Survey Of Application layer security protocols

By: Albaihan ,Abdullah.
E-mail:aalbaihan@yahoo.com
Date: 24/01/2007.

Abstract

Within the millions of people entry to Internet world, increase the need for security in sending and receiving emails and encryption and decryption files and Confidentiality and Integrity Authenticity, etc.. that we must use some protocols that help us to secure our data and messages .The application layer has some security protocols and programs E.g. SSH, HTTPS , PGP, etc..

Introduction

As we know the TCP/IP includes four layers, Application Layer ,Transport Layer, Internetwork Layer, Network Access Layer. the axel in this paper is Application Layer. It Provides services to send and receive data over the network, e.g., telnet (port 23), mail (port 25), finger (port 79).And Interface to the transport layer: Operating system dependent, Socket interface. Application Layer Security has some Advantages and Disadvantages. The Advantages are:

- Most flexible.
- Executing in the context of the user → easy access to user's credentials.
- Complete access to data → easier to ensure nonrepudation and small security granularity.
- Application-based security

And the disadvantages:

- Most intrusive.
- Implemented in end hosts.
- Need for each application →
  - Expensive.
  - Greated probability of making mistake.

The application layer has some security protocols and programs E.g. SSH, HTTPS , PGP,etc... This paper Shows SSH protocol and PGP program in details.

Outline

This Paper is organized as follows: Section 1 presents SSH protocol, overview, history, features, how it works and SSH architecture. Section 2 presents PGP program, overview, history, features, When we need PGP , and How PGP works. Section 3 presents comparisons between the SSH protocol and PGP protocol.

1. SSH Protocol:

In 1995, Tatu Ylönen, a researcher at Helsinki University of Technology, Finland, designed the first version of the SSH protocol. [3]

Secure Shell (SSH) is a protocol to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another.[11]

The goal of SSH was to replace the earlier rlogin, TELNET and rsh protocols, which did not provide strong authentication or guarantee confidentiality.

The SSH protects against:

* Eavesdropping of data transmitted over the network.
* Manipulation of data at intermediate elements in the network (e.g. routers).
* IP address spoofing where an attack hosts pretends to be a trusted host by sending packets with the source address of the trusted host.
* DNS spoofing of trusted host names/IP addresses.
* IP source routing. [12]

But SSH does not protect against:

* Incorrect configuration or usage .
* A compromised root account. If you login from a host to a server and an attacker has control of root on either side, he/she can listen to your session by reading from the pseudo-terminal device, even though SSH is encrypted on the network, SSH must communicate in clear text with the terminal device.
* Insecure home directories: if an attacker can modify files in your home directory (e.g. via NFS) he may be able to fool SSH. [12]

Some features of SSH:

* Strong authentication. Closes several security holes (e.g., IP, routing, and DNS spoofing).
* Improved privacy, All communications are automatically and transparently encrypted.
* Arbitrary TCP/IP ports can be redirected through the encrypted channel in both directions (e.g., for e-cash transactions).
* Host authentication key distribution can be centrally by the administration, automatically when the first connection is made to a machine.
* Any user can create any number of user authentication RSA keys for his/her own use.
* An authentication agent, running in the user's laptop or local workstation, can be used to hold the user's RSA authentication keys.
* The client is customizable in system-wide and per-user configuration files.
* Complete replacement for rlogin, rsh, and rcp. [11]

In 1996, a revised version of the protocol, SSH-2, was designed, incompatible with SSH-1. SSH-2 features both security and feature improvements over SSH-1. Better security, for example, comes through Diffie-Hellman key exchange and strong integrity checking via MACs. New features of SSH-2 include the ability to run any number of shell sessions over a single SSH connection. [3]

How Secure Shell Works

SSH can be divided into two broad parts:

1- Establishment of a secure connection between the SSH client and server:

SSH sets up a secure connection between the client and server to protect the privacy of any communication that occurs over the network. Privacy refers to protecting the secrecy of the data from being interpreted by an attacker who might be listening in on the connection. To ward off such threats, SSH encrypts all the data transmitted between client and server using strong encryption algorithms. In the present context, a secure connection not only entails privacy protection of all transmitted data, but also guards against data tampering in what is known as integrity checking.

