Software Evaluation of smart cards : Detection of abnormal behavior of a smart card application

Germain Jolly

GREYC, CRNS UMR 6072
Équipe Monétique et Biométrie - ENSICAEN
6, boulevard du Maréchal Juin
14050 Caen cedex
germain.jolly@ensicaen.fr

October 14, 2014

Introduction

Figure : My research team : http://www.epaymentbiometrics.ensicaen.fr/

- Third year PhD student
- Laboratory : GREYC (computer science, electronic and electrical engineering)
- E-Payment & Biometrics
- affiliated with ENSICAEN, CNRS and University of Caen

Figure : Castle of Caen

Figure : Landing during the WWII

I The topic
The methodology

Objectives

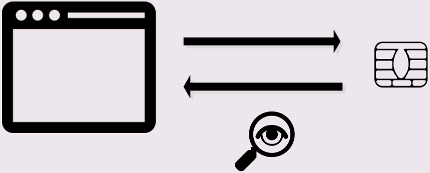


Figure : we focus on communication

- Evaluation of chips (a generic, easy and blackbox methodology)
- It is difficult for a campaign of intensive testing to trace the root reason of a malfunction of the smart card application
- A complementary method usable during a test phasis

1. Observation of the communication between the terminal and the chip
2. Definition of properties based on the theorical behaviour of the chip's application
3. Detection of anomaly on the fly with the violation of properties

II Analysis of the EMV application

Anomaly detection

Automat approach and Property approach

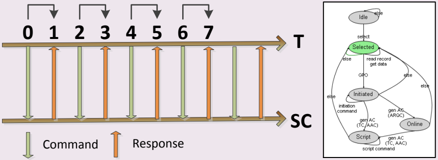


Figure : Automat conformance

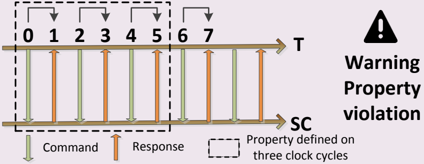
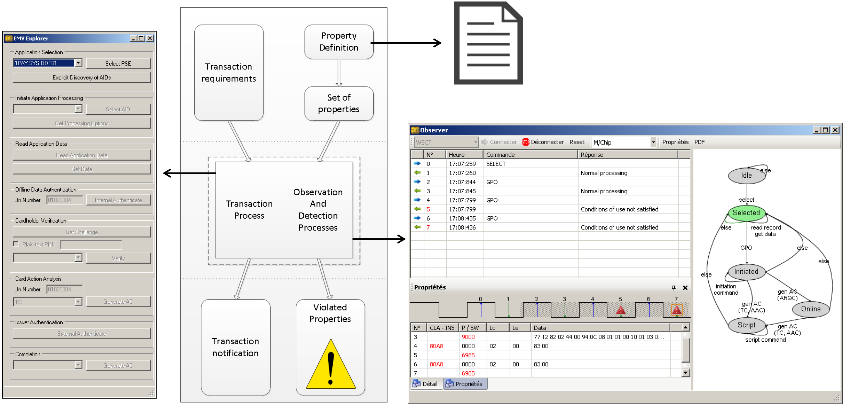


Figure : Property conformance

Property Definition :
Germain Jolly, Sylvain Vernois and Jean-Luc Lambert, Improving Test Conformance of Smart Cards versus EMV-Specification by Using on the Fly Temporal Property Verification, 2014

III Proof of concept with WSCT Framework

View of the tool



EMV Explorer

Application Selection: 1PAY.SYS.DDF01

Offline Data Authentication – Un.Number: 01020304

Cardholder Verification – □ Plain text PIN:

Card Action Analysis – Un.Number: 01020304 – TC

	N°	Heure	Commande	Réponse
→	0	17:07:259	SELECT	
←	1	17:07:260		Normal processing
→	2	17:07:844	GPO	
←	3	17:07:845		Normal processing
→	4	17:07:799	GPO	
←	5	17:07:799		Conditions of use not satisfied
→	6	17:08:435	GPO	
←	7	17:08:436		Conditions of use not satisfied

