Chapter XII

TLS, SSL, and SET

In an Internet commercial transaction, the secure Web server and the buyer’s computer authenticate each other and encipher the data transmitted using transport layer security (TLS) or secure socket layer (SSL) protocols.

When a purchase is made online using a credit card, does the customer’s bank need to know what was purchased? Not really. Does the seller need to know the customer’s credit card number? Actually, the answer is no. The responses to these questions were the main premises of the secure electronic transaction (SET). In the late 1990’s, SET was approved as the credit card standard, but it failed to be accepted because of its cost and the problems regarding distribution of end-user certificates. However, SET is explained in this chapter as an ideal protocol, from the point of view of certificates, digital signatures, and cryptography for securing credit card transactions over the Internet.

Objectives

- Learn how TLS and SSL provide security services to IP Networks
- Fully understand the SET protocol and transactions

Copyright © 2008, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
Online commerce is growing at a substantial rate, partially because of the implementation of several protocols that secure Internet transactions. When people purchase an item over the telephone, they give their credit card information to a person who may then sell the information to someone else. In an Internet transaction, buyers enter their credit card information into their computers, and when they hit the “Submit” button, the Web browser secures the credit card transaction. In that secure transaction, the secure Web server and the buyer’s computer authenticate each other and encipher the data transmitted.

Several protocols are used to secure an Internet transaction, but the most widely used are SSL from Netscape, and the Internet standard of SSL, known as transport layer security (TLS). TLS versions 1.1, 1.0 and SSL versions 3.1 and 3.0 are very similar, which makes supporting both TLS and SSL easy. SSL and TLS are built into all Web browsers.

Even though both Netscape and Internet Explorer implemented SSL in their Web browsers, they did it differently. This meant that companies had to deploy a separate application for each of the two browsers. SSL 3.0 and 3.1 outgrew being just a Netscape standard, and continued development of the protocol is now the responsibility of the Internet Engineering Task Force. As a result, SSL 3.0 and 3.1 developed into a proposed standard for Transport Layer Security 1.0, RFC 2246, and TLS 1.1, RFC 4346 (Dierks & Rescorla, 2006). In this chapter, the TLS 1.1 protocol is explained, but all explanations are also applicable to the SSL 3.1 protocol.

The TLS and SSL protocols are used to secure a client-server communication over the Internet, and they negotiate and provide the essential functions of a secure transaction: mutual authentication, data encryption, and data integrity. There are two SSL versions: SSL 2.0 supports server authentication only; SSL 3.1 supports both client and server authentication. TLS 1.0 and 1.1 support both client and server authentication.

TLS and SSL allow users to define the level of security that best meets their needs. Both are industry standards and are used in millions of Internet transactions. Users can select RC4, DES, 3DES, or AES for encryption and, for authentication, they can select RADIUS (username and password), RSA SecurID (username and token + pin), or X.509 digital certificates.

A secure client-server communication requires server and client authentication, a cryptographic key exchange where both parties agree on a pre-master secret key, and the enciphering of data using keys generated from the pre-master key. When a client and a server agree to communicate using the TLS or SSL protocol, they also need to agree on several other key points: (1) which protocol and version (TLS 1.0, 1.1, SSL2 or SSL3) to use, as well as which cryptographic algorithm; (2) whether or not to authenticate each other; (3) that certain public-key encryption techniques will be used to generate a pre-master secret key; and (4) that session keys will be created to encipher the message. These processes are performed in the TLS or SSL handshake protocol.

Digital certificates allow the client and the server to identify each other. In all TLS and SSL handshakes, the client will authenticate and verify the identity of the server using digital certificates. The server can also request that the client send its a client digital certificate (optional). Because digital certificates are issued by certificate authorities, the TLS or SSL client must trust the certificate authority that issued the server’s certificate in order for the
Related Content

Designing Information Systems and Network Components for Situational Awareness
www.igi-global.com/chapter/designing-information-systems-network-components/62378?camid=4v1a

Security Issues in Web Services
Priyanka Dixit (2018). Handbook of Research on Network Forensics and Analysis Techniques (pp. 57-64).
www.igi-global.com/chapter/security-issues-in-web-services/201604?camid=4v1a

Trust Management and Context-Driven Access Control
www.igi-global.com/chapter/trust-management-context-driven-access/22064?camid=4v1a
Financial Early Warning System for Risk Detection and Prevention from Financial Crisis