

White Paper:

An Introduction to SSL/TLS

June 2003

Introducing SSL and TLS

This document provides an overview of SSL or TLS. SSL stands for Secure Sockets Layer and TLS stands for Transport Layer Security. They are essentially the same thing as will be described. SSL is being used to provide secure web access for e-commerce applications, secure web access for internally protected systems (such as Human Resources) and secure remote access from devices as diverse as a laptop or mobile phone. There are many other areas where SSL is or will be used, but these three are the most popular and it is the last category (Remote Access) that we wish to explore in some depth.

What are SSL's Origins?

SSL was developed by Netscape as a mechanism to provide secure communication over an insecure medium such as the Internet. Users of the early Internet would have been reluctant (quite rightly) to perform credit card transactions without security, and the advent of SSL-enabled web browsers and servers allowed secure communications to take place.

Netscape published the SSL specification and provided support in both their browsers and server software. Other vendors followed including open source server solutions such as Apache and SSL became the defacto tool for secure web transactions.

With the availability of strong encryption in all users' web browsers, the scene was set for the e-commerce market to take off. Despite early scepticism by the media, e-commerce is now firmly established as a way of shopping. Strong encryption is available in most browsers today including those devices from Nokia such as the 92x0 and many general -purpose phones. Encryption strength is something that is negotiated at set-up and it is possible for both the browser and the server to discover the highest or most compatible version of encryption they both support. At this stage, a decision can be made whether to proceed with the session establishment.

SSL is now an IETF (Internet Engineering Task Force) standard and is referenced as Transport Layer Security or TLS and is defined in RFC 2246 (<http://www.ietf.org/rfc/rfc2246.txt>).

Authenticating Users

SSL is an independent security layer added into the communications stack. It is usually operated over IP, but can, in fact, operate over many other protocols as it has been designed to be protocol independent. With IP it usually operates over the TCP layer and ensures the encryption of all data from a particular application (i.e. the web browser session) between the user's device and the server. Several things are negotiated during set-up including certification or proof of identity of both the client (browser) machine and the server. What is not performed during any of this is authentication of the user.

Early e-commerce systems used server -based solutions to authenticate the users and terminate the SSL session. It very quickly became apparent that the server performance was a bottleneck to mass market e-commerce. To authenticate the users, the server would associate a particular session with an individual and go through an authentication sequence. Most servers now support a wide variety of schemes and allow authentication using everything from passwords to two factor token -based schemes such as SecurID and biometric systems such as retina scans. Most users' experience of authentication is via password at the online bank or on the e-commerce site.

Using SSL to Provide Secure Connectivity

Secure Connectivity is a requirement for all enterprises that have communications with employees, partners and associates. Remote connections to third parties should be controlled, logged and secure. Recently there has been a surge in growth for IPsec based VPN solutions. These have great benefits in that they allow any medium to be utilised for communication including wired and wireless and allow any application that is available on the wired network to be utilised by a remote user. Access control and authentication are usually included, and the user goes through an authentication and establishment phase. Access control can be enabled by deploying an appropriate security policy to the VPN devices or

clients and it is then possible to restrict partner access to the appropriate parts of the network. Nokia has developed a leading IPSec VPN solution that has client support for Windows, Linux, Macintosh, Symbian and Pocket PC. All clients are managed by the same policy server allowing the user similar access regardless of the device they are using to access the network.

At first sight, SSL seems nicely pigeon-holed into the e-commerce slot. However if you take a closer look, it has many of the same features as an IPSec VPN. It can include strong authentication, it can prove the server and the browser ID, it encrypts the communication using strong encryption, but it only supports web browsers and therefore web enabled applications. Email solutions had required a special client such as Outlook for users to access email and calendar. Microsoft, Lotus and others started offering a web interface into their email servers, allowing users to access these services using a standard browser.

If you could therefore put together a server that could terminate a lot of SSL sessions without performance degradation, authenticate the users and offer network level reliability, SSL-based remote access solutions look interesting for specific types of users. This is what several server manufacturers started to do in order to support large populations of e-commerce or e-banking customers.

SSL in the Enterprise

SSL is also interesting to many corporate users for a remote access solution for a number of key reasons. Most IT departments have ceased development of specific client server applications as they are costly to develop, require a client to be installed and managed and tend to lock the customer into a single supplier as the customer's systems expand. SSL does not require the enterprise to install any client software as it utilizes the encryption capabilities of the web browser that is standard with most PC's, PDA's and modern phones.

Most users spend their online time performing PIM functions (Personal Information Management) such as Email, Calendar and Intranet access. As many specialist applications are now available web enabled, SSL is an attractive solution. Web enabled applications such as Email (Outlook and Notes), CRM (Customer Relationship Management) and ERP (Employee Resource Planning) are available to browser-based clients including suppliers and customers. What is needed is some form of access control and logging in order to restrict users to the resources they are allowed to access. If this can also be included, it becomes possible to provide secure connectivity to all forms of remote users as long as they have a device with a secure browser that meets certain criteria.

SSL is therefore attractive for a number of key reasons:

- No client is required on the user's device, dramatically reducing support costs and allowing any device with a secure browser to be utilized
- SSL is as secure as an IPSec VPN and in fact may be more secure in specific mobile situations. For example a browser-based solution only allows a single page at a time to be viewed or downloaded. An IPSec VPN could allow access to the entire database file
- It is easier to quickly add a partner to the remote access solution without having to deploy and support specific client software or hardware
- Home users and employees without a company provided laptop can be securely supported
- The solution is flexible, elegant and simple