Global Information Assurance Certification Paper

Alejandro Bravo
Abravo@oas.org
W 202-458-6162
H 301-263-0391
5703 Wilson Lane
Bethesda, MD 20817

Secure Servers with SSL in the World Wide Web

Introduction

The Internet is one of the most current and largest sources of data-sharing information. The web offers multimedia capabilities along with hypertext to make it easy for anybody to browse, wander over and participate. Navigators such as Internet Explorer, Netscape and others give the inexperienced Internet user access to information with seemingly effortless work; however, they bring some security concerns. The protocol used by the Internet components (servers, client and proxies, etc.) of the web is the Hyper Text Transfer Protocol (HTTP) which has little or no security features. The much-criticized traditional HTTP protocol has served as a channel for the development of new security server protocols, methodologies, approaches, techniques and tools. Security protocols have been developed to resolve the problems caused by client software, access control, authentication, confidentiality and integrity issues.

Security Issues

This paper will examine security issues that need to be resolved to provide maximum security for Internet sites and web users. These concerns can be divided into three categories: the threat that client software poses to the local computer environment, the threat of access control to Internet servers and robustness of authentication, confidentiality and integrity issues.

Clients who without regard or discretion download software from various web sites on the Internet are one of the biggest threats to computer security. The software may not safely verify or interpret data. It may contain viruses such as "Trojan horses" which can take several forms of malicious URLs or rogue code executed through interpreters such as postscripts in the client workstation or the Java VM. If the contents of the software are not properly screened, there is the potential for this data to corrupt the programs that reside on the client system.

Modification of server data is one of the threats to a server. Unauthorized users with access to a server could modify, corrupt or delete data stored in the server. Inefficient authentication mechanisms and access control or the total absence of these security features could allow easy access the server information by unauthorized users. Also, bugs in the server software could compromise the system by creating an access point for unauthorized users.

Point-to-point security threats depend on client and server features to protect and provide a secure transmission. Today Internet architecture enables businesses and clients to conduct commerce transactions via the web. Clients will provide sensitive information such as credit card numbers, personal information and account information via insecure communication. The threats of performing web transactions through the Internet can be summarize as information disclosure, information tempering, information destruction and denial of services. Some of the associated risks with these threats are financial, life threatening and reputation. A solution to these issues is to provide a mechanism for privacy, authentication, integrity and non-repudiation.

Most organizations today are protected by an Internet firewall which implements security policies based on the network services permitted within the organization. URL's support several resource types such as file, FTP, HTTP, NNTP, TELNET, RLOGIN, etc. Most firewalls will permit the implementation of only a subset of these resources. However, web servers provide these services independent from the normal mechanism, such as the normal FTP channels. Therefore, it is possible to bypass the security firewall policy by using the services offered by the web.

This paper will examine a proposed scheme provided by Netscape. Netscape has proposed a protocol called SSL or Secure Socket Layer, which is built to offer private and authentication communications. This new, state-of-the-art technology addresses and provides a solution for most of the problems that make running a web site a dangerous proposition for various organizations.

Netscape developed a protocol called **SSL** (Secure Socket Layer), a secure protocol that provides means for authentication and a private communications. SSL is not a modification to HTTP, but is a lower level protocol used to provide security for HTTP, FTP and TELNET by including a layer of security between TCP and these protocols. **RSA** is an asymmetric cryptography algorithm and it is the base encryption algorithm for authentication of SSL protocol. This protocol is implemented in Netscape browser and the e-commerce server[1]. The protocol allows users to transfer financial data such as credit card and personal information from a Netscape or Internet Explorer browser to the Netsite server in a secure manner. Some of the financial organizations using SSL to provide real-time, online credit card authorization include Bank of America, First Data Card Services, Electronic Funds Services (EFS) and MCI, which provides a secure online shopping mall.

Definition Overview

Secure Socket Layer (SSL)

Netscape Communications' Secure Sockets Layer (SSL) is an open, nonproprietary protocol. SSL security protocol is designed to provide privacy over the Internet through the authentication of the server and, optionally, the client. SSL has been presented to the W3C (World Wide Web Consortium) to be evaluated as a standard security protocol for web browsers and servers on the Internet. It is designed to layer beneath applications' protocols such as HTTP, SMTP, Telnet, FTP and NNTP. Netscape is now closely working with W3C, including members of EIT. The

group's main goals are to develop and standardize a common, robust security mechanism and protocols in the Internet.[2] The main objective of the SSL protocol is to provide privacy via a key exchange encryption algorithm such us Deffie-Hellman and KEA. The SSL protocol allows authentication through the use of certificates issued by a third party (normally in compliance to the X.509 standards). Integrity is achieved by calculating the hash function of the MAC (Message Authentication Code). Finally, non-repudiation is achieved by utilizing a unique token via the support of the Fortezza, SHA and DSS algorithms[3].

