Security Features of Sena Products

Technical Tutorial

2002 – 12 - 06

Table of Contents

1. Introduction

Today most network traffic for both the Internet and corporate intranets is based on TCP/IP. However, the original Internet Protocol (IP) failed to define any structures for security, so application layer implementations, such as Secure Sockets Layer (SSL) and Secure HyperText Transfer Protocol (S-HTTP) have been used to provide data security over the Internet. This document gives technical readers a basic overview of Security protocols such as 3DES, SSL, Firewall, Kerberos, SSH, RADIUS, TACACS+, LDAP.

2. 3DES

DES is a NIST-standard secret key cryptography method that uses a 56-bit key. DES is based on an IBM algorithm, which was further developed by the U.S. National Security Agency. It uses the block cipher method, which breaks the text into 64-bit blocks before encrypting them. There are several DES encryption modes.

DES decryption is very fast and widely used. The secret key may be kept a total secret and used over again. Or, a key can be randomly generated for each session, in which case the new key is transmitted to the recipient using a public key cryptography method such as RSA.

Triple-DES is a much stronger algorithm than DES. It uses a double length key (112 bits) and does three DES operations, one after each other. In other words, Triple-DES is 256 times stronger than DES. Put another way, if you could crack a DES key by brute force in 1 second, it would still take two billion years to crack a Triple-DES key in the same way.
But it requires multiple passes and takes more time.

3. SSL

Secure Sockets Layer is a protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL connection. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with https: instead of http:.

4. Firewall

A system designed to prevent unauthorized access to or from a private network. Basically, a firewall, working closely with a router program, examines each network packet to determine whether to forward it toward its destination.

Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. A firewall is a set of related programs, located at a network gateway server that protects the resources of a private network from users from other networks.

There are several types of firewall techniques:

4.1. Packet filter: Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.

4.2. Application gateway: Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose a performance degradation.

4.3. Circuit-level gateway: Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.

4.4. Proxy server: Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

5. Kerberos

Kerberos is designed to enable two parties to exchange private information across an otherwise open network. It works by assigning a unique key, called a ticket, to each user that logs on to the network. The ticket is then embedded in messages to identify the sender of the message.

Kerberos is a secure method for authenticating a request for a service in a computer network.

Briefly and approximately, here's how Kerberos works:

5.1. Suppose you want to access a server on another computer (which you may get to by sending a Telnet or similar login request). You know that this server requires a Kerberos "ticket" before it will honor your request.

5.2. To get your ticket, you first request authentication from the Authentication Server (AS). The Authentication Server creates a "session key" (which is also an encryption key) basing it on your password (which it can get from your user name) and a random value that represents the requested service. The session key is effectively a "ticket-granting ticket."

5.3. You next send your ticket-granting ticket to a ticket-granting server (TGS). The TGS may be physically the same server as the Authentication Server, but it's now performing a different service. The TGS returns the ticket that can be sent to the server for the requested service.

5.4. The service either rejects the ticket or accepts it and performs the service.

5.5. Because the ticket you received from the TGS is time-stamped, it allows you to make additional requests using the same ticket within a certain time period (typically, eight hours) without having to be re-authenticated. Making the ticket valid for a limited time period make it less likely that someone else will be able to use it later.

6. SSH

Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels.

Secure Shell (SSH), sometimes known as Secure Socket Shell, is a UNIX-based command interface and protocol for securely getting access to a remote computer. It is widely used by network administrators to control Web and other kinds of servers remotely.

SSH (Secure Shell) is a popular, robust, TCP/IP-based product for network security and privacy, supporting strong encryption and authentication.

7. RADIUS

Short for Remote Authentication Dial-In User Service, an authentication and accounting system used by many Internet Service Providers (ISPs). When you dial in to the ISP you must enter your username and password. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access to the ISP system.

RADIUS (Remote Authentication Dial-In User Service) is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share.

8. TACACS+

TACACS (Terminal Access Controller Access Control System) is an authentication protocol that was commonly used in UNIX networks. TACACS allows a remote access server to communicate with an authentication server in order to determine if the user has access to the network.

In spite of its name, TACACS+ is an entirely new protocol. TACACS+ and RADIUS have generally replaced the earlier protocols in more recently built or updated networks. TACACS+ uses the Transmission Control Protocol (TCP) and RADIUS uses the User Datagram Protocol (UDP).

9. LDAP

Lightweight Directory Access Protocol is a protocol used to access a directory listing. LDAP support is being implemented in Web browsers and e-mail programs, which can query an LDAP-compliant directory. It is expected that LDAP will provide a common method for searching e-mail addresses on the Internet

An LDAP directory is organized in a simple "tree" hierarchy consisting of the following levels:

- The root directory (the starting place or the source of the tree), which branches out to
- Countries, each of which branches out to
- Organizations, which branch out to
- Organizational units (divisions, departments, and so forth), which branches out to (includes an entry for)
- Individuals (which includes people, files, and shared resources such as printers)

10. Security features supported by Sena Products

Below table shows the list of security features supported by the Sena Products.

10.1. Security features supported by HelloDevice Lite Series

Specification	HelloDevice Lite Series
Security Features	User ID & Password

10.2. Security features supported by HelloDevice Pro Series

Specification	HelloDevice Pro Series
Security Features	3DES IP filtering User ID & Password

10.3. Security features supported by HelloDevice Super Series

Specification	HelloDevice Super Series
Security Features	SSL IP filtering User ID & Password

10.4. Security features supported by IALink100

Specification	IALink100
Security Features	3DES IP filtering User ID & Password

10.5. Security features supported by IALink100-MODBUS

Specification	IALink100-MODBUS
Security Features	User ID & Password

10.6. Security features supported by POSLink

Specification	POSLink
Security Features	SSL User ID & Password

10.7. Security features supported by UPSLink

Specification	UPSLink
Security Features	IP filtering User ID & Password

10.8. Security features supported by VTS

Specification	VTS
Security Features	SSH IP filtering Kerberos RADIUS TACACS+ LDAP