Smartcard security development using formal method tool SPIN

Naohisa ICHIHARA
Hiroyuki KAMODA, Hiroyuki OGURO

NTTDATA Corporation

Copyright © 2008 NTT DATA Corporation
Contents

1. Background
2. Key to succeed
3. Modeling
4. Modeling framework
5. Example
6. Summary
1. Background

- CC evaluation experience (for smartcard)
  - (1) Smartcard “Xaica-alpha” for JUKI-card, EAL4+, DCSSI (France), CC v2.1, 2005
  - (2) Smartcard “Xaica-alpha 64K” for e-Passport, EAL4+ (includes ADV_SPM.3), CC v2.3, DCSSI (France), 2007

- Why Formal methods?
  - Technical challenge as R&D
  - Establish high quality security development
2. Key to succeed

● Preparation:
  - Understanding of ADV_SPM.3, AIS 34
  - Study of Formal methods
  - Technical Approach
    • Scope of modeling
    • Choice of tool (to modelize and prove)
    • Step toward the goal
  - Draw up a project
    • Milestone scheduling
    • Team formation
  - Negotiation with Certification Body, ITSEF
    • Tool choice, Approach, Modeling scope, Interpretation of CC requirements, … etc
2. Key to succeed

- Technical approach
  - Scope of modeling
  - What we verify?
  - How we prove?
  - Step toward the formal modeling and verification

- Project management
  - Team formation (Developer, ST author, Formal modeler)
  - Formal Method Education
  - Internal Review
  - External Meeting/Review with ITSEF, CB
2. Key to succeed

- Internal Review (in detail)

Model is correct, from ST, TSP and CC requirement points of view

Model is correct, from TOE design and implementation points of view

Model is correct, from formal and logical points of view
2. Key to succeed

- External Review (in detail)

ST
TOE Design
TOE Implementation

TOE Model
(Abstract Model)

Formal Model
(Model Works on Tool)

Sponsor

Model satisfies requirements of ADV_SPM.3 as well as AIS34

Recommends;
- Apply AIS34
- Understand the Formal method tool, approaches and models

ITSEF

CB

- AIS34 as interpretation
- Formal method tool could be applied
3. Modeling

- Approach overview (and why SPIN/Promela?)


- Step 1. TSP definition
- Step 2. Transform to State transition model

- Step 3. Risk definition
  Risk1 = 3 c t
  Risk2 = 2 b p

- Step 4. Implementation and verification

Copyright © 2007 NTTDATA Corporation

8th ICCC Presentation, Naohisa Ichihara, NTTDATA (2007)
3. Modeling

- Security Target (ST)
- TOE Security Policies
- Intended Usage
- Threats
- Security Objectives
- Security Functional Requirements
- TSFs/FSP/HLD/LLD
- TOE implementation

- TOE Model
- Verification formula
- Environment Model
  - Users
  - Scenario
- TOE Model
  - Initial status
  - Resources
  - Interface
  - Behavior

- Formal Model
  - LTL formula
  - *.ltl

- SPIN Source code
  - *.pml

Copyright © 2008 NTT DATA Corporation
3. Modeling

Security Target (ST) → TOE Model → Formal Model

Users

Scenario

Verification formula

R/W

TOE

Command

Response

Behavior

Interface

Resources

Initial status
3. Modeling

Security Target (ST) → TOE Model → Formal Model

Users

Admin (knows Key1)
Cardholder (knows Key2)
Unknown (knows nothing)

Scenario

Verification formula

Behavior

Verify
Get Data
Change Ref Data

Resources

Security Attributes
ACL
Error Limit
Status
Error Counter

External Files

Lifecycle Status
Card Status

Initial status

Example
In order to ease modeling

Security Target (ST)

Verification formula

Environment Model

TOE Model

Hard to Climb up …

LTL formula

*.ltl

SPIN Source code

*.pml

User defined model (To be tailored)

Readymade Model (e.g. Smartcard model)

Translated smoothly

LTL formula

*.ltl

SPIN Source code

*.pml

Modeling framework
## 4. Modeling framework

<table>
<thead>
<tr>
<th></th>
<th>Common</th>
<th>R/W</th>
<th>Smartcard</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Readymade</td>
<td>User defined</td>
</tr>
<tr>
<td>Verification formula</td>
<td>pattern</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Behavior</td>
<td>Channel</td>
<td>Main routine</td>
<td>Scenario</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Send command</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Receive response</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>User change</td>
<td></td>
</tr>
<tr>
<td>Users</td>
<td>-</td>
<td>Unknown user</td>
<td>(Intended) users</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Key known by user</td>
</tr>
<tr>
<td>Interface</td>
<td>-</td>
<td>Command with or without value</td>
<td>(additional) user defined commands with or without value</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Response with or without value</td>
<td></td>
</tr>
<tr>
<td>Resources</td>
<td>-</td>
<td>-</td>
<td>Environmental status</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Keys, Files with Value, Error Limit</td>
</tr>
<tr>
<td>Initial Status</td>
<td>-</td>
<td>-</td>
<td>Initial user</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Error Counter, Lifecycle status</td>
</tr>
</tbody>
</table>

- Behavior of (additional) user defined commands
5. Example (SPIN)

Security Target (ST) → TOE Model → Formal Model

(TBD)
6. Summary

● Technical approach
  - Choice of a tool e.g. SPIN
    • Easy for developer?
    • Experience of CC evaluation?
  - What we prove?
    • TSP
  - How we model?
    • Framework approach

● Project Management
  - Internal Review; share and understand the model by all those involved
  - External Meeting/Review with ITSEF, CB; negotiation