9th ICCC in Korea, 2008

Smartcard security development using formal method tool SPIN

Naohisa ICHIHARA
Hiroyuki KAMODA, Hiroyuki OGURO

NTTDATA 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

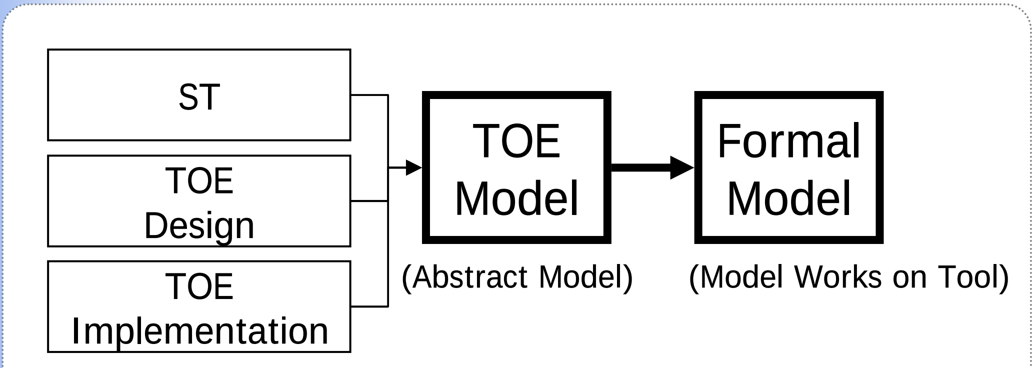
2. Key to succeed

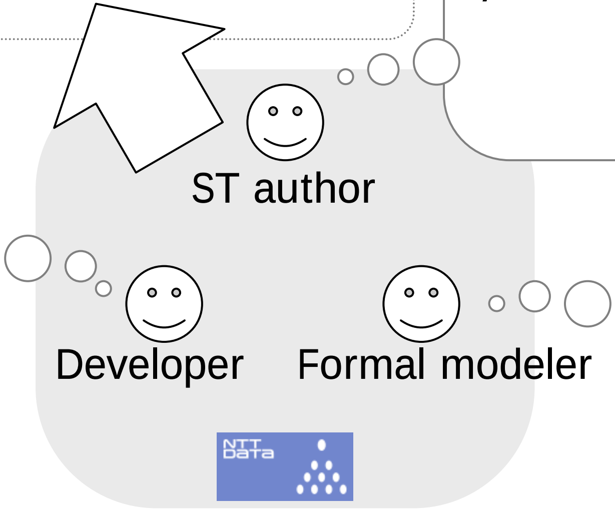
- Technical approach
  - Scope of modeling
  - What we verify?
  - How we prove?
  - Step toward the formal modeling and verification

- 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)





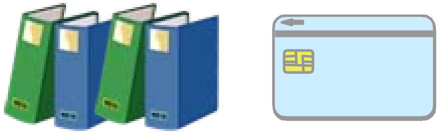
Model is correct,
from ***ST , TSP***
and CC requirement
points of view