A certain amount of preparation is needed prior to the establishment of a secure connection. This multistep process involves:

1.1 disclosure between the client and server of supported SSH protocol versions;

1.2 authentication of the server to the client;

1.3 agreement between client and server regarding encryption, compression, and authentication methods to be used for the session; and

1.4 generation of the symmetric key for encryption . [5]

A secure connection is set up if all the preceding steps complete successfully. Henceforth, all communication between client and server will be encrypted for secrecy and checked to guard against corruption or deliberate tampering.

2- Authentication of the client to the server :

The client then attempts to authenticate itself to the server using any of the following methods until one succeeds.

Under the SSH-1 protocol, six authentication methods are tried in the following order:

Kerberos , Rhosts , RhostsRSA ,Public-Key , TIS , User password.

while the SSH-2 protocol only supports three:

Public-key , RhostsRSA , User password. [5]

SSH architecture

SSH has a client/server architecture, as shown in Figure 1-1. An SSH server program, typically installed and run by a system administrator, accepts or rejects incoming connections to its host computer. Users then run SSH client programs, typically on other computers, to make requests of the SSH server, such as "Please log me in," "Please send me a file," or "Please execute this command." All communications between clients and servers are securely encrypted and protected from modification. [10]

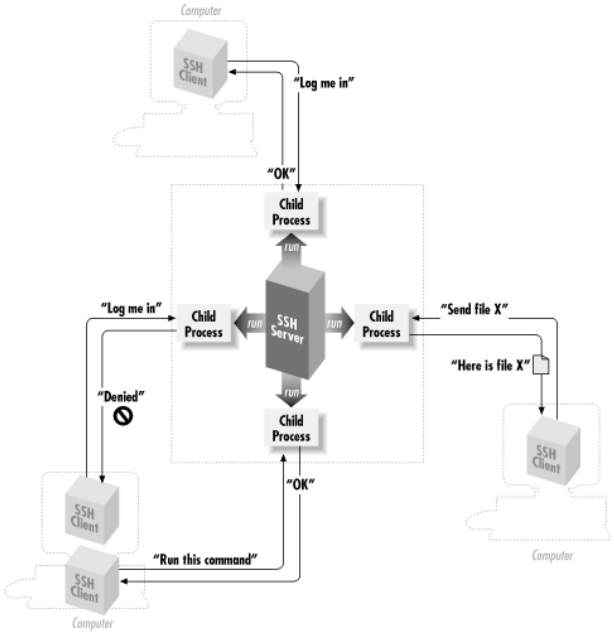

Figure 1-1. SSH architecture

The SSH protocol covers authentication, encryption, and the integrity of data transmitted over a network, as shown in Figure 1-2

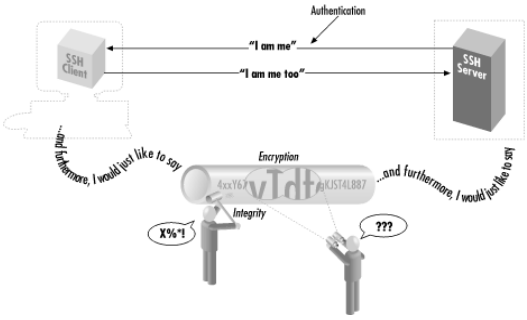

Figure1-2. Authentication, encryption, and integrity

SSH makes network connections

between computers, with strong guarantees that the parties on both ends of the connection are genuine. It also ensures that any data passing over these connections arrives unmodified and unread by eavesdroppers. [10]

2. PGP Program:

PGP "Pretty Good Privacy" is a powerful, free cryptography package. PGP lets people exchange files in a private, encrypted format, and also provides message authentication.
PGP is called a public key system. Each person using PGP has two keys, a public and a private key. [14]

Philip R. Zimmermann is the creator of PGP, an email encryption software package. PGP was published for free on the Internet in 1991.

