A STUDY ON EFFECTIVENESS OF SOFTWARE VULNERABILITY ASSESSMENT FOR COMPONENT-BASED SOFTWARE DEVELOPMENT

K.L. Dasun

138205B

Degree of Master of Science/Master of Engineering

Department of Computer Science and Engineering

University of Moratuwa
Sri Lanka

December 2016

A STUDY ON EFFECTIVENESS OF SOFTWARE VULNERABILITY ASSESSMENT FOR COMPONENT-BASED SOFTWARE DEVELOPMENT

K.L. Dasun

138205B

Thesis/Dissertation submitted in partial fulfilment of the requirements for the degree Master of Science/Master of Engineering in Computer Science and Engineering

Department of Computer Science and Engineering

University of Moratuwa
Sri Lanka

December 2016

Declaration

I declare that this is my own work and this dissertation does not incorporate without acknowledgment 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 acknowledgment is made in the text.

Furthermore, I hereby grant to University of Moratuwa the non-exclusive right to reproduce and distribute my dissertation, 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 (such as articles or books).

…………………………………………… ……..…………………………….

K.L.Dasun Date

The above candidate has carried out research for the Masters Dissertation under my supervision.

…………………………………………… ………………………………..

Dr. Chandana Gamage Date

(Research Supervisor)

Abstract

Security is an essential aspect for software development as many critical and vital functions, systems and services are now controlled by software. Operating systems to middleware to applications, integrated systems to embedded systems to firmware, and networks of all sizes and complexities are now controlled and managed by software. Thus, assurance of security in such software and thereby the protection of sensitive data is essential.

Due to the complexity, scalability and maintainability factors, the software industry is moving rapidly towards component-based systems development where various artefacts are integrated to achieve a variety of functionality. This integration occurs in different phases in the life cycle of a system and usually at a rapid pace. Therefore, it is doubtful if the correct level of emphasis is placed in the development process to assure the security of composing a system with such diverse components, even if they have a high level of security individually.

While there are many tools to test the potential for exploitation of vulnerabilities in software systems, these tools are most often optimized to test certain application scenarios, development phases, and specific software categories or methodologies. Therefore, with the increasing use of composed development of software systems and also the expansion in the tools and techniques available for software vulnerability exploitation, it is vital to evaluate the effectiveness of existing vulnerability assessment scheme on composed software development. This research is focused on determining the direction for improved effectiveness of software vulnerability tools in the composed system development paradigm.

Acknowledgements

I would like to express my special appreciation and thanks to my supervisor Dr Chandana Gamage, you have been a tremendous mentor to me. I would like to thank you for guiding me through your experience to make this research more worthwhile.

I would also like to take this opportunity to thank Dr Malaka Walpola, Dr Shehan Perera for guiding us in Research Seminar lecture sessions and for the extended support and kindness granted to us. At last but not least, I would thank all the academic staff members for helping, guiding, encouraging us and disseminating knowledge throughout the program.

Table of Contents

Declaration ii

Abstract iii

Acknowledgements iv

Table of Contents v

List of Figures viii

List of Tables ix

List of Abbreviations x

1. Introduction 1

1.1 Software Security 1

1.2 Security of the Component-Based Systems 2

1.3 Methods of Software Vulnerability Assessment 3

1.4 Motivation for the Research 3

1.5 Research Problem 4

1.6 Benefits of the Research 4

2. Literature Review 5

2.1 Composed Systems 5

2.1.1 Component 5

2.1.2 Component Interface 6

2.1.3 Component Composition 7

2.1.4 Component Composition Patterns 10

2.2 Issues and Problems of Composed Systems 11

2.2.1 Maximizing the Reusability 11

2.2.2 Quality of the Components 11

2.2.3 Standards and Certifications 12

2.2.4 Component Search and Repository 12

2.2.5 Other Issues..13

2.3 Security of Composed Systems 14

2.3.1 Scenario Based Component Security 15

2.3.2 Characterization of Component Security..15

2.4 Measuring the Security of Component-Based Systems 17

2.5 Software Security Testing Methodologies 20

2.5.1 Security in the Requirement Gathering & Design Phase..........................21

2.5.2 Static Analysis & Code Reviews 21

2.5.3 Fault Injections..21

2.5.4 Dynamic Testing 22

2.5.5 Binary Analysis..22

2.5.6 Penetration Testing...23

2.5.7 Vulnerability Scanning 23

3. Methodology..24

3.1 Introduction..24

3.2 Existing Experiment Efforts 24

3.3 Goals and Motives of the Experiment..25

3.4 Experiment Design...26

3.5.1 Test Data Selection...26

3.5.2 Test Tool Selection..28

3.6 Experiment Setup...29

3.6.1 Quantitative Analysis of Tools..29

3.6.2 Qualitative Analysis of Tools for CBSD 31

3.6.3 Support for Agile Development 32

3.7 Measurement Methods 33

4. Results & Evaluation 35

4.1 Experiment I 35

4.1.1 Assessment of SAST 37

4.1.2 Assessment of DAST..40

4.1.3 Overall Assessment 43

4.2 Experiment II 48

4.3 Experiment III..49

4.4 Limitations & Improvements to the Experiment 52

5. Conclusion...54

5.1 Findings 54

5.2 Conclusion 55

5.3 Future Improvements 56

References 58

List of Figures

Figure Index	Name	Page
Figure 2.1	Structure of component interface	6
Figure 2.2	The Structure of the characterization scheme	16
Figure 2.3	A Security characterization process framework	17
Figure 2.4	An Assessment scheme	18
Figure 2.5	An evaluation template for the banking system	19
Figure 2.6	Security assessment approach	20
Figure 3.1	OWASP benchmark basic structure	27
Figure 4.1	Interpreting the results	35
Figure 4.2	FindSecBugs vulnerability assessment statistics	38
Figure 4.3	FindSecBugs effectiveness	39
Figure 4.4	OWASP ZAP vulnerability assessment	41
Figure 4.5	OWASP ZAP vulnerability assessment effectiveness	40
Figure 4.6	True Positive count of the product	43
Figure 4.7	False Positive count of the products	44
Figure 4.8	False Negative count of the products	45
Figure 4.9	Product wise True Negative count	45
Figure 4.10	Overall score gained by products	46
Figure 4.11	Overall effectiveness of products	47
Figure 4.12	Number of issues in incremental versions	50
Figure 4.13	Overall progression in incremental versions	51

List of Tables

Table Index	Name	Page
Table 2.1	Advantages and disadvantages of COTS components	8
Table 2.2	Compositional forms of component models	9
Table 3.1	Number of vulnerabilities in each category	30
Table 3.2	Products and versions used in experiment I	30
Table 3.3	Details of vulnerable components in development	31
Table 3.4	Incremental product versions in the Excrement II	32
Table 4.1	FindSecBugs vulnerability assessment statistics	37
Table 4.2	OWASP ZAP vulnerability assessment statistics	40
Table 4.3	Overall vulnerability assessment statistics	43
Table 4.4	Experiment II results	48
Table 4.5	Vulnerability assessment in incremental versions	49
Table 4.6	Feature analysis of the security tools	52

List of Abbreviations

Abbreviation	Description
SDLC	Software Development Life cycle
COTS	Commercial Off The Shelf
FOSS	Free and Open Source Software
CBSE	Component Based Software Engineering
CBSD	Component Base Software Development
SAST	Static Application Security Testing
DAST	Dynamic Application Security Testing
IAST	Interactive application Security Testing
TP	True Positive
TN	True Negative
FP	False Positive
FN	False Negative
TPR	True Positive Rate
FPR	False Positive Rate
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration