UNIVERSITI TEKNOLOGI MARA

NONINTRUSIVE SSL/TLS PROXY TECHNIQUE WITH JSON-BASED POLICY

SUHAIRI BIN MOHD JAWI @ SAID

Thesis submitted in fulfillment
of the requirements for the degree of
Master of Science
(Information Technology And Quantitative Sciences)

Faculty of Computer & Mathematical Sciences

November 2017

ABSTRACT

Certificate and SSL/TLS connections are two security aspects needs to be handled simultaneously in HTTPS. Some previous studies focused more on trust relationship in certificates whereas the properties of SSL/TLS connections were more prevalent in SSL/TLS surveys. Thus, this study proposes a non-intrusive proxy technique that merges this gap. The first part of this study discusses the components of the proposed proxy which handles two categories of attributes classified as static or dynamic. These attributes are compared against a set of policies written in JavaScript Object Notation (JSON). Second part of this study considers the practical implementation of this proxy for monitoring both SSL/TLS certificates and connection properties in between web browsers and SSL/TLS web server. It moderates the ongoing and subsequent SSL/TLS sessions from clients that proxy serves. This proxy can be considered as a localized notary with single path probing as compared to other notary services which use the concept of multipath probing via multiple network vantage points. Benefit of this work will be demonstrated as a simpler implementation for clients who have no effective means to authenticate and secure HTTPS connection except provided by the browser. The proxy successfully detects and warns some well-known issues regarding SSL/TLS although it may miss some SSL/TLS issues that require intensive and time-consuming analysis such provided by Qualys' SSL Server Test.

ACKNOWLEDGEMENT

Firstly, I wish to thank God for giving me the opportunity to embark on my MSc and for completing this long and challenging journey successfully. My gratitude and thanks go to my supervisor Dr. Fakariah Hani Hj Mohd Ali.

My appreciation goes to Hazlin Abdul Rani, Manager of Cryptography Development Department of CyberSecurity Malaysia who provided the facilities and flexibility to meet my educational needs. Special thanks to my colleagues and friends for helping me with this project.

Finally, this thesis is dedicated to my mother, beloved wife and daughters as well as in the loving memory of my very dear late father for the vision and determination to educate me. This piece of victory is dedicated to all of them. Alhamdulilah.

TABLE OF CONTENTS

CHAPTER ONE
INTRODUCTION

1.1 Research Background

HTTP Secure (HTTPS) or HTTP over SSL/TLS, relies on X.509 Public Key Infrastructure (PKI) certificate for trust relationship between client and server. Besides certificate, each SSL/TLS connection use cryptographic mechanisms for authentication, key exchange, encryption and hashing. However, issues and problems emerge from usage of certificate and weak SSL/TLS connection properties as there have been numerous incidents, attacks and new findings reported in the news and research literatures. Over the past ten years, numerous studies and surveys have been conducted to examine the state of HTTPS connections that monitor the properties of X.509 certificates, roles and practices in the PKI, Certificate Authorities (CA) and SSL/TLS-enabled web servers; and the elements of algorithms in SSL/TLS ciphersuites. There are also several proposals to improve the X.509 PKI landscape using extended certificate validations to strengthen certificate issuance and notary services to monitor the usage of the certificate.

Notary service firstly proposed by Wendlandt (2008) and was called Perspective which authenticates server public key by probing a large number of network services over time to make better security decision. The concept of Perspective has been adapted by subsequent studies and several notary services have been proposed such as MECAI, CertLock, ICSI Notary, CrossBear, DIV, Convergence, Cert-Shim and Open Systems AG's Notary. These latter notary services implemented several methods such as Voucher Authority (VA), browser add-on, passive network monitoring, network traceroutes, certificate crawlers, SSL hooking and Squid web proxy. Meanwhile, SSL surveys for present state of SSL employ passive and active network monitoring techniques. These surveys usually ended with statistics concerning issues mostly on SSL/TLS certificates and some authors extends their findings in the form of notary services to provide third party opinions regarding certificates and connections.