This made Zimmermann the target of a three-year criminal investigation, because the government held that US export restrictions for cryptographic software were violated when PGP spread worldwide. [8]

PGP offers several features and utilities :

* Encrypt/sign and decrypt/verify within any application.
With the PGP menus and email plug-ins, you can access PGP functions while in any application.

* Create and manage keys. Use PGPkeys to create, view, and maintain your own PGP key pair as well as any public keys of other users that you have added to your public keyring.

* Create self-decrypting archives (SDAs).
You can create self-decrypting executable files that anyone can decrypt with the proper password. This feature is especially convenient for sending encrypted files to people who do not have PGP installed.

* Permanently erase files, folders, and free disk space.
You can use the PGP Wipe utility to thoroughly delete your sensitive files and folders without leaving fragments of their data behind.

You can also use PGP Free Space Wiper to erase the free disk space on your hard drive that contains data from previously deleted files and programs.
Both utilities ensure that your deleted data is unrecoverable.
* Secure network traffic.
You can use PGPnet, a Virtual Private Network (VPN), to communicate securely and economically with other PGPnet users over the internet. [7]

When we need PGP?

- Distribute new passwords.
- Encrypt your personal password store.
- Directives with sensitive data.
- Credit card numbers.
- Personal messages having to go through untrusted 3rd parties.

How PGP works ?

PGP combines some of the best features of both conventional and public key cryptography. PGP is a hybrid cryptosystem. When a user encrypts plaintext with PGP, PGP first compresses the plaintext. Data compression saves modem transmission time and disk space and, more importantly, strengthens cryptographic security. Most cryptanalysis techniques exploit patterns found in the plaintext to

crack the cipher. Compression reduces these patterns in the plaintext, thereby greatly enhancing resistance to cryptanalysis.

PGP then creates a session key, which is a one-time-only secret key. This key is a random number generated from the random movements of your mouse and the keystrokes you type. This session key works with a very secure, fast conventional encryption algorithm to encrypt the plaintext; the result is ciphertext. Once the data is encrypted, the session key is then encrypted to the recipient's public key. This public key-encrypted session key is transmitted along with the ciphertext to the recipient. [13]

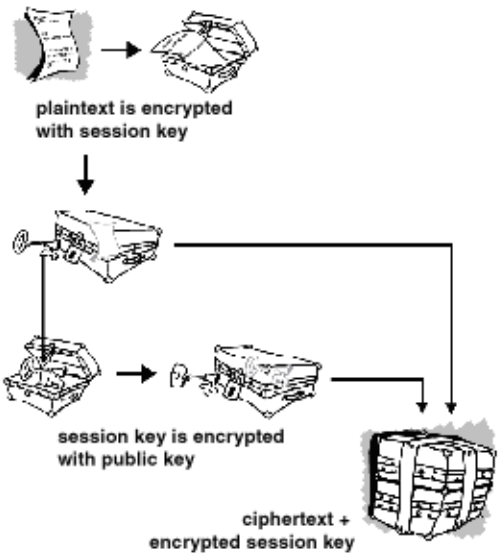

Figure 2-1. How PGP encryption works

Decryption works in the reverse. The recipient's copy of PGP uses his or her private key to recover the temporary session key, which PGP then uses to decrypt the conventionally-encrypted ciphertext.