Xaica-alpha64K
Security Target

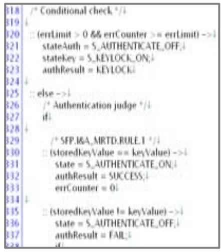
NTTDATA CORPORATION

May 9, 2008

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

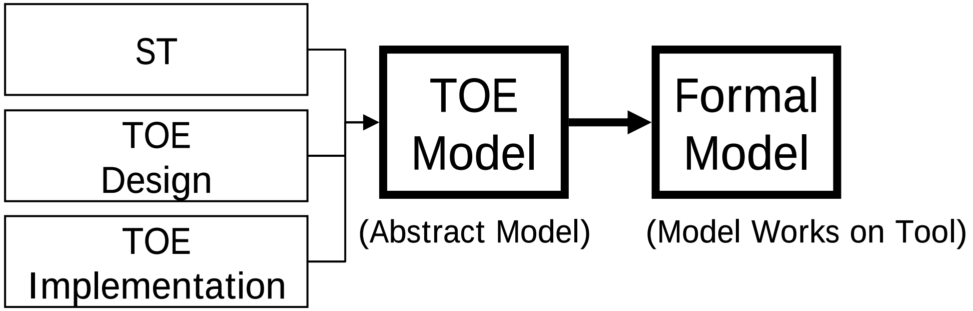


Model is correct, from ***formal and logical*** *points of view*


```
 /* Conditional check */
 
 :: (errLimit > 0 && errCounter >= errLimit) ->
     stateAuth = S_AUTHENTICATE_OFF;
     stateKey = S_KEYLOCK_ON;
     authResult = KEYLOCK
 
 :: else ->
     /* Authentication judge */
     if
 
       /* SFP.I&A_MRTD.RULE.1 */
     :: (storedKeyValue == keyValue) ->
       state = S_AUTHENTICATE_ON;
       authResult = SUCCESS;
       errCounter = 0
 
     :: (storedKeyValue != keyValue) ->
       state = S_AUTHENTICATE_OFF;
       authResult = FAIL;
       if
```

2. Key to succeed

●External Review (in detail)



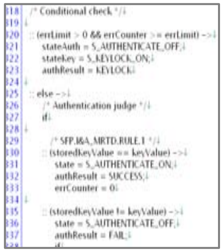
(Abstract Model)

(Model Works on Tool)

Xaica-alpha64K
Security Target

NTTDATA CORPORATION

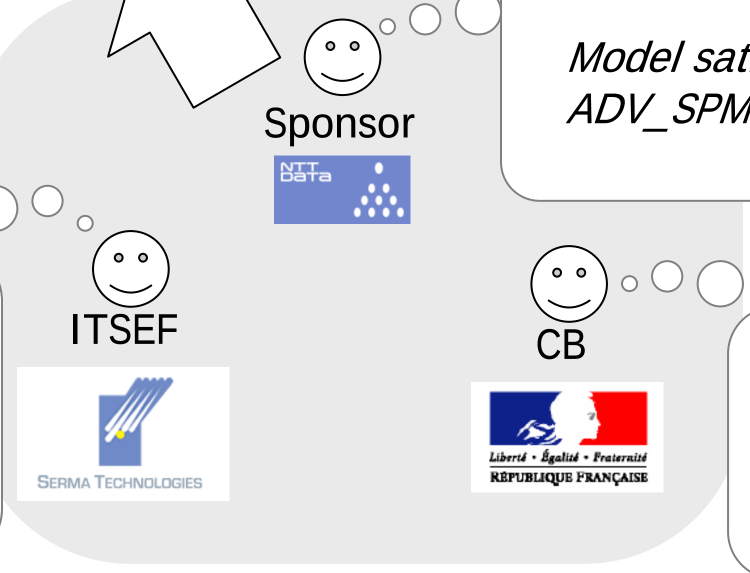
May 6, 2008



```
/* Conditional check */
:: (errLimit > 0 && errCounter >= errLimit) ->
   stateAuth = S_AUTHENTICATE_OFF;
   stateKey = S_KEYLOCK_ON;
   authResult = KEYLOCK

:: else ->
   /* Authentication judge */
   if

     /* SFP.I&A_MRTD.RULE.1 */
     :: (storedKeyValue == keyValue) ->
       state = S_AUTHENTICATE_ON;
       authResult = SUCCESS;
       errCounter = 0

     :: (storedKeyValue != keyValue) ->
       state = S_AUTHENTICATE_OFF;
       authResult = FAIL;
       if
```

Formula
Load
Operation
Property holds for: All Executions (desired behavior) No Executions (error behavior)
Notes
Use Load to open a file or a template
Symbol Definitions
Never Claim
Generate
Verification Result: valid
Run Verification
Help
Clear
Close
Save As

