UNIVERSITI PUTRA MALAYSIA

MODELING OF POST-INCIDENT ROOT CAUSE ANALYSIS FOR CROSS SITE REQUEST FORGERY (CSRF) ATTACK

MOHD NAWAWI BIN MUSTAFA

FSKTM 2015 39

MODELING OF POST-INCIDENT ROOT CAUSE ANALYSIS FOR CROSS SITE REQUEST FORGERY (CSRF) ATTACK

By

MOHD NAWAWI BIN MUSTAFA

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia

in Fulfilment of the Requirements for the Master of Computer Science

JULY 2015

DEDICATIONS

This thesis is dedicated to:

My beloved wife, Kartina bt. Omar.

Thank you for the support, encouragement and constant love.

Your sacrifice and contribution is my success secret.

Also to my supervisor, Dr. Mohd Taufik Abdullah

Your encouragement, support, advice and guidance is an outline to my achievement.

Finally, to all my friends,

Thank you for the support and encouragement.

ABSTRACT

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfillment of the requirement for the Master of Computer Science

MODELING OF POST-INCIDENT ROOT CAUSE ANALYSIS FOR CROSS SITE REQUEST FORGERY (CSRF) ATTACK

By

MOHD NAWAWI BIN MUSTAFA

JULY 2015

Supervisor : Dr. Mohd Taufik Abdullah

Faculty : Faculty of Computer Science and Information Technology

Abstract: With the advancement of ICT technology, especially on web technologies, people have changes their way of doing this. Online transactions have become more popular compared to physically going at the specific location to do transactions. However, the advancement of web technology has also introduced new security threats to the businesses and the clients.

OWASP Top 10 security project has classifies web application security incident into ten categories of most commonly exploited vulnerabilities. Even though the countermeasures for those vulnerabilities have been available for some time, the numbers of exploited web applications are increasing each year. One of the factors that contributes to the increasing number of ICT security incidents is failure to determine the root cause of an incident, thus allowing the attacker to repeat an attack on the system in the future by exploiting the same vulnerability.

This study will propose a model for post-incident root cause analysis to determine the suitable countermeasures in rectifying the Cross Site Request Forgery (CSRF) vulnerabilities. The proposed model were consists of attacker component, countermeasure component and inference component.

The proposed model will be developed using Colored Petri Nets. CSRF attack simulation was performed using Damn Vulnerable Web Application (DVWA) as the target machine and tested based on recommendations by the previous researchers.

To test the effectiveness of the developed model, the result of the CSRF attack simulations were compared with results by other researchers in the same category.

Hopefully, the proposed post-incident root cause analysis will benefit web application developers, security auditors and other related parties to identify and fix CSRF vulnerabilities on their web applications.

ABSTRAK

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia
sebagai memenuhi keperluan untuk ijazah Sarjana Sains Komputer

MODELING OF POST-INCIDENT ROOT CAUSE ANALYSIS FOR CROSS SITE REQUEST FORGERY (CSRF) ATTACK

Oleh

MOHD NAWAWI BIN MUSTAFA

JULAI 2015

Penyelia : Dr. Mohd Taufik Abdullah

Fakulti : Fakulti Sains Komputer dan Teknologi Maklumat

Abstrak: Selaras dengan kemajuan teknologi ICT, terutamanya teknologi web, masyarakat telah mengubah cara mereka melakukan kerja. Transaksi atas talian telah menjadi semakin popular. Walaubagaimana pun, kemajuan teknologi web telah memperkenalkan ancaman keselamatan baharu kepada perniagaan and para pelanggan.

Projek keselamatan *OWASP Top 10* telah mengklasifikasikan insiden keselamatan aplikasi web kepada sepuluh kategori kelemahan yang biasa di eksploit. Walaupun kaedah mengatasi kelemahan ini telah ada, bilangan

aplikasi web yang di eksploit terus meningkat setiap tahun. Antara factor yang menyumbang kepada peningkatan insiden keselamatan ICT adalah kegagalan mengenalpasti punca insiden tersebut yang membolehkan pencerobohan berulang ke atas sistem berkenaan pada masa akan datang dengan mengeksploit kelemahan yang sama.

Kajian ini akan mencadangkan sebuah model bagi menjalankan analisa punca selepas insiden berlaku untuk mengenalpasti kaedah pengukuhan yang sesuai bagi mengatasi kelemahan CSRF. Model yang dicadangkan terdiri dari komponen penyerang, komponen pengukuhan dan komponen analisa.

