Chapter 38
Performance Evaluation of Secure Data Transmission Mechanism (SDTM) for Cloud Outsourced Data and Transmission Layer Security (TLS)

Abdullah A. Alhaj
The University of Jordan-Aqaba Branch, Jordan

ABSTRACT

The Cloud has become a significant topic in computing; however, the trend has established a new range of security issues that need to be addressed. In Cloud, the data and associated software are not under their control. In addition, with the growing demands for Cloud networks communication. With the increasing demand for computer communications the need for security is growing dramatically. The existing research related to security mechanisms focuses on security of the data transmission in the communication networks only. The authors developed specific Secure Data Transmission Mechanism (S SDTM) for cloud outsourced data is a set of technologies and solutions to enforce security policy and bandwidth compliance on all devices seeking to access network computing resources, in order to limit damage from emerging security threats and to allow network access only to compliant and trusted endpoint devices. IPSec is a suite of protocols that adds security to communications at the IP level. Protocols within the IPSec suite make extensive use of cryptographic algorithms. Since these algorithms are computationally sophisticated, some hardware accelerators are needed to support high throughput. In this paper, the authors compare between secure data transmission mechanism for cloud outsourced data with preemption control algorithm and TLS to improve the properties of the S SDTM and the Virtual Private Networks (VPN) built with both protocols.

DOI: 10.4018/978-1-4666-6539-2.ch038

1. INTRODUCTION

The concept of cloud computing offers new methods and approaches for information processing and data transmission and however, the Federal CIO Vivek Kundra has emphasized that information security is still a top concern about cloud computing (Worthen, 2009). For instance, In Cloud, the data and associated software are not under their control (Aljawarneh, 2011).The increasing demand for communication over public networks has brought with it a need to securely protect sensitive information sent over this open network (Alhaj, 2013). The TLS protocol has become a de facto standard for cryptographic protection of the Internet http traffic. After developing its limitations, TLS3.0 aims to provide Internet client/server applications with a practical security mechanism (Rescotla, 2001).

IPSec is a suite of protocols designed to provide high quality cryptographically-based security for IPv4 and IPv6. IPSec provides security services: access control, integrity, authentication, confidentiality (encryption), and replay protection to the IP layer as well as the layers above (Stallings, 2003).

IPSec is a suite of protocols that adds security to communications at the IP level. This suite of protocols is becoming more and more important as it is included as mandatory security mechanism in IPv6. IPSec is mainly composed of two protocols, Authentication Header (AH) and Encapsulating Security Payload (ESP). The former allows authentication of each IP datagram's selected header fields or depending on the operational mode that has been selected – of the entire IP datagram. The latter allows encryption – and optionally authentication – of the entire IP datagram or of the IP payload, depending on the operational mode that has been selected, namely the transport and the tunnel modes. The former was designed for being used in host machines, while the latter is for secure gateways. In tunnel mode the entire original IP datagram is processed; the result becoming the data payload of a new IP datagram with a new IP header. In transport mode only parts of the original IP datagram are processed (e.g., the data payload for the ESP protocol) and the original IP header is kept with some small modifications. Through encryption, authentication, and other security mechanisms included in IPSec (e.g., anti-reply), data confidentiality, data authentication, and peer's identity authentication can be provided [1, 2, 3].

The SDTM will investigate IPSec to secure the communication between one or more paths, between two pairs of hosts, between a pair of security gateways, and a host and a security gateway (SG). This is why we will compare between TLS and the SDTM to show the properties of the SDTM.

1.1. Description of the SDTM

The main goal of the S SDTM is to data transmission algorithm with preemption control algorithm in heterogeneous networks and providing quality of service data transmission: possibly, maximizing throughput, minimizing delay and lost packets by implementing the strongest security strategy and investigating various security algorithms.

2. THE MAIN FEATURES OF THE SDTM

- When SDTM is implemented in a firewall or gateway, it provides strong security that can be applied to all traffic crossing the perimeter. Traffic within a workgroup or company does not incur the overhead of security–related processing;
- SDTM in a firewall is resistant to bypass if all traffic from the outside must use IP, and the firewall is the only means of entrance from the Internet into the organization;
- SDTM as it investigates the IPsec is below the transport layer (TCP, UDP) and so is transparent to application. There is no need to change software on a user or server system when it is implemented in the firewall or gateway;