Model satisfies requirements of ADV_SPM.3 as well as AIS34

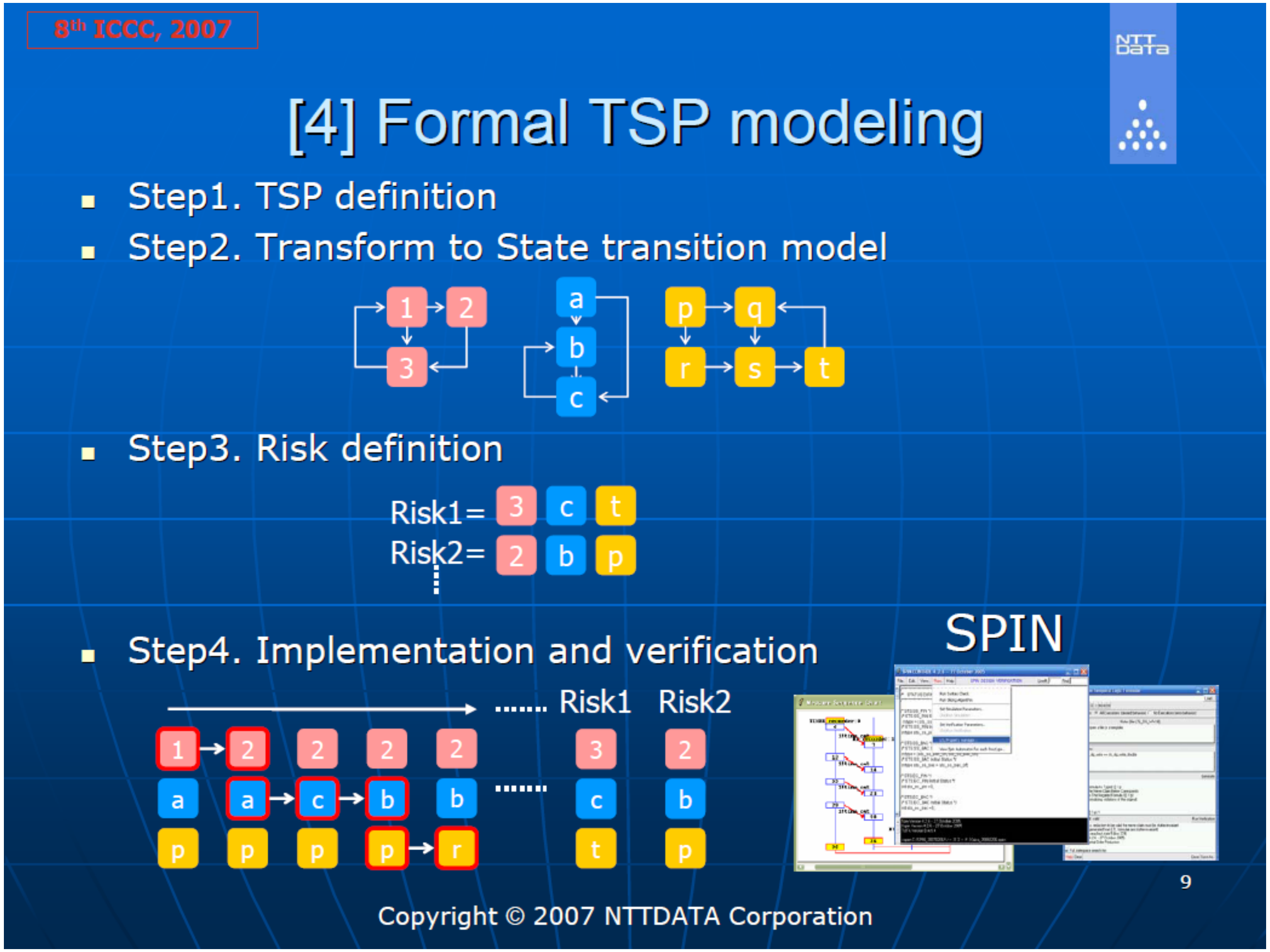


Recommends;
- Apply AIS34
- Understand the Formal method tool, approaches and models

- AIS34 as interpretation
- Formal method tool could be applied

3. Modeling

● Approach overview (and why SPIN/Promela?)



8th ICCC, 2007

[4] Formal TSP modeling

- Step1. TSP definition
- Step2. Transform to State transition model

- Step3. Risk definition

Risk1= 3 c t

Risk2= 2 b p

- Step4. Implementation and verification

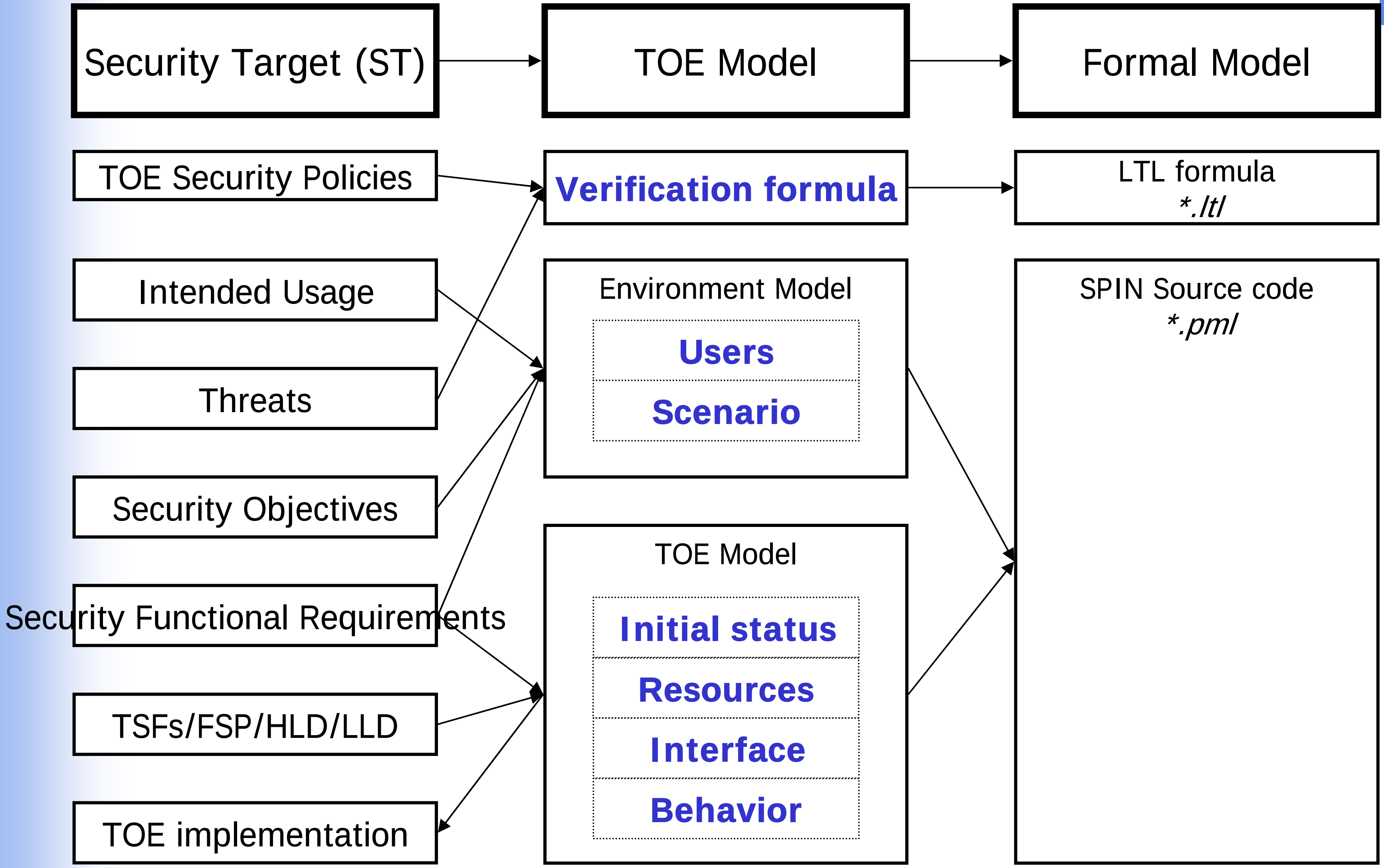
SPIN

9

Copyright © 2007 NTTDATA Corporation

8th ICCC Presentation, Naohisa Ichihara, NTTDATA (2007)

