacts on the CC evaluation approach
BSI-PP-0035 defines a generic TOE lifecycle:

1. **Phase 1**: Security IC Software Development
   - Security IC Software Developer

2. **Phase 2**: Security IC Development
   - TOE manufacturer

3. **Phase 3**: Security IC Manufacturing
   - TOE manufacturer

4. **Phase 4**: Security IC Packaging
   - Card manufacturer

5. **Phase 5**: Composite Product Integration
   - End user

6. **Phase 6**: Personalisation

7. **Phase 7**: Operational Usage
Impacts on evaluation: lifecycle (2/2)

- Delivery of the Security IC Software may take place at different steps

**Phase 1**  
Security IC Software Development  
If implemented in ROM and EEPROM

**Phase 2**  
Security IC Development

**Phase 3**  
Security IC Manufacturing

**Phase 4**  
Security IC Packaging

**Phase 5**  
Composite Product Integration

**Phase 6**  
Personalisation

**Phase 7**  
Operational Usage

If loaded into the NVM

After TOE Delivery, the TOE is in an operational environment, not covered by ALC-DVS, but by AGD

ICCC 2012: Certification of a loader in a Secure MCU  19/09/2012
Impacts on the evaluation: How?

• A loader integrated in the Secure MCU must be part of the TOE

• Either without impacting the Security Problem Definition => loader just declared
  • The SFRs from the Protection Profile will apply to it, without really addressing it
  • It will be added in the ADV, ATE & AGD documentation
  • It will be assessed against AVA_VAN.5

• Or impacting the Security Problem Definition => functional augmentation
  • Specific threats or security policies are defined
  • Resulting in specific SFRs, then verified in depth during the vulnerability analysis

• The second strategy was chosen by STMicroelectronics (ST) for its ST33 family
STMicroelectronics approach for the ST33 loader certification
## ST approach: Loader security features

<table>
<thead>
<tr>
<th>Security features</th>
<th>Purpose</th>
<th>Main SFRs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication of loading authority</td>
<td>Avoid abuse of functionality in protected production environment</td>
<td>Security attribute based access control (FDP_ACF.1)</td>
</tr>
<tr>
<td>Loading of encrypted code</td>
<td>Ensure code confidentiality during transport and loading</td>
<td>Import of user data without security attributes (FDP_ITC.1)</td>
</tr>
<tr>
<td>Code integrity check during loading</td>
<td>Ensure code integrity</td>
<td></td>
</tr>
<tr>
<td>Loading mechanism not usable after loading (before Phase 7)</td>
<td>Avoid abuse of functionality in end-user environment</td>
<td>Limited capabilities (FMT_LIM.1) Limited availability (FMT_LIM.2) Guidance</td>
</tr>
</tbody>
</table>
ST approach: Impact on the Security Target

• The Loader is explicitly part of the TOE

• Functional augmentations related to the Loader:
  • One OSP / one Objective “Controlled loading of the Security IC Embedded Software”
  • 8 SFRs (Security Functional Requirements):
    • 6 defined in CC part 2
    • 2 defined in the PP (CC part 2 extended)
  • 2 SFPs (Security Function Policies) linked to the SFRs
ST approach: Impacts on the evaluation

• Impact on CC classes / families:
  • ASE: Functional augmentations to the Security Target
  • ADV: Loader functionalities and design detailed in all deliveries (ADV_ARC, ADV_FSP, ADV_TDS, ADV_IMP)
  • ATE: Loader functionalities detailed in all deliveries + related evaluator functional testing (ATE_IND)
  • ALC: Adapted delivery and new lifecycle for loader (ALC_DEL). Loader integrated into all other ALC families.
  • AGD: Specific User Manual in AGD_PRE, Installation Manual in AGD_OPE
  • AVA_VAN: Vulnerability analysis including loader and related to specific SFRs claimed in the Security Target @ AVA_VAN.5 (code review, penetration testing, fault injection, …)

• Impact on evaluation workload:
  • Reasonable increase, proportional to the loader functionalities
ST approach: Results / benefits

- First certificate in 2010, last one in 2011 (ANSSI-CC-2011/07), maintained and in surveillance in 2012

- Customer confidence: our customers use ST’s loader, including some who had their own loader

- Customer development savings: no need to develop their own loader

- Customer composite evaluation savings and simplification: the loader is fully evaluated during the platform certification

- Customer supply chain rationalization:
  - Allows versatile code loading strategy, from Phase 3 up to Phase 6
  - Better protection of customer code during transportation and code loading
Conclusion
Conclusion

- The development of loaders is a recent evolution in the Smartcard and Similar Devices domain

- The BSI-0035-PP cannot be fully adapted to this new optional element of the TOE (due to strict conformance)

- The definition of associated constraints and/or related functional augmentations to the Security Target could be a future project for the ISCI working group 1 (supporting document)
• Questions and answers

• Duly limited by confidentiality constraints
Thank you for your attention