Comparison of internet security protocols

Profession

Introduction

I have been asked to research and compare two of the most widely used internet security protocols, Transport Layer Security (TLS) and Secure Shell (SSH). In this report I shall research both protocols and then compare the two listing similarities and differences in how they operate as security protocols. I shall examine the features of both giving advantages and disadvantages, examples will be given for both security protocols and any infrastructure needs.

As per instruction I will be using varied sources for my research including books, magazines and the internet, as with any report I shall reference all of my sources of information.

Transport Layer Security

Today the need for network security is of uppermost importance. We would all like to think that data is transmitted securely, but what if it wasn’t. Credit card crime for example would be a lot easier if there was no network security. This is one of many reasons why we need network security, and to achieve this we need protocols to secure the end to end transmission of data.

An earlier protocol that was widely used in the early 1990’s this was the Secure Socket Layer protocol (SSL). SSL was developed by Netscape but had some security flaws and used a weak algorithm and did not encrypt all of the information. Three versions of SSL where developed by Netscape and after the third the Internet Engineering Task Force (IETF) were called in to develop

an Internet standard protocol. This protocol was called the Transport Layer Security (TLS) protocol. The main goal was to supply a means to allow secure connections for networks including the internet.

How it works

The Transport Layer Security protocol uses complex algorithms to encrypt information as it is sent over the network. The protocol comprises of two main layers the Transport Layer Security Record and the Handshake Protocol.

TLS Handshake Protocol

The TLS Handshake protocol is used to; in principle agree a secret between the two applications before any data is sent. This protocol works above the TLS Record protocol and sends the secrets in the order in which they have to be sent. The most important feature here is that no data is sent in securing connection, the first bit sent is a start bit to the whole process and only when secure connection achieved is data sent over the network.

TLS Record Protocol

The Transport Layer Security Record encrypts the data using cryptography and uses a unique key for connection which is received from the Handshake protocol. The TLS Record protocol may be used with or without encryption. The data which has been encrypted is then sent down to the Transmission Control (TCP) layer for transport. The record also adds a Message Authentication Code (MAC) to the outward data and confirms using the MAC. I have used the image below to show how this is achieved.

Where TLS is used

The Transport Layer Security protocol is normally used, above any of the Transport Layer protocols. So the TLS protocol operates at Open Systems Interconnection (OSI) level 4, where it joins itself to other transport layer protocols, for example Hypertext Protocol(HTTP) and File Transfer Protocol (FTP) although its main partner is Transmission Control Protocol(TCP).

Main area of use would be the internet in applications that need end to end security. This data is usually carried by HTTP and with TLS becomes HTTPS. TLS is therefore used to secure connections with e-commerce sites. VoIP also uses TLS to secure its data transmissions." TLS and SSL are most widely recognized as the protocols that provide secure HTTP (HTTPS) for Internet transactions between Web browsers and Web servers." (Microsoft, 2011)

The Transport Layer Security protocol is also used in setting up Virtual Private Networks (VPN), where end to end security is a must but again is used alongside other protocols.

How Secure Is It?

Secure Shell

The Secure Shell (SSH) is used for safe remote access between clients through an untrusted network. SSH is widely used software in network security. The need for such protocols is paramount in today'stechnologybased world. In the modern office for example employees may wish to transfer files to their home computer for completion, this would be an unwise option if it wasn't for security protocols. A man in the middle

attack could take place by listening on the network for traffic and picking up all your company secrets or personal ones.

How it works

The Secure Shell develops a channel for executing a shell on a remote machine. The channel has encryption at both ends of the connection. The most important aspects of SSH is that it authenticates the connection and encrypts the data it also ensures that the data sent is the data received.

Bibliography

TLS protocol. (2011, 03 23). Retrieved March 23, 2011, from wikipedia: http://it. wikipedia. org/wiki/File: EAP-TLS_handshake. png

Microsoft. (2011, March 23). What is TLS. Retrieved March 23, 2011, from Microsoft TechNet: http://technet. microsoft. com/en-us/library/cc784450%28WS. 10%29. aspx