Model yang dicadangkan tersebut akan dibangunkan menggunakan *Colored Petri Nets*. Simulasi bagi serangan CSRF dilakukan menggunakan aplikasi DVWA sebagai sasaran serangan and di uji berdasarkan saranan oleh pengkaji-pengkaji yang terdahulu.

Untuk mengkaji keberkesanan model yang dibangunkan, hasil simulasi serangan CSRF yang dijalankan dibandingkan dengan hasil kajian oleh pengkaji-pengkaji lain di dalam kategori yang sama.

Adalah diharapkan model bagi menjalankan analisa punca selepas insiden berlaku yang dicadangkan ini akan dapat membantu pembangun aplikasi web, pengaudit keselamatan dan lain-lain pihak yang berkenaan untuk mengenalpasti and memperbaiki kelemahan CSRF pada aplikasi mereka.

ACKNOWLEDGEMENTS

Alhamdulillah, all praises to Allah S.W.T for the strength and blessing in completing this thesis.

I would like to express the deepest appreciation to my supervisor, Dr. Mohd Taufik Abdullah, for the patient and truthful guidance and unlimited confidence in me. I would also like to thank him for being an open person and for encouraging and helping me to shape my interest and ideas. His guidance helped me in all the time of research and writing of this thesis.

My sincere thanks and gratitude also dedicated to the Dean and members of FSKTM for their endless support. Their care and support help me overcome setbacks and stay focused on my graduate study. I deeply appreciate their believed in me.

My greatest appreciation and friendship goes to my friends, especially in Universiti Putra Malaysia, who were always a great support in all my struggles and frustrations in my studies. Thanks to them for questioning me about my ideas, helping me think rationally and even for hearing my problems.

Finally, I would like to thank my wife for always believing in me, for her continuous love and their supports in my decisions. Without whom I could not have made it here.

APPROVAL

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfillment of the requirement for the degree Master of Computer Science. The members of the Supervisory Committee were as follows:

Mohd Taufik Abdullah, PhD
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Supervisor)

Zurina Mohd Hanapi, PhD
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Assessor)

Date: July 2015

DECLARATION

I declare that the thesis is my original work except for the quotations and citations which have been duly acknowledged. I also declare that it has not been previously submitted for any other degree at Universiti Putra Malaysia or at any other institutions.

Signature : ______________________________

Name : MOHD NAWAWI BIN MUSTAFA

Matric No. : GS37498

Date : ________________

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
CERT	Computer Emergency Response Team
CPN	Colored Petri Nets
CSRF	Cross Site Request Forgery
CVSS	Common Vulnerability Scoring System
DFRWS	Digital Forensic Research Conference
DVWA	Damn Vulnerable Web Application
FSKTM	Faculty of Computer Science and Information Technology, Universiti Putra Malaysia
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISO	International Organization of Standardization
LDAP	Lightweight Directory Access Protocol
OS	Operating System
OWASP	Open Web Application Security Project
PHP	Hypertext Preprocessor
SQL	Structured Query Language
URL	Uniform Resource Locator
XSS	Cross Site Scripting

CHAPTER 1

INTRODUCTION

1.1 Background

This chapter discusses about the background of the research area problem statement, research objectives, scope of the study and thesis organization.

CSRF is a website vulnerability which is less known to website developers so it is exist in many websites (Siddiqui, 2011). Many of the web application developers are not aware of the vulnerability. A successful exploit of the vulnerability will impact the integrity and non-repudiation of the company, thus might deter their clients as they have loss of reputation and confidence on their company's services. Therefore, a root cause analysis model for CSRF attack will help to guide the web developers and security auditors to implement the right countermeasures on their web application to reduce the risk of CSRF attacks in the future.

1.2 Problem Statement

Based on OWASP report (OWASP, 2013), Cross Site Request Forgery (CSRF) is one of the commonly found vulnerabilities in a web applications. Detection of CSRF attack is currently difficult to do since each web application behaves differently upon receiving requests from users. Automated detection techniques such as ModSecurity on Apache web server and scoring system used in CVSS are not be able to provide satisfactory level of accuracy (Hannes, 2015). CSRF attack can be easily launch by clicking a link in an email that contains a specially encoded link or a link that redirects a user to a vulnerable web site, which then executes the CSRF attack. Even though there are several researchers that suggest countermeasures for CSRF vulnerability, the existence of post-incident root cause analysis model has not been paid much attention (Tondel, 2014).

The previous model developed by Philippe (2011) focused on developing client-side protection against CSRF attacks. Even though the solution able to provide protection against CSRF attack to the user, it would not be able to protect all users since the user need to install the developed add-on package for the Firefox browser on the client-side. Furthermore, the add-on might not compatible with the latest version of the web browser.

