Available online at www.sciencedirect.com

ScienceDirect

AASRI Procedia 4 (2013) 132 – 137

AASRI Procedia

www.elsevier.com/locate/procedia

2013 AASRI Conference on Intelligent Systems and Control

Neural Network VS. Bayesian Network to Detect Java Card Mutants

Ilhame El Farissi[a,*], Mostafa Azizi[a], Jean-Louis Lanet[b], Mimoun Moussaoui[a]

[a]*MATSI LAB, ESTO,Mohammed first University,Oujda, Morocco*
[b]*SSD Team Xlim,University of Limoges, Limoges, France*

Abstract

Being a vital element for the different domains such as communication system, authentication, and payment, multiple attackers manipulate the Card fraudulently in order to access to the services offered by this one. Smartcards are often the target of software and hardware attacks. The most recent attacks are based on fault injection which modifies the application behavior. By disrupting the Java Card operation, the fault attack modifies the compiled code intended to be executed in order to meet what the attacker wants instead of the initial program. So, to tackle this problem, we suggest two classification and detection methods based on artificial intelligence, especially the neural and Bayesian networks. Then, we compare between the obtained results of these two methods in terms of the detection rate.

Selection and/or peer review under responsibility of American Applied Science Research Institute

Keywords: SmartCard ; Java Card ; Security; Neural network; Bayesian network; Fault attack; Classification; Detection; Mutant;

1. Introduction

A smartcard is a secure, efficient and cost effective embedded system device comprising of a microcontroller, memory modules (RAM, ROM, EEPROM) serial input/output interfaces and data bus. One

* Corresponding author. Tel.: +212-671-590-065; fax: +212-536-505472.
E-mail address: ilhame.elfarissi@gmail.com.

2212-6716
Selection and/or peer review under responsibility of American Applied Science Research Institute
doi:10.1016/j.aasri.2013.10.021

chip operating system is contained in ROM and the applications are stored in the EEPROM. A smartcard can also be viewed as an intelligent data carrier which can store data in a secure manner and ensure the integrity, the confidentiality and the availability, then the security of data during transactions. Security is one of the important issues in smartcard development and the level of threat imposed by malicious attacks on the integrated software is of high concern. Multiple means are operated to return the secret information, fault injection seems to be the most efficient and effective one. In order to prevent and detect such attacks, smartcard manufacturers try to implement new options in their operating systems. Software fault injection is a technique of producing errors into the program, this technique allows attackers to analyze the system behavior, study its internal state and modify the application execution in order to deduce secret information.

It has been demonstrated in [1] that it is possible to predict the ability of an application to generate a hostile code while the smartcard is hit by a laser. Unfortunately this tool is based on a brute force attack and thus can only be used as a prevention tool. To detect such an attack during the run-time, several counter measures have been described in the literature but often they require additional information. For current platform, there is no solution that can be adapted to different effects of the attack. So, we propose here new schemes based from one side on Neural networks and on Bayesian Network from the other side, to detect during the run-time if an application has been mutated.

2. Java based smartcard

Java Card is a platform of smart cards. It is based on Java, but it has its own specifications in three aspects:

- Restriction of language
- The Run time environment
- The applet life cycle

Furthermore, due to the limited resources in smart cards, the Java Card Virtual Machine (JCVM) is split into two parts:

- Off-card: The byte code verifier (invoking the converter) that converts the java Card program to CAP file and verifies its validity is executed off-card.
- On-card: This part contains the interpreter, the API and the Java Card Run time Environment (JCRE).

Smart cards are nowadays used throughout the world on a daily basis, wherever the notion of digital security appears. Smart cards have strong constraints as for computing power and for memory size. Based on the Java technology, the Java Card architecture is compound of different layers on top of the smart card hardware and the operating system. The most important component is the Java Card Runtime Environment which includes the Java Card Virtual Machine (JCVM) and the API. The JCVM can somehow be seen as an abstract processor with its own instruction set and internal mechanisms. The JCVM provides several mechanisms enforcing the security of the system, based on the security mechanisms inherited from the standard Java specifications and some specific to this platform. As specific component dedicated to the security the firewall enforces applications isolation with the concept of security context. Due to limited memory an important component for the security the Byte Code Verifier (BCV) must be executed on a host platform. Because of the sensitivity of the data they contain and of their inherent robustness, smart cards are the target of particular kinds of attack: hardware attacks.

3. Fault Attack

Developed by Bonech, DeMillo and Lipton [3], the fault attack aims to disrupt the physical environment of the processor in order to produce errors. Initially, the fault attack targeted public-key cryptographic algorithms such as RSA and DES. Faults are injected into the chip by perturbing its environment execution.