3. Modeling



Security Target (ST) → TOE Model → Formal Model

TOE Security Policies

Intended Usage

Threats

Security Objectives

Security Functional Requirements

TSFs/FSP/HLD/LLD

TOE implementation

Verification formula

Environment Model

- **Users**
- **Scenario**

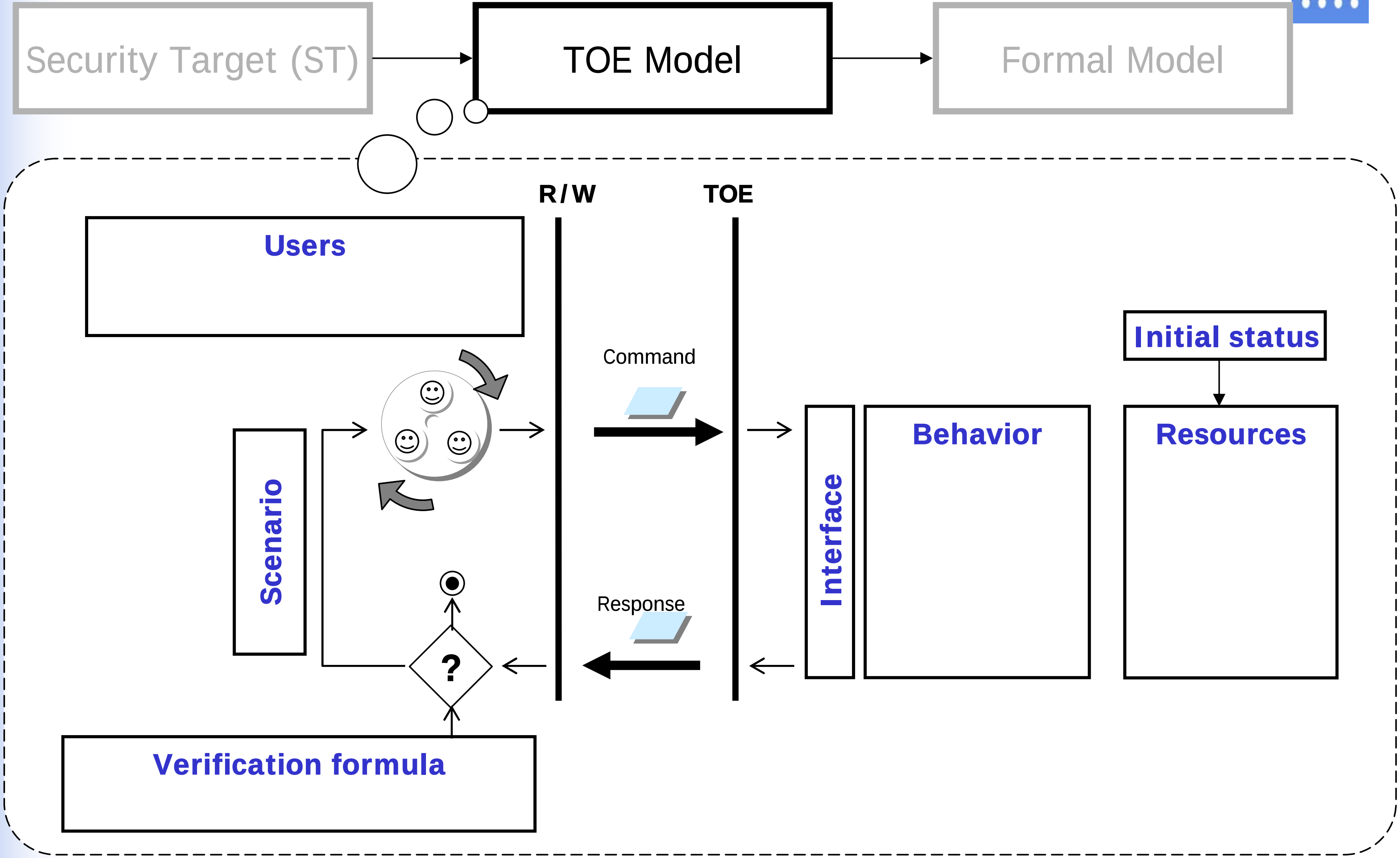
TOE Model

- **Initial status**
- **Resources**
- **Interface**
- **Behavior**

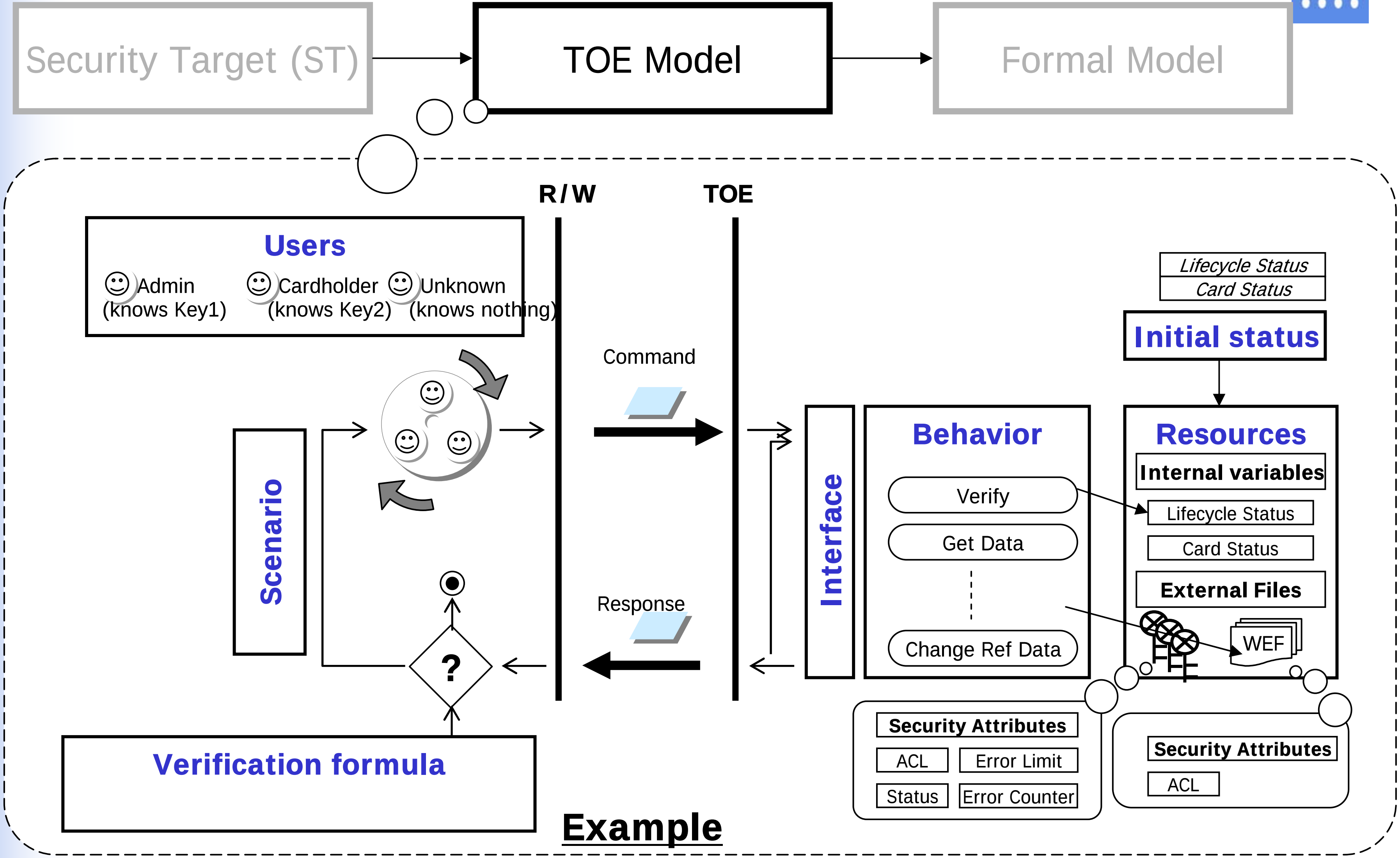
LTL formula
**.ltl*

SPIN Source code
**.pml*

3. Modeling

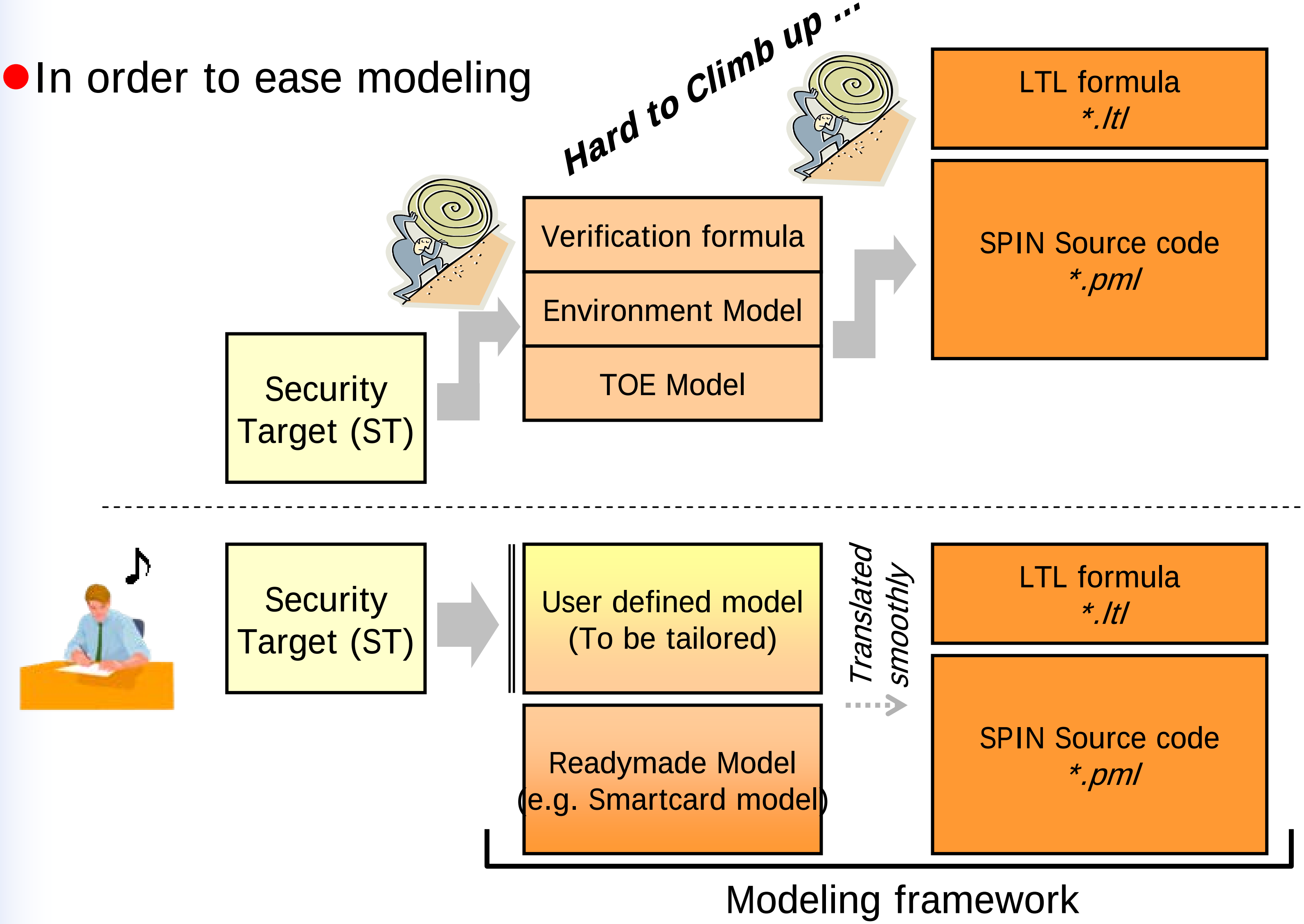

Security Target (ST)
TOE Model
Formal Model
R / W
TOE
Users
Command
Initial status
Scenario
Behavior
Resources
Interface
Response
?
Verification formula

3. Modeling


Security Target (ST)
TOE Model
Formal Model
R/W
TOE
Users
Admin (knows Key1)
