Universiti Teknologi MARA

Prevention of Man-In-The-Middle Attack Against HTTPS Website

Nur Syahirah Binti Zainalabidin

Thesis submitted in fulfilment of the requirements for
Bachelor of Science (Hons) Data Communications and Networking
Faculty of Computer and Mathematical Sciences

July 2020

ACKNOWLEDGEMENT

Alhamdulillah, praises and thanks to Allah SWT because of His Almighty and His utmost blessings, I was able to finish this research within the time duration given.

First of all, I would like to express my highest gratitude to my supervisor, DR. Zolidah Kasiran for his guidance, advice and support in order to complete this final year project. I appreciate every single knowledge she taught me.

Special appreciation goes to my beloved parents Zainalabidin Bin Abid and for always motivate and pray for me to easiest in order to complete this project.

Last but not least, thank you very much to all my dearest friends who helping me during the completions of this proposal report by discussing, sharing and exchanging ideas. Not to overlook, those who was directly or indirectly involved in writing this study.

Thank you very much.

ABSTRACT

The Man-In-The-Middle (MITM) attack is one of the most well-known attacks on computer security, posing one of the greatest issues for security professionals. MITM addresses the actual data that flows between endpoints, and the confidentiality and privacy of the data itself. Nonetheless, secure web sites typically use HTTPS connection to secure transactions such as money transfers, online payment, and e-commerce. The use of HTTPS provides a sense of security against threats such as man in the middle (MITM) attack. The objective of this paper are to design the counter-measure against MITM in target machine and counter-measure of the MITM are proposed. Also, in this paper we have discussed about how MITM attack can attack HTTPS sites even though it is known as secure websites and we have designed the counter-measure of it using the correct tools.

TABLE OF CONTENTS

CHAPTER ONE

INTRODUCTION

1.1 Introduction

A Man-in-the-Middle attack (MITM) involves the taking over of a malicious third party by intercepting and transmitting transit traffic from a communication channel between two or more endpoints. The attacker at centres, by eavesdropping, manipulating, producing, and drops traffic on the network, is able to damage the confidentiality, integrity, availability of user content. Generally speaking, an MITM assault model in a local area network (LAN), can access the network, intercept transit traffic, and control, manipulate or drop traffic, exists three steps. Access may be achieved by connecting to a public Wi-Fi point such as the cafe, the airport or others or physically connecting to an exposed network cable or network switch depending on the scenario. The intruder may also remotely target a virus that has a trusted device compromised inside the current network. Use of known vulnerabilities in network protocols can achieve interception once the access is gained. For example, an attacker might spray a domain name server (DNS) to intercept any web traffic in a host resolution table (ARP) to collect local traffic. (Mirsky et. al., 2019)

However, protected websites generally use Hypertext Transfer Protocol Safe communication (HTTPS) to provide users with a secure transaction, including money transactions, e.g. online payment, etc. HTTPS works simply by providing secure link and authentication by providing encrypted passwords. Use of HTTPS gives the impression of being highly secure from attacks like a middle-to-middle attack. Nonetheless, HTTPS links such as Gmail, Yahoo Mail, and Bank account can be targeted and also MITM can be avoided by using the appropriate tools available free of charge. (Mohiudin & Zubaida 2010)