Ain Shams University
Faculty of Engineering
Computers and Systems Department

Security Architecture for Multi-Applications Smart Cards

By

Ahmed Mamdouh Ahmed Mohamed

B.Sc., Electrical Engineering

(Computer and Systems Engineering Department)

Ain Shams University, 2008

A Thesis

Submitted In Partial Fulfilment of the Requirements for the Degree of

Master of Science in Electrical Engineering, Computer and Systems Dept.

Supervised By

Dr. Ayman Mohammad Bahaa Eldeen Sadeq

Associate Professor at Computer and Systems Engineering Department

Faculty of Engineering, Ain Shams University

Dr. Mohamed Ali Sobh

Lecturer at Computer and Systems Engineering Department

Faculty of Engineering, Ain Shams University

Cairo, Egypt

DECEMBER, 2015

Ain Shams University

Faculty of Engineering

Computer and Systems Engineering Department

Examiners Committee

Name	**:**	Ahmed Mamdouh Ahmed Mohamed
Thesis	**:**	Security Architecture for Multi-Applications Smart Cards
Degree	**:**	Masters of Science in Electrical Engineering

Name, Title, and Affiliate Signature

Prof. Dr. Nawal Ahmed El-Fishawy ....

Electronics and Electrical Communications Department
Faculty of Electroni Engineering,
Menoufia University, Menouf, Egypt

Prof. Dr. Hani M. Kamal Mahdi ....

Computer and Systems Engineering Department
Faculty of Engineering,
Ain Shams University, Cairo, Egypt

Dr. Ayman M. Bahaa-Eldin ....

Computer and Systems Engineering Department
Faculty of Engineering,
Ain Shams University, Cairo, Egypt (Supervisor)

Date: / /

Abstract

Ahmed Mamdouh Ahmed Mohamed

Security Architecture for Multi-Applications Smart Cards

Masters of Science dissertation

Ain Shams University, 2015

The increasing power of smart cards has made their use feasible in applications such as electronic passports, military and public sector identification cards, and cell-phone based financial and entertainment applications. As the prime uses of smart cards are identification, authorization and encryption, it is crucial that sufficient trust be established between different applications executing on the same smart card.

This research focuses on developing and enhancing techniques for securing smart cards' multi-applications operating system. Smart card hardware provides limited resources with respect to traditional computer; adding many challenges for developing and securing the operating system. It is required to minimize the code size, memory usage, and to increase the security, the performance and the development flexibility.

The research proposes a novel method to analyze the bytecode of applets installed on the smart card. The resources limitations forces the usage of an on-demand methodology for dynamic analysis of the bytecode. The proposed method is verified against security and performance requirements and is found to be efficient in both.

Keywords:

Multi-applications smart card, Java Card, Bytecode Verification, Embedded Software Design, Software Security

Publications

Ahmed Mamdouh, Ayman M. BahaaEldin and Mohamed Sobh, “On-demand Distributed On-card Bytecode Verification”, ICCES 2014 9th International Conference on Computer Engineering & Systems, Cairo, Egypt, December 2014.

Acknowledgements

First, I would like to thank ALLAH for his great support to me in accomplishing this work.

I would like to express my gratitude to Dr. Ayman Mohamed Bahaa El-din for his encouragement to me on continuing this work.

I would like to express my gratitude to Dr. Mohamed Ali Sobh for his leading efforts in the development of different parts of this work from the technical development to the documentation work.

Statement

This dissertation is submitted to Ain Shams University for the degree of Masters of Science in Electrical Engineering (Computer and Systems Engineering).

The work included in this thesis was out by the author at Computer and Systems Department, Ain Shams University.

No part of this thesis has been submitted for a degree or qualification at other university or institution.

