Final Meeting Project Test Development for GP2.1.1

G&D, 24.11.2005

Amar Khelil

Topics

- Original concept
- Overview of the B-Models developed/ generated AT
- Current State of Test Development (done/todo)
- Lessons Learned
- Some Conclusions about the Methodology

1. Original Concept

- **To develop B models in cooperation with LEIRIOS**
  - **Secure Messaging** Mechanism according to SCP01 and SCP02 as described in GP2.1.1 (ISD only)
  - **Life Cycle State Machine for card and applets** as described in GP2.1.1
  - **Dispatcher** as described in GP2.1.1
  - **Crypto-Tests** according to JC2.2
- **To generate Abstract Tests (AT) with LTG (Leirios Test Generator)**
- **To convert the AT into CASCATE Format**
- **To run the tests on target Sunflower**

2.1 Crypto; LCS of Card/Applets; B-Models

B-Models for the Crypto-Tests

- focus lies on generation of combined test cases (TC)

	jcCrypto		jcCrypto_KeyBuilder		jcCrypto_MessageDigest	
	Metrics	Comment	Metric	Comment	Metrics	Comment
ModelScope	-		-		-	
Lines of code (comments excluded)	654	total=704(comments=7,1%)	860	total=921 (comments=6,7%)	603	total=665 (comments=9,3%)

B-Models for Life Cycle States of Card and Applets

- Many transitions are irreversible. In order to minimize execution time, the generated TC must be ordered. LTG cannot do this presently.
  => Model Development has been stopped

2.2 Secure Messaging; B-Models (completed)

		Secure Messaging SCP01		Secure Messaging SCP02	
		Metrics	**Comment**	**Metrics**	**Comment**
Model Scope		-	Secure Messaging SCP01 (ISD only)	-	Secure Messaging SCP02 (ISD only)
Lines of code (comments excluded)		**543**	total = 800 (comments=32%)	**606**	total=895 (comments=32%)
Number of APDU commands		**2**	INITIALIZE_UPDATE EXTERNAL_AUTHENTICATE	**2**	INITIALIZE_UPDATE EXTERNAL_AUTHENTICATE
Number of B operations	Total	**5**		**5**	
	Target	**3**	**INITIALIZE_UPDATE** **EXTERNAL_AUTHENTICATE** **GP_CMD_SCP**	**3**	**INITIALIZE_UPDATE** **EXTERNAL_AUTHENTICATE** **GP_CMD_SCP**
	Preambule/postambule/ observation	**2**	preambule: SELECT_BY_NAME preambule: MANAGE_CHANNEL_CLOSE	**2**	preambule: SELECT_BY_NAME preambule: MANAGE_CHANNEL_CLOSE
Number of variables	Total	**6**		**9**	
	State Variables	6	Same variables used in both models	6	Same variables used in both models
	Configuration Switches	0		3	
Max Number of atomic B-expressions in a compound B-one		2		2	
Number of behaviors	Total	**215**	=208 (target) + 7 (out of focus)	**315**	=308 (target) + 7 (out of focus)
		28	**INITIALIZE_UPDATE**	**132**	**INITIALIZE_UPDATE**
		44	**EXTERNAL_AUTHENTICATE**	**44**	**EXTERNAL_AUTHENTICATE**
		136	**GP_CMD_SCP**	**132**	**GP_CMD_SCP**
		3	SELECT_BY_NAME	3	SELECT_BY_NAME
		4	MANAGE_CHANNEL_CLOSE	4	MANAGE_CHANNEL_CLOSE

2.3 Dispatcher; B-Model (completed)

		Dispatcher	
		Metrics	**Comment**
ModelScope		-	All behaviors specified for the Dispatcher in GP2.1.1 **and JC2.2**
Lines of code (comments excluded)		**3475**	total = 5866 (comments=40%)
Number of APDU commands		**3**	RESET SELECT MANAGE_CHANNEL
Number of B operations	Total	**8**	
	Target	**5**	**RESET_procedure** **APDU_SELECT_byName** **APDU_MANAGE_CHANNEL_open** **APDU_MANAGE_CHANNEL_close** **COMMAND_2_DISPATCH_NO_SM_NO_CDATA**
	Preambule/postambule/ observation	3	preambule: TRANSITION_LCS_OF_CLIENT preambule: TRANSITION_LCS_OF_SD preambule: TRANSITION_LCS_OF_CARD
Number of variables	Total	**26**	
	State Variables	14	
	Configuration Switches	12	
Max Number of atomic B-expressions in a compound B-one		**10**	
Number of behaviors	Total	**633**	= 366 (Target) + 247 (out of focus)
		6	**RESET_procedure**
		231	**APDU_SELECT_byName**
		96	**APDU_MANAGE_CHANNEL_open**
		33	**APDU_MANAGE_CHANNEL_close**
		10	COMMAND_2_DISPATCH_NO_SM_NO_CDATA
		120	TRANSITION_LCS_OF_CLIENT
		115	TRANSITION_LCS_OF_SD
		22	TRANSITION_LCS_OF_CARD

2.4 Secure Messaging; Automated Test Generation (done)

					Secure Messaging SCP01		Secure Messaging SCP02	
					Metrics	**Comment**	**Metrics**	**Comment**
Test campaign generation	Number of tests campaign			**Total**	**1**		**1**	
	Number of test targets	**All campaign**		**Total**	**208**		**436**	
			Reachable	Reached	**208**		**304**	
				Unreached	**0**		**4**	Has it been analyzed?
			Unreachable		**0**		**128**	Does the model need corrections ?
	Number of test			Total	**200**	one single campaign	**256**	one single campaign
	Time to generate			Total	**5 min**	one single campaign	**17 min**	one single campaign