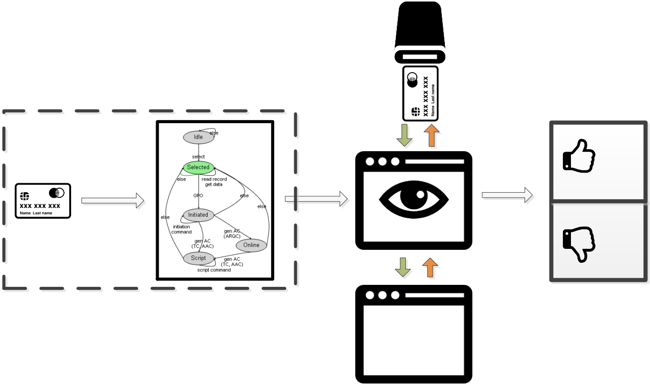
Propriétés

N°	CLA - INS	P / SW	Lc	Le	Data
3		9000			77 12 82 02 44 00 94 0C 08 01 01 00 10 01 03 0...
4	80A8	0000	02	00	83 00
5		6985			
6	80A8	0000	02	00	83 00
7		6985			

Figure : Proof of concept

Source code of WSCT Framework : https://github.com/wsct

Conclusion



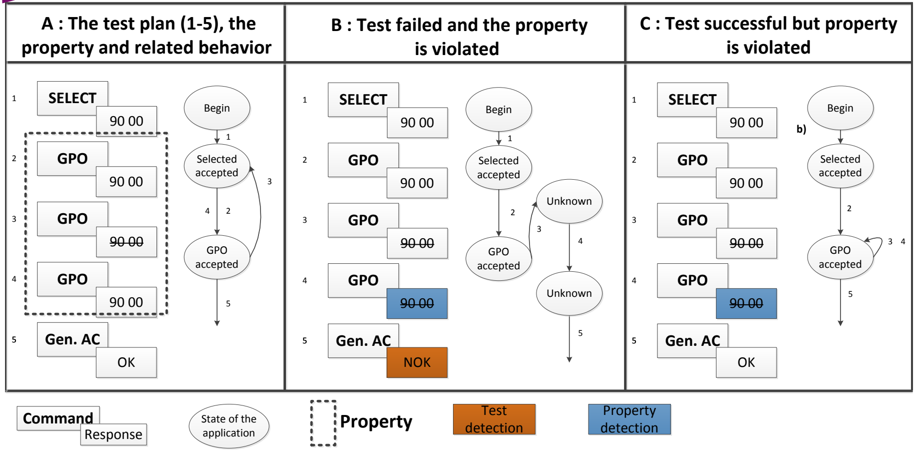
I am currently working on generation of a complete collection of properties :

- from a model (theorical machine state).
- from transactional flows (data mining approach).

Bibliography

- EMV Integrated Circuit Card Specifications for Payment Systems, version 4.3 EMVco, 2011
- M/Chip 4 Card Application Specifications for Credit and Debit, MasterCard International, 2002
- Un framework de fuzzing pour cartes a puce: application aux protocoles EMV, J. Lancia, 2011
- ISO/IEC 7816, International Organization for Standardization and the International Electrotechnical Commission
- Assertion-Based Design, Harry D. Foster, Adam C. Krolnik, David J. Lacey, 2010
- Source code of WSCT, https://github.com/wsct
- Analyse de la sécurité de transactions à puce avec le framework WinSCard Tools, Benoît Vibert, Vincent Alimi, Sylvain Vernois, 2012

Annex :
Link between APDU communication and the machine state



A : The test plan (1-5), the property and related behavior

B : Test failed and the property is violated

C : Test successful but property is violated

- **A** : Definition of the test plan (Gen. AC accepted) and the property
- **B** : We know why the Gen. AC has failed (see property)
- **C** : Even the test is successful, the application contains an error