Cardholder (knows Key2)
Unknown (knows nothing)
Command
Response
Scenario
?
Verification formula
Interface
Behavior
Verify
Get Data
Change Ref Data
Lifecycle Status
Card Status
Initial status
Resources
Internal variables
Lifecycle Status
Card Status
External Files
WEF
Security Attributes
ACL
Error Limit
Status
Error Counter
Security Attributes
ACL
Example

4. Modeling framework

- In order to ease modeling



Hard to Climb up …

Security Target (ST)

Verification formula

Environment Model

TOE Model

LTL formula *.ltl

SPIN Source code *.pml

Security Target (ST)

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

	Common	R/W		Smartcard	
		Readymade	User defined	Readymade	User defined
Verification formula	pattern	-	-	-	-
Behavior	Channel	Main routine Send command Receive response User change	Scenario	Main routine Receive command Dispatch Send out response Commands Authentication Access Control File access	Behavior of (additional) user defined commands
Users	-	Unknown user	(Intended) users Key known by user	-	-
Interface	-	Command with or without value Response with or without value	(additional) user defined commands with or without value	Command with or without value Response with or without value	(additional) user defined commands with or without value
Resources	-	-	Environmental status	Keys, Files with Value, Error Limit	Value, Error Limit
Initial Status	-	-	Initial user Initial environmental status	Error Counter, Lifecycle status	Error Counter, Lifecycle status

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