2018 International Conference on Advanced Science and Engineering (ICOASE), Kurdistan Region, Iraq

# Boost Secure Sockets Layer against Man-in-the-Middle Sniffing Attack via SCPK

Mohammed Abdulridha Hussain
*Computer Science Department,*
*College of Education for Pure Science, University of Basrah*
Basrah, Iraq
mohsubber@gmail.com

Zaid Alaa Hussien
*Technical Business Management Department, Management Technical College*
*Southern Technical University*
Basrah, Iraq
zaidpc2005@gmail.com

Zaid Ameen Abduljabbar
*Computer Science Department,*
*College of Education for Pure Science, University of Basrah*
Basrah, Iraq
alsulamizaid@gmail.com

Sarah Abdulridha Hussain
*National Center for Managment Development and Information Technology,*
Basrah, Iraq
sarah_subberidsco@hotmail.com

Mustafa A. Al Sibahee
*School of Computer Science and Technology,*
*Huazhong University of Science and Technology*
Wuhan, China
mustafa.a@hust.edu.cn

**Abstract— Recently, variety purposes of Internet used present a demand to embody highest levels of security in every network-connected device. This proposal strives to address a secure network connection via Secure Certificate Public Key (SCPK) to resist the Man-in-the-Middle Sniffing attack on SSL. The model aims to encrypt Certificate Public Key and authenticate between clients and servers. Drawing on our simulation, proposed key is secure, efficient and safely monitor.**

**Keywords— Web Security, SSL, Man-in-the-Middle attack, Sniffing MITM, HTTPS**

## I. INTRODUCTION

The emerging need for HTTPS is to secure communication and authentication between clients and servers, as well as protection against Hypertext Transfer Protocol (HTTP) attacks. HTTPS is an aggregation of HTTP and Secure Socket Layer (SSL), notably known as Transport Layer Security (TLS). Generally SSL deployed to protect data sent via HTTP between clients and servers. This technique is called HTTP Over transport layer security (HTTPS) [1].

Currently, web applications based on Hypertext Transfer Protocol (HTTP) are widely used for several services. Yet, their security concern is crucial. HTTPS secures the communication after the middle of the SLL handshake procedure. The communication is encrypted when the client receives the server certificate, in which the first messages are cleared for transfer without encryption. Where an attacker can easily steal unencrypted session information [2].

Nowadays infrastructure for securing connections on the Internet heavily relies on X.509 and public-key infrastructure (PKI), which is maintained by Certificate Authorities (CAs) [5].

Hence, the verification logic is completely controlled by the application, or in other words the application is responsible for implementing the SSL/TLS certificate validation correctly. Further if such a validation scheme is not correctly employed, users face the risk of a Man-in-the Middle (MITM) attack [10]. Such attacks can have significant implications especially in the financial sector, which increases the importance in the domain of secure connection.

Recent research outlined HTTPS protection against MITM attacks [1–4] showing some drawbacks, cache memory problem and excessive consumption of server processing time.

However previous researches often fail to implement proper certificate validation in their custom SSL/TLS implementations and thus fail to secure the network communication [10].

Das et al. [11] proposed a solution which can resist the MITM attack on SSL/TLS-enabled applications. In the present work, we proposed to resist sniffing MITM attack by encryption of the public key of the web server in the certificate. This approach is called Security Certificate Public Key (SCPK). The main contributions of our paper in network security are:

1) Our proposed scheme can withstand MITM sniffing attacks by encrypting the web server public key of the certificate.
2) Our proposed scheme can prevent an attacker from modifying or creating a forged certificate, so the malicious attacker cannot eavesdrop on transmitted data.
3) Combining the server name with its public key prevents client from being cheated on by the attacker. The client can compare the requested web server name with the received name within the certificate.

The rest of the paper is organized as follows. Section II discusses related works. Section III presents the background of the proposal. Section IV discusses the SCPK design and strengths. Section V explains implementation and results. Section VI demonstrates the SCPK strength through a discussion on security. Finally, Section VII presents the conclusion.

978-1-5386-6696-8/18/$31.00 ©2018 IEEE