UNIVERSITI TEKNOLOGU MARA

UITM WEBSITE SSL/TLS VULNERABILITY AND MITIGATION

SUFIAN BIN IBNU HASSAN

Dissertation submitted in partial fulfillment
of the requirements for the degree of
Master of Science
(Computer Networking)

Faculty of Computer and Mathematical Science

July 2018

ABSTRACT

Secure Socket Layer (SSL) / Transport Layer Security (TLS) protocol has become a standard way for establishing a secure communication channel in internet application. In recent years several vulnerabilities related to SSL/TLS protocol were disclosed. TLS is a protocol that provides privacy and data integrity between two communicating applications. It's the most widely deploy security protocol used today, and is used for web browsers and others applications that require data to be securely exchanged over a network, such as file transfers, Virtual Private Network (VPN) connections, instant messaging and Voice over Internet Protocol (IP). Implementation flaws have always been a big problem with any encryption technology and SSL/TLS is no exception. A variant of the attack has exploited certain implementation of the SSL/TLS protocol that doesn't correctly validate encryption padding. In this paper, the researcher aims to disclose the vulnerabilities contained on the Universiti Teknologi Mara (UiTM) website and presents an analysis and evaluation of attack on SSL/TLS. Three tools (DNSRecond, SSLlabs.com and Auto Scanning to SSL Vulnerability A2SV) are used to test the output of a system without knowing the process inside the system itself. The experiments on UiTM website focused on SSL/TLS protocol and gathers information about existing SSL/TLS in the server. The experiments started with gathering information about the UiTM server using DNSRecond tool which is it perform top level domain scan. The result showed all server information, Domain Name Server (DNS), Mail Exchange (MX) and IP range in UiTM website. Secondly scanning the website using SSLlabs.com which is researcher discovered some vulnerability on the server such as certificate validity status and cipher suite weak. The last testing using A2SV tool which scan more detailed on vulnerability on the UiTM server. Additionally, in this paper dummy server testing scenario conducted to show how server handles invalid/expired SSL certificate. This experiment compared two type of browser chrome and internet explorer (IE). Researcher deployed invalid SSL certificate on both web browser and surprisingly IE validated certificate while chrome is otherwise. Based on the testing result information, researcher comes out with mitigation technique and compiled as a report that can be share with UiTM website administrator for better security implementation. In addition from the finding, researcher suggest that better tools and education programs for SSL/TLS security are needed to help UiTM administrator keep their system up-to-date with security patches.

ACKNOWLEDGEMENT

Thanks to Allah SWT, whom with His willing giving me this opportunity and strength to complete this research dissertation. There have been many people alongside me during the last one and a half year. I would like to thank and express my appreciation to each and every one of them. My special thanks go to my respected supervisor, Dr. Kamaruddin Bin Mamat for his guidance, advice effort, cooperation and valuable suggestions throughout the process of completing this research project. I would also like to acknowledge the panel of examiners especially Prof. Dr. Mazani Manaf, Dr. Mohd Faisal Ibrahim, Dr. Siti Arpah Ahmad for their very insightful comments, assistance and assessment along this journey.

A very big thank you must also go to my beloved wife, kids and friends who always give support and prayer for my success in studies and to those involved, whether directly or indirectly in helping me in finishing this research project.

Finally, this thesis is dedicated to the loving memory of my very dear late father Ibnu Hassan Bin Kalibugan and mother for the vision and determination to educate me. This piece of victory is dedicated to both of you. Alhamdulilah.

TABLES OF CONTENTS

CHAPTER ONE

1.1 INTRODUCTION

The first chapter about the initial appearance of a research project title “SSL/TLS vulnerability on UiTM portal and Mitigation.” This chapter begins with a background of a SSL/TLS attack, type of attack, vulnerability and scanner tools. The rest of this chapter is discussed in other topic including Problem statement, research question, research objective, research scope and limitation and Significant of research.

1.2 BACKGROUND OF STUDY

In everyday life, many activities on the internet such as online shopping, bank transfer, and others that require input data is confidential. Data transfer is done via wired or wireless network, and then required a strong security mechanism to be implemented on the TCP / IP protocol stack known as Transport Layer Security (TLS) or Secure Socket Layer (SSL). SSL or Secure Socket Layer is the way a website creates a secure connection with the user's web browser. Whenever a web surfer visits a secure site that uses SSL technology it creates an encrypted link between their browser session and the web server.

SSL is an industry standard for secure web communications and is used to protect millions of online transactions daily. The web server must have an SSL certificate before it can establish an SSL connection. When someone activates the SSL protocol on their web server, they are asked to answer questions that will build their identity.

Questions ask for information about both sites and companies. After the requested SSL certificate, the web server creates two cryptographic keys, one is private key and the other is Public Key. This button is used in conjunction with the encryption formula to create a secure connection between the web server and the browser session.