A report on transport layer security (tls) and secure shell (ssh)

Law, Security

Introduction

Transport Layer Security (TLS)vs. Secure Shell (SSH)– A battle for security.

In this modern time, individuals, businesses and organizations worry about security on a regular basis, be it online or offline, over a network computer or just with a personal computer.

Security of a computer connected to the internet and within a network is very essential as people need to protect their information and data from unwanted or unauthorised access.

My task here is to look into two most widely used security protocols on the internet network, these protocols are Transport Layer Security (TLS) and Secure Shell (SSH). I will be comparing these two protocols, looking into their similarities and differences, advantages and disadvantages and giving related examples where necessary.

An Overview of the Protocols

First and foremost what is TLS It is the replacement for secure socket layer (SSL) and it is a protocol that makes sure that there is privacy between a communicating application and its users on the internet. TLS offers an end point authentications and communications privacy over the internet using encryptions.

For instance, if a server and a client communicate, TLS makes sure that no one without the right authority can listen, intrude or forge any messages between them.

TLS has two layers, the TLS record protocol and the TLS handshake protocol.

The TLS Record Protocol is at a lower level where it is placed on top of some reliable transport protocol as Transport Control Protocol (TCP). This is needed in other to send messages in two directions, forward and backward and it also has a security property that is used to establish a reliable and private connection. The record protocol is then responsible for changing position of data between two ends of the link using the values agreed through the handshake protocol.

The information that then come from the application to the TLS record protocol, are compressed and encrypted as required before they are sent to the other end. And if the other end is valid, the information is then uncompressed and decrypted before delivery. The TLS handshake protocol also uses the record protocol to send its messages during the hand shake stage.

There are additional offers that are commonly overlooked which are provided by TLS, “ integrity guarantees and replay prevention”.

TLS streamscommunicationhave inbuilt controls to prevent tampering with any portion of its encrypted data. And there are other inbuilt controls to stop captured streams of TLS information from being replayed at other times.

On the other hand, SSH is a protocol that determines the performance of a secure communication over a network. This has been used to replace telnet, rsh, rlogin for insecurity. Prior to any transfer taking place, the SSH client

and server must first establish a secure connection. This will then allow them to share private information between each other.

The SSH protocol is responsible for authentication, encryption, and the way data is transmitted over a network.

“ The encryption used by SSH is intended to provide confidentiality and integrity of data over an unsecured network, such as the Internet”.

There are two types of versions for the SSH, the first is SSH1 and the second is SSH2. Although, these two protocols are different.

The SSH1 is the original protocol and it has its own shortfalls, so it is not normally recommended or in use today. But SSH2 is the common of the two SSH protocols and is commonly used today as it is more secure and efficient than SSH1. The SSh1 uses server and host keys to verify the networks while SSH2 uses just the host keys to verify the networks and even more, they are not compatible with each other.

SSH works in the following way

When a client contacts a server, they disclose the SSH protocol versions that they support. Then, they switch to a packet based protocol. When the server identifies itself to the client and provides session parameters, the client then sends the server a secret key. Both sides turn on encryption and complete server authentication. Then, a secure connection is created.

Similarities and Differences

Similarities

In terms of similarities, one can say they provide the same level of security within any giving scenario. They both make sure that information passed about over the internet is protected with dependable encryption. They can also make sure that the server a user connects to is the right one.

The two protocols provide 128-256 bit encryption.

Differences

Inrespectto their similarities, they do have some differences as well. Most obvious is the fact that SSH uses username and password to authenticate its users which is inbuilt. While TLS “ authentication is left up to the daemon receiving the connections”

SSH is at the top of the model at the application layer while, TLS is able to offer security at the transport layer.

SSH is connection oriented which use TCP only, and it is primarily used for shell based solutions.

SSH offers number of client authentication options, TLS only uses the public key option.

There are SSH components such as its connection protocol SSH-CONN. SSH-CONN provides multiple logical data channels to the applications using SSH-TRANS which TLS does not have.

SSH Advantages and Disadvantages

Advantages

It is reliable, it is available free and also in commercial versions

It never trusts the network

If the network is experiencing a hostile takeover, it will only disconnect the SSH, but any decryption or connection take over is impossible.

It is possible to tunnel TCP based applications through SSH, e. g., email protocols.

For system administrators, SSH is a popular remote administration platform.

Although, the server runs on UNIX, Linux and VMS, SSH clients can run on most platforms.

“ Many authentication methods including Kerberos, TIS, SecurID and RSA. Can be SOCKS5 proxy aware”

Disadvantages

SSH is not designed to be added into network gateways such as routers or firewalls.

Performance for SSH can be a problem on old machines.

Its port range and dynamic ports cannot be forwarded.

A client on the Internet that uses SSH to access the Intranet can expose the Intranet by port forwarding.

When a user authenticates themself on a server, it is always sent in clear text

TLS Advantages and Disadvantages

Advantages

TLS is easy to use. Probably the most used security on the internet.

TLS do not need any Operating system support.

When messages are exchanged over the Internet, they are checked while transmitting from one computer to another. This feature offers reliability of the web based communication.

TLS protocol stops unauthorized user access from interfering as a third party in the middle of a communication on the Internet. The third party will only take part in the communication when it has been noticed by two authorized users

TLS is in use by most web browsers

It is widely recognized as the secure HTTP (HTTPS) Protocol

Disadvantages

TLS often mistake firewalls as man in the middle attack.

It is exposed to clogging over TCP

Security Weakness

Examples

TLS can be used in many applications; client/server applications but it has mostly been used with the Hypertext Transfer Protocol “ HTTP” for security. This allows it to offer an encrypted conversation and to securely identify a network web server. The added security it offers allows HTTPS to be used for all level of transaction over the internet world wide.

Secure Multipurpose Internet Mail Extensions “ SMIME” when combined TLS can be used to secure IETF VoIP signalling.

TLS can also be used in these following applications: PKIX, LDAP, BEEP, SASL, L2TP, SMTP, IMAP, and POP3.

An example can be seen below with my home web browsers. I have two screenshots from Internet Explorer and Firefox web browsers.

Internet Explorer 9Firefox version 3. 6. 15

SSH can also be used in some applications as well. SSH do have some features such as port forwarding and secure tunnelling.

Port forwarding can tell the SSH daemon to listen to information conversations on a particular port and forward this conversation to an encrypted SSH session. This allows protectection for other services as well.

Summary

there are no magical solution for web, but good enough protocols, the real deal is that there is no better protocol, they all have their benefits.

In order to decide which one to use, one really need to understand what one is trying to secure.

References

I have been able to obtain and generate ideas from the following sources

Books

Mark Minasi, Christa Anderson, Michele Beveridge, C. A. Callahan

Mastering Windows Server 2003, copyright, 2003 Sybex Inc

O’Reilley. Daniel J Barrett, Richard E Silverman and Robert G Byrnes

SSH, the secure shell, the definitive Guide, copyright, 2005

William Stallings. 2006 Fourth Edition

Cryptography and Network Security

Bill Ferguson (Sybex)

Network + Fast Pass, copyright 2005

IBM TCP/IP Tutorial and Technical Overview

December 2006

Internet Research

Wikipedia

http://en. wikipedia. org/wiki/Secure_Shell#Definition

Last modified on 16 March 2011 at 10: 48

http://en. wikipedia. org/wiki/Secure_Shell#Definition

Last modified on 16 March 2011 at 13: 11