The proposed model in the research focused on the server-side solutions, so that it can be benefited by all users and not limited by the additional protection for CSRF installed on their machine.

1.3 Research Objective

Drupsteen (2014) has identified that the intrusions of web application are due to the related person are not able to learn from the incident occurs. There are cases on intrusion of web applications by exploiting the same vulnerability that was not properly addressed during the post-incident phase of incident management.

The objective of this study is to propose a post-incident root cause analysis model for CSRF attack based on DFRWS investigative framework in finding the optimal countermeasures by focusing on the server-side solution.

1.4 Research Scope

This project focuses on developing a post-incident root cause analysis model for CSRF attack using Colored Petri Nets. The model would be able to determine the root cause of a CSRF intrusion and suggests countermeasures that can be implemented on the server-side that should be done by the web developers to reduce the risk of incident in the future.

1.5 Thesis Organization

This chapter discussed on the motivation of this study, problem statement, research objective and research scope. This thesis is organized into six chapters.

Chapter 2 explains the literature review and related works regarding ICT security incident management, Cross-Site Request Forgery, Post-Incident Root Cause Analysis and Colored Petri Nets.

Based on the information grasp in literature review, the research methodology was proposed and discussed in Chapter 3.

Chapter 4 discusses on the requirements for the implementation and simulation of the study. In this chapter, research parameters, topology, simulation and performance metric were discussed. Hardware and software requirements were also discussed to ensure there are no interruptions during the study.

Result and findings of the research were recorded and discussed in Chapter 5. Each of the findings has been analyses and discussed accordingly. The result of the study was compared with the previous researcher for performance analysis.

Finally, the conclusion of the thesis and proposed future work of this thesis was tabled in Chapter 6.

REFERENCES

Adam, B., Collin, J., John C. M. (2008). Robust defenses for cross-site request forgery. *Proceedings of the 15th ACM conference on Computer and communications security*, pp. 75-88.

Alexenko, T., Jenne, M., Roy, S. D., Zeng, W. (2010). Cross-Site Request Forgery: Attack and Defense. *7th IEEE Consumer Communications and Networking Conference (CCNC)*, pp. 1 – 2.

Blatz, J. (2008). CSRF: Attack and Defense. McAfee White Paper. http://www.mcafee.com/us/resources/white-papers/wp-csrf-attack-defense.pdf

Drupsteen, L., Hasle, P. (2014). Why do organizations not learn from incidents? Bottlenecks, causes and conditions for a failure to effectively learn. Accident Analysis & Prevention, vol. 72, pp. 351–358.

Hannes, H., Afridi, K. K. (2015). An expert-based investigation of the Common Vulnerability Scoring System. *Computers & Security*, vol. 53, pp. 18-30.

Kurt, J., Lars, M. K., Lisa, W. (2007). Coloured Petri Nets and CPN Tools for modelling and validation of concurrent systems. *International Journal on Software Tools for Technology Transfer*,vol. 9, issue 3-4, pp. 213-254.

OWASP Foundation. OWASP Top 10 – 2013. http://owasptop10.googlecode.com/files/OWASP Top 10 - 2013.pdf

Philippe, D. R., *et al*. (2011). Automatic and Precise Client-Side Protection against CSRF Attacks. *Lecture Notes in Computer Science*, vol. 6879, pp. 100-116.

Purnima, K., Purnima, B. (2014). Vulnerabilities and Defensive Mechanism of CSRF. *International Journal of Computer Trends and Technology (IJCTT)*, 4, vol. 13, pp. 171 – 174.

Sentamilselvan, K., Lakshmana, P. S., Ramkumar, N. (2014). Cross Site Request Forgery: Preventive Measures. *International Journal of Computer Applications (0975 – 8887)*, vol. 106, no.11.

Siddiqui, M. S., Verma, D. (2011). Cross Site Request Forgery: A common web application weakness. *IEEE 3rd International Conference on Communication Software and Networks (ICCSN)*, pp. 538 – 543.

Stephenson, P. (2004). The Application of Formal Methods to Root Cause Analysis of Digital Incidents. *International Journal of Digital Evidence*, vol. 3, issue 1.

Stephenson, P. (2003). Modelling of Post-Incident Root Cause Analysis. *International Journal of Digital Evidence*, vol. 2, issue 2.

Tondel, I. A., Line, M. B., Jaatun, M. G. (2014). Information security incident management: Current practice as reported in the literature. *Computers & Security*, *45*, pp. 42–57.

Zeller, W., Felten, E. W. (2008). Cross-Site Request Forgeries: Exploitation and Prevention. Technical Report, Princeton University.