Date : December 2015

Signature :

Name : Ahmed Mamdouh Ahmed Mohamed

Table of Contents

List of Figures and Illustrations

List of Tables

List of Abbreviations

AID	Application ID
APDU	Application Protocol Data Unit
BCV	Bytecode Verification
CAP	Converted Applet
COS	Card Operating System
CVM	Card Holder Verification Method
dJVM	defensive Java Virtual Machine
ESCOS	Egyptian Smart Card Operating System
GP	Global Platform
HAL	Hardware Abstraction Layer
JAR	Java Archive
JC/JCS	Java Card /Java Card System
JCRE	Java Card Runtime Environment
JCVM	Java Card Virtual Machine
JVM	Java Virtual Machine
LFG	Logical Flow Graph
ML	Metalanguage
MMU	Memory Management Unit
MRTD	Machine Readable Travel Document
OBCV	On-card Bytecode Verification
SLCOS	Softlock$^{©}$ Card OS
VM	Virtual Machine

Chapter 1: Introduction

1.1 Motivation

Nowadays, multi-applications smart cards became the trend of the smart cards. They support the installation/uninstallation of the applications after the issuance of the cards. Therefore, conventional approaches must be revisited in order to develop a novel techniques to defend cards against malfunction or malicious applications. Applications installed on these cards are able to exchange information and include data that may be very sensitive. Thus, the security of these cards should be reinforced not to let applications exchange illegal or not permitted data. Researchers in many parts of this field suffice with theory and hypothesis instead of targeting to really solve the problems that they maintain or to implement their proposed solutions in the industry. Thus, many of the proposed solutions are of no practical application and ignore some important practical issues such as complying with standards, verifier integration with card sub-modules, verifier configurability and modularity.

1.2 Contribution

In this research, a new methodology for verifying Smart Card applications is introduced.

Mainly the proposed methodology adds the following contributions in the field of bytecode verification:

- On-demand Verification: not to waste time of verifying unreachable code.
- Combination of static (load-time) and dynamic (run-time) verification
- Addition of dynamic (run-time) verifications that only can be done at run-time
- Industrial Verification: The proposed verifier is implemented and deployed in the Softlock© Card OS (SLCOS) smart card operating

system, and is intended to provide a real industrial solution. To the best of our knowledge, no other Java Card Virtual Machine’s (JCVM) verifier, proposed in the literature, targets an already-existing smart card operating system; instead, researchers suffice with theory and hypothesis.

Softlock Smart Card Operating System (SLCOS), is the second generation of the Egyptian Smart Card Operating System, or (ESCOS) which is a Java-based, secure and open smart card operating system [1]. The proposed verification is implemented within the SLCOS operating system.

1.3 Overview

The rest of this dissertation is split into four chapters. The second chapter constructs the background of our researches. By the end of the background, the statement of “Java Card Bytecode Verification” will be clear.

Chapter Three demonstrates the Proposed Solution, namely, “On-demand Distributed On card Bytecode Verification” preceded by an overview of the Operating System where the proposed solution resides. Following the proposed solution, the implementation details of the solution within the Operating System will be revealed.

Chapter Four will show the results followed by Chapter Five for the conclusion of this research and finally our future vision for developing this research.

Chapter 2: Background

Before proceeding in the description of the research, this chapter constructs the essential fundamentals of the domain of this research. It starts by discussing the concept of the Multi-applications cards revealing its technology, evolution and applications. Then, the notion of the "Java Card" is revealed followed by its development lifecycle, its security model and its security concerns and threats. Two useful comparisons are carried out; the first one compares the Java Card versus the Standard Java and the other one is between the two Java Card editions, that is, the classic edition and the connected edition. The main concept of this research, namely "Java Card Bytecode verification" is, also, discussed in this chapter. Finally, this chapter traverses the related work in solving the latter stated security issues.

2.1 Multi-application Smart Cards

Nowadays, Smart Cards are adopted in many fields ranging from eGovermnent, eCommerce, eHealth, etc. across a variety of applications in each field. Thus, a need was raised not to have a smart card for each application, which leads to the evolution of multi-applications smart cards. Mainly, multi-applications smart cards have many advantages for the card issuer, the application developer and for the cardholder:

1. Usability: The cardholder will have one smart card for different applications instead of one card for each application.
2. Changeability: In case of smart cards supporting post-loaded applications, the application developers will have the chance to update, change or resolve defects of their applications.
3. Low-cost: The issuers can share the cost of the smart cards, which will save their investments. Moreover, the cardholders may only buy one card for all applications.