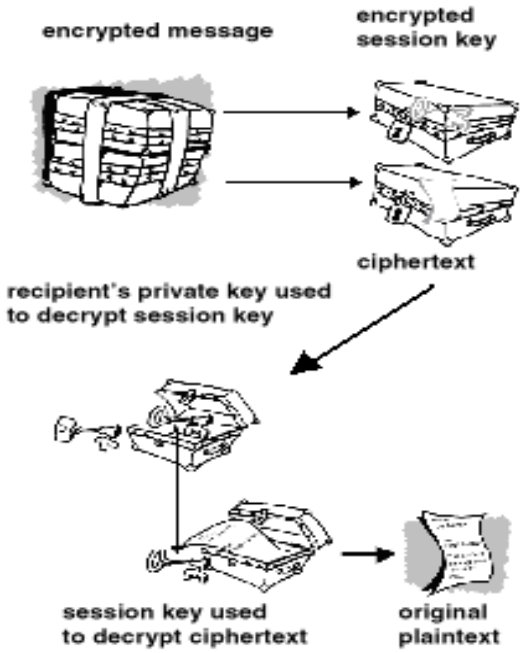

Figure 2-2. How PGP decryption works

The combination of the two encryption methods combines the convenience of public key encryption with the speed of conventional encryption. Conventional encryption is about 1, 000 times faster than public key encryption. Public key encryption in turn provides a solution to key distribution and data transmission issues. Used together, performance and key distribution are improved without any sacrifice in security. [13]

3. Comparisons

3.1 SSH protocol.

- Running on Unix, Sun OS, Mac OS Linux, Microsoft Windows.
- Open Source code.
- The SSH Version 2 can run with PGP.
- SSH use for Provides secure encryption communication between two hosts over an insecure network. Remote login. Executing command. Connect to

Remote computer without password. Replace telnet, rsn, rcp.

- SSH base on RSA algorithm.
- Last version of SSH is 3.2.9.
- SSH program is shareware.
- SSH is legal in US and Canada.
- SSH Support for:
    - Host and user authentication.
    - Data Compression.
    - Data Confidentiality.
    - Integrity protection.
    - Encryption.
- SSH is a Protocol.
- SSH is a Program.

3.2 PGP protocol.

- Running on Unix, OS/2, Mac OS , DOS, Microsoft Windows.
- Open Source code.
- The PGP can run with SSH Version 2 .
- PGP use for email, File, Disk, Network traffic.
- PGP base on RSA, IDEA, MD5 algorithm.
- Last version of PGP is 8.0 for Windows and Mac OS, and version 5.0i For other O.S.
- PGP program is Free.
- PGP is not legal in US and Canada.
- PGP Support for:
    - User authentication.
    - Data Compression.
    - Integrity protection.
    - Encryption.
- PGP is a Program.

Conclusion

The SSH protocol/ program has more secure ,useful, powerful usage. SSH protocol uses port 22. SSH encryption all traffic (Include password). SSH Provides us with similar services like SSL:

-Mutual authentication

-Encrypted sessions between two endpoints.

Any application running on top of TCP can be secured by SSH.

The PGP program as part of any security structure. It is very secure against eavesdroppers . It is uses faster encryption algorithm to encrypt the message. It is automatically divides long message. It is Available worldwide for different platforms. It is Wide range of applicability. It is not developed or controlled by government standards.

References

[1]www.pgp.com/products/commandline/mainframes/faqs.html

[2]http://tldp.org/linuxfocus/English/Archives/lf-2003_01-0278.pdf

[3]www.unix.org.ua/orelly/networking_2ndEd/ssh/index.htm

[4]www.unix.org.ua/orelly/networking_2ndEd/ssh/index.htm

[5]www.tacc.utexas.edu/resources/userguides/ssh_detailed

[6]www.phildev.net/pgp/pgp-020206.pdf

[7]www.cs.sunysb.edu/files/pgp/PGP65WinUsersGuide.pdf

[8] www.philzimmermann.com

[9]www.acad.bg/beginner/gnrt/security/pgp.html

[10]www.oreilly.com/catalog/kerberos/chapter/ch01.pdf

[11] http://old.cpsc.ucalgary.ca/

[12] http://www.boran.com/security/sp/ssh-part1.html

[13] http://www.pgpi.org/doc/

[14] http://kb.iu.edu/index.cgi