2.5 Dispatcher; Automated Test Generation (in progress)

					Metrics	Comment
Test campaign generation	Number of tests campaign			**Total**	**18**	
				Campaign_id1	1	RESET_procedure
				Campaign_id2	1	APDU_SELECT_byName
				Campaign_id3	10	APDU_MANAGE_CHANNEL_open 1 campaign per initial state where one applet of each package is the default selected applet
				Campaign_id4	1	APDU_MANAGE_CHANNEL_close
				Campaign_id5	5	COMMAND_2_DISPATCH_NO_SM_NO_CDATA 1 campaign per parameter to apply all criteria (CLA, LC, INS, P1, P2)
	Number of test targets	**All campaign**		**Total**	**376**	
			Reachable	Reached	**210**	
				Unreached	**87**	to be discussed in the details of campaigns: - in some cases the model has to be corrected - in others the LTG has to be optimized
				Unreachable	**79**	configurations not covered by implementation
	Number of test cases			Total	**5570**	
				Campaign_id1	6	Campaign for RESET_procedure
				Campaign_id2	87	Campaign for APDU_SELECT_byName
				Campaign_id3	226	Campaigns for APDU_MANAGE_CHANNEL_open
				Campaign_id4	11	Campaign for APDU_MANAGE_CHANNEL_close
				Campaign_id5	**5240**	Campaign for COMMAND_2_DISPATCH_NO_SM_NO_CDATA
	Time to generate			Total	**30h**	
				Campaign_id1	1h	Campaign for RESET_procedure
				Campaign_id2	**17h**	Campaign for APDU_SELECT_byName
				Campaign_id3	10h (1h / campaign)	Campaigns for APDU_MANAGE_CHANNEL_open
				Campaign_id4	1h	Campaign for APDU_MANAGE_CHANNEL_close
				Campaign_id5	1h	Campaigns for COMMAND_2_DISPATCH_NO_SM_NO_CDATA

3.1 State of Test Development (done/to do)

	Analysis of Specifications	Status	Done Leirios	Done G&D	To do Leirios	To do G&D
1	Secure Messaging	Done ?	-	?	0	?
2	LCS Card/Applets	Done ?	-	?	0	?
3	Dispatcher	Done = Word document identifies the behaviors graphically BUT: - Requirement Tags have only been introduced into the B-Model - No connection in DOORS	-	26,4d	0	7d?

	Modeling	Status	Done Leirios	Done G&D	To do Leirios	To do G&D
1	Secure Channel	- Model is complete and used for Test Generation - Should the model be adapted? (see unreached targets)	-	?	0	?
2	Dispatcher	- Model is complete and used for Test Generation - Model should be adapted in order to eliminate unreached targets - Some requirements may need to be adapted	-	28,5d	0	1-2d

	Test Campaign Configuration	Status	Done Leirios	Done G&D	To do Leirios	To do G&D
1	Secure Messaging	Done	?	?	0	0
2	Dispatcher	In progress	7d	0	?	?

3.2. State of Test Development (done/to do)

	Adapter Development	**Status**	**Done Leirios**	**Done G&D**	**To do Leirios**	**To do G&D**
1	For all models	In progress	**4d**	?	?	**1d**

	Model specific Adaptation Layer for CASCATE	**Status**	**Done Leirios**	**Done G&D**	**To do Leirios**	**To do G&D**
1	Secure Channel	done	0	?	0	**0**
2	Dispatcher	Not yet started	0	**0**	0	?

	Support/Training/Consulting	**Status**	**Done Leirios**	**Done G&D**	**To do Leirios**	**To do G&D**
1	General	Done	20d	-	-	-
2	Secure Channel	Done	-	-	-	-
3	Dispatcher	In progress	-	-	**2d?**	-

3.3 Remarks to Test Development

- Test Development Focus shifts to Analysis/Modeling (and a better representation of what is tested)
- A good model can be reused in other projects (e.g. configuration variables)
- The CASCATE Adapter is not model/project specific

4.1 Lessons Learned: Analysis

- **To plan enough time**
  - To identify the reference documents (GP alone, GP/JC)
  - To identify **all** behaviors (specified, unspecified, contradiction between specifications(!?)
  - To document the behavior representation
    - use **graphics** instead of text
    - include requirements

- **To review behavior identification before modeling starts**

4.2. Lessons Learned: writing B-Models

- **To think twice about signatures of B-operations**
- **To bear in mind the Test Generation Step when writing the B-Code** (expressions are more or less difficult to treat by the search algorithms)
- **To plan enough time to animate the model** (one way to validate the model)
- **To review the B-model with B specialist** (detect errors, optimize B-expressions)

4.3 Lessons Learned: Test Generation

- **Analysis of un-reached test targets may imply adaptation of the B-model** (Principally LTG should reach all targets, one way to validate the model)
- **The number of generated TC is no indicator of the Model Complexity**

5.1 First Conclusions about the methodology

- The Methodology is suitable
  - For generating lots of **Combined Test Cases** (Crypto)
  - For dealing with **Complex Behaviors** (Dispatcher)

- Problems if testing **Irreversible State Machines** and Execution Time is a major concern (Calculation of post-ambles)

- I will/would recommend to use Formal Modeling Techniques in order to develop Compliance Tests for GP2.2

THANK YOU FOR YOUR ATTENTION