AN AUTOMATED TOOL FOR DETECTION AND ENFORCEMENT OF SECURITY IN MOBILE APPLICATION DEVELOPMENT

P. A. I. U. Amarasekera

148202X

Degree of Master of Computer Science

Department of Computer Science and Engineering

University of Moratuwa
Sri Lanka

May 2018

AN AUTOMATED TOOL FOR DETECTION AND ENFORCEMENT OF SECURITY IN MOBILE APPLICATION DEVELOPMENT

P. A. I. U. Amarasekera

148202X

This dissertation submitted in partial fulfillment of the requirements for the Degree of Master of Computer Science specializing in Mobile Computing

Department of Computer Science and Engineering

University of Moratuwa
Sri Lanka

May 2018

DECLARATION

I declare that this is my own work and this MSc. project report does not incorporate without acknowledgement any material previously submitted for a degree or diploma in any other University or institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement and declaration are made in the text.

Also, I hereby grant to University of Moratuwa the non-exclusive right to reproduce and distribute my thesis, in whole or in part in print, electronic or other medium. I retain the right to use this content in whole or part in future works.

---------------------------------   ---------------------------------

P.A. I. U Amarasekera   Date

I certify that the declaration above by the candidate is true to the best of my knowledge and that this project report is acceptable for evaluation for the MSc. research project.

---------------------------------   ---------------------------------

Dr. Malaka Walpola   Date

ABSTRACT

With the large number of mobile applications being developed and used, the mobile application security has become a key concern to the mobile application users as well as to the mobile application designers, developers and testers. Numbers of security guidelines and prevention mechanisms have been introduced through previous research work and considerable amount of mobile security frameworks, testing tools and source code analyzers have been implemented upon those research outcomes. However it was identified that these tools and instruments majorly support the testing phase of secure software development life cycle and there is a research gap open for developing a technically supportive program for the developers to build secure mobile applications.

The intention of this project is to come up with a concept where the developer is enforced to build a secure mobile application based on a predefined set of security criteria during the application development phase. These security criteria are defined based on security requirements of the mobile application project. The source code will be validated against these security criteria and if any issue is found, it will be fixed automatically during the source code compilation. This system is implemented in java platform with the help of java annotation processor and xml parser. The source code is written as s a set of reusable jar file which is published as “buildsec” library. This library is tested and evaluated in android mobile platform by injecting vulnerable codes snippets into the android mobile source code and “buildsec” library was able to find and fix those security issues in the source code. The automatic fixing of security issues during compile time will help the development team to ensure that the mobile application is security compliance in advance. This will reduce the testing effort as well as development re-work that takes to fix the security issues originated from the development phase.

ACKNOWLEDGEMENTS

I would like to start off by expressing my deepest love and affection to my parents and family for their love and immense support, which has been a constant source of strength throughout this journey.

My deepest gratitude and admiration goes to my supervisor, my mentor; Dr. Malaka Walpola, for his invaluable guidance by providing extensive knowledge, materials, advice and supervision throughout this research work. His expertise and continuous guidance enabled me to accomplish my research. Furthermore my appreciation goes to Mr. Amodth Jayawardena and Mr. Prasad Sooriyaarachchi for providing valuable resources, technical support and advice in the area of this research.

Last but not the least; I express my profound love and admiration to all my colleagues for their invaluable help on finding relevant research material, sharing knowledge and experience and for their generous encouragement.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

Abbreviation	Description
API	Application Program Interface
APK	Android Package Kit
APN	Access Point Name
CIA	Confidentiality, Integrity, Availability
DEX	Dalvik EXecutable
DHS	Department of Homeland Security
DNS	Domain Name System
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hyper Text Transfer Protocol with Secure Sockets Layer
IP	Internet Protocol
IPA	IPhone Application Archive
IPC	Inter Process Communication
JAR	Java ARchive
MAM	Mobile Application Management
MDM	Mobile Device Management
MFA	Multi-Factor Authentication
NIST	National Institute of Standards and Technology
OS	Operating System
OWASP	Open Web Application Security Project
PIN	Personal Identification Number
QA	Quality Assurance
QARK	Quick Android Review Kit
SAST	Static Application Security Testing
SD	Secure Digital
SDK	Software Development Kit
SDLC	Software Development Life Cycle
SFR	Security Functional Requirements
SMS	Short Message Service
SQL	Structured Query Language
SSC	Software Security Checklist
SSL	Secure Sockets Layer
SSLC	Secure Software Life Cycle
TFA	Two-Factor Authentication

TLS	Transport Layer Security
UAT	User Acceptance Testing
UDP	User Datagram Protocol
UI	User Interface
URL	Universal Resource Locator
UUID	Universal Unique Identifier
WiFi	Wireless Fidelity