UNIVERSITI TEKNOLOGI MARA

ENHANCEMENT OF SECURED WEB PROTOCOL USING ATTESTATION AND PSEUDONYMIZATION TECHNIQUES

FAZLI BIN MAT NOR

Thesis submitted in fulfillment
of the requirements for the degree of
Master of Science

Faculty of Computer & Mathematical Sciences

August 2016

ABSTRACT

Lack of security awareness among end users when dealing with internet transactions leaves open many client-side application vulnerabilities as well as privacy threats. Attackers could exploit these vulnerabilities and launch client-side attacks such as the Man in the Middle (MitM) attack or the malicious software attack due to lack of measures to detect malicious changes on the client-side platform and privacy protection. Thus, there is a need to implement a trusted environment and privacy enhancement between the client and the server. This research aims to enhance existing web protocol and preserve the privacy of users using attestation and pseudonymization technique with new proposed protocol, MyTrust. The advantages of proposed protocol include an end-to-end trusted environment which prevents identity impersonation by illegitimate parties. Prior to proposed protocol, this research presented a discussion on related works in term of its advantages and disadvantages. Subsequently, the proposed protocol is analyzed and evaluated based on its security vulnerabilities attack and performance. The analysis results showed that adding this additional preventive measure improved the overall protocol resistance to attack, and the performance of this approach is still comparable with existing implementations. This research emphasizes the significance of trusted computing technology and privacy enhancement technology for web protocols in aid of preventing client-side attacks.

ACKNOWLEDGEMENT

First of all, all praises and thanks to Allah, The Mighty Gracious Most Merciful, for giving me the strength, patience and ability to complete this thesis.

I would like to express my highest gratitude to my supervisors, Dr. Kamarularifin Abd Jalil and Dr. Jamalul-lail Ab Manan for giving me support, guidance and assistance through of completion of this thesis. Without their continuous support and interest, this thesis would not have been completed.

I am also thankful to my beloved wife, Haida @ Nurul Huda Habil upon her understanding, precious helps and endless supports in making the research possible. Her moral support contributes big impact in completing the research. For my daughter, Nur Batrisyia Qistina, thanks for your sense of fun and humors.

Last but not least, I would like to thank Universiti Teknologi MARA for funding this research under the Excellence Fund. Special thanks also go to all the people who had involved directly or indirectly in helping me throughout conducting this research. Hopefully, Allah would bless all the efforts and contributions.

TABLE OF CONTENTS

CHAPTER ONE
INTRODUCTION

1.1 BACKGROUND OF STUDY

Internet transactions such as online banking and electronic commerce (e-commerce) have become increasingly important services as more and more users come to depend on these services to manage their daily financial affairs. In some internet transactions, users are required to expose their sensitive data, including credit card information, banking account information, home address, and payment or transaction details. This information might be collected by a third party, or the merchant involved in the transaction as part of their marketing strategy, and then be used or sold on to another businesses (Mane, Sawant, & Sinha, 2012). In such transactions, the sensitive data is normally protected by a secure web protocol like Hypertext Transfer Protocol Secure (HTTPS) that provides a secure channel between the user's machine and the e-commerce server. However, the effectiveness of HTTPS can be limited by poor browser implementations, server software or a lack of support for some algorithms. Furthermore, although HTTPS secures the data as it travels between the server and the client, once the data is decrypted at the destination it is only as secure as the host machine.

The ability of internet browsers to extend their functionality through the use of external plugins exacerbates the vulnerability of browsers to client-side attacks. Adversaries use the same distribution channels as legitimate plugins to distribute malicious software to user machines with or without user consent. Client-side attacks are becoming more prevalent due to a lack of initiative by traditional security measures (antivirus) in identifying these attacks. Compromised software on the client-side leads to malicious agents manipulating transaction information between the client and server, and the theft of sensitive information.

One solution for overcoming this vulnerability is the remote attestation technique introduced by the Trusted Computing Group (TCG specification architecture overview, 2007). Remote attestation allows the remote host (server) to verify the integrity of another host's (client) platform over a network. The remote host is then able to trust that the integrity of the client platform is unaffected by malicious