SECURITY AND COMMUNICATION NETWORKS
*Security Comm. Networks* (2014)
Published online in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1113

RESEARCH ARTICLE

# TSSL: improving SSL/TLS protocol by trust model

Maryam Asadzadeh Kaljahi[1]*, Ali Payandeh[2] and Mohammad Bagher Ghaznavi-Ghoushchi[3]

[1] Department of IT, Tehran University, Tehran, Iran
[2] Department of Computer Engineering, Maleke-ashtar University, Tehran, Iran
[3] School of Engineering, Shahed University, Tehran, Iran

## ABSTRACT

Transport Layer Security (TLS) is the most popular security protocol of the transport layer. It is widely used to provide basic security services of authentication, confidentiality, and integrity of sensitive data. It is carried out in critical untrusted networks between client and server entities, such as e-commerce and online transactions. Despite multiple capabilities, TLS protocol is vulnerable to the malicious server attacks that may cause a serious threat to TLS-based e-commerce communications. This should be considered as the first problem of this protocol. The other problem of TLS is sending many messages during the handshake phase for providing a successful negotiation and a secure communication. So, this phase is the most complex and time-consuming phase of the TLS protocol. This causes decreasing of service capacity and using more time. We are going to propose a new protocol based on trust model called "TSSL protocol" in this paper. This model is used to conquer the disadvantages with security of the TLS protocol. Through this paper, it is going to be indicated that the proposed model has higher levels in both security and performance compared with the conventional TLS. Copyright © 2014 John Wiley & Sons, Ltd.

**KEYWORDS**

authentication; TLS protocol; Secure Sockets Layer/Transport Layer Security; handshake protocol; trust Model

***Correspondence**

Maryam Asadzadeh Kaljahi, Department of IT, Tehran University, Tehran, Iran.
E-mail: m.asadzadeh@ut.ac.ir

## 1. INTRODUCTION

Nowadays, Internet brings threats to the information security and has become increasingly important because of the steadily growing data volume. Every user sends various types of the sensitive data such as career, financial data, and usernames/passwords that must be carefully protected when they are transmitted across untrusted networks and the open internet. To this end, a practical Transport Layer Security (TLS) protocol has been adopted for the protection of the confidentiality and reliability of the data in transition encompassing all network services that use Transmission Control Protocol (TCP)/Internet protocol (IP) [1–8]. The TLS protocol allows the server and the client to authenticate each other to negotiate encryption algorithms and cryptographic keys in the handshake before sending and receiving the first byte of data [9]. In this way, it shields the operation of the underlying security functionalities of web browsers from the users [3]. At the present time, HTTP over Secure Sockets Layer (SSL)/Transport Layer Security (TLS) is the dominant paradigm to guarantee security for web interaction and web-based applications relying on the HTTPS protocol. But the TLS is not perfect in the practical application [10], and new innovative methods are needed to secure communication. In detail, TLS has two main defects. First, the initial handshake protocol needs intensive computational resources because of the cost of public-key cryptography operations especially decryption at the server and also depending upon digital certificate [9,11–17] and the second difficulty is vulnerability to malicious servers [10,18,15,6]. The goal of this work is to overcome the TLS protocol's problems by designing TSSL protocol that uses the traditional TLS and a trust model to promote the security and performance of TLS. Unlike previous efforts, our current design of trust-based protocol mainly focuses on detection and isolation of unreliable servers. The trust model integrates past history, recent feedback, and reputation of servers in a dynamic way and identifies the current trust level. Here, TSSL protocol employs Dynamic Trust Model (DTM) trust model to the rate reliability of the servers that mostly concentrates on enhancing the accuracy in choosing a trustworthy server to interact with, in the presence of malicious agents. In terms of efficiency, in trusted-server case, TSSL protocol allows a client to use an abbreviation handshake while defeating malicious server attacks.

This paper is organized according to the following plan: Section 2 overviews and recalls some basic TLS's features and existing problems. Trust models and the related works