This is a brief description of Version 3.0 of the SSL protocol that provides privacy over the Internet. The protocol will provide the client/server applications for communicating in a safe way. It will restrict intrusion and eavesdropping from other users. SSL is designed to be portable with no major restriction or specification about the underlying environment. SSL Version 3 protocol is fully backward compared with Version 2; however, it adds three important capabilities:

- Support for alternative key-exchange algorithm, including Diffie-Hellman and KEA.
- Support for hardware "tokens" — a device that allows discovery of the symmetric encryption key.
- Support for SHA, DSS and Fortezza.

The main advantage of the SSL protocol is that it is protocol independent of any application. Application protocols such as HTTP, FTP, TELNET, etc. can layer on top of the SSL Protocol seamlessly. The SSL Protocol can both negotiate an encryption session key and authenticate a server before an application protocol can transmit or receive a byte of data. Every application protocol data is encrypted before being transmitted to provide privacy.

The SSL protocol is formed of two distinct protocols that are the *SSL Record Protocol* and *SSL Handshake Protocol*. The SSL Record Protocol resides at the lowest level layered on top of some reliable transport protocol and is used for encapsulation of all transmitted and received data including the Handshake Protocol. The SSL Handshake Protocol's main task is to establish security parameters[4].

Analysis of SSL

The SSL protocol provides an additional layer for the implementation of encryption between the application and the TCP/IP connection layers in the network protocol stack. SSL is a protocol that layers security beneath application protocols such as HTTP, NNTP and Telnet. SSL allows for server and optionally client authentication. One of the most important advantages of this protocol is mixing the better of two different encryption key techniques, symmetric and asymmetric encryption algorithms. "The advantage of symmetric encryption is efficiency – it is easier for the computer to decrypt using a symmetric key. The disadvantage is security – you have to pass the symmetric key around, and sometimes it gets lost. The advantage of an asymmetric algorithm, or public key, encryption is security – you do not have to pass around a

private key and risk the loss of the key. The disadvantage is efficiency – it takes a lot of computing power to decrypt asymmetrically encrypted message."[5]

Conclusion

There is much more that needs to be resolved before any security communication approach is sufficiently secure. Information transmitted throughout the Internet is susceptible to fraud and misuse by other parties. Information that travels from a client work station and servers uses a routing process where information is passed over many computer systems. Each computer system represents a potential threat to access the flow of information between the client and server. Unfortunately the Internet does not provide a built-in security system that will prevent intermediaries from deceiving you, eavesdropping, copying from, damaging the communication, etc. Most organizations face these security concerns. Efforts from SSL protocol to solve some of the security issues in the WWW have contributed to increased security on the Internet. However, incident such as Netscape's security flaw highlights issues revolving the security in the Internet in general. There are also several misconceptions that need to be cleared. Most Internet users believe that security is either *on* or *off*. Security in general is a system that needs to be continually refined and tested. This is a mechanism that carries a high cost and complexity; however, it adds value and benefit. Netscape's flaws simply underline that the security technology is not a perfect but an incremental process with a wide range of security categories. Security systems are not perfect and destined to have week point or flaws that are resolved by the interactive process of users and hackers. The more people stress and test the level of security of the SSL protocol, the better. This research shows that the utilization of SSL greatly contributes to system success as well as user satisfaction. Their ability to provide faster responses to the changing environment enhanced the attractiveness for security engineering.

---

[1] Netscape, "How SSL Works", 1
http://developer.netscape.com/tech/security/ssl/howitworks.html

[2] http://webopedia.internet.com/TERM/S/Secure_Socket_Layer.html

[3] Brian Lashley and Tarski, "SSL", 1-2
http://www.cs.umu.se/~tdv94ati/ssl/ssl.html

[4] Alan O. Freier, Netscape Communications, Philip Karlton, Netscape Communications, Paul C. Kocher, Independent Consultant , "The SSL protocol",
http://home.netscape.com/eng/ssl3/ssl-toc.html

[5] See Lawrence Lessig, *CODE and other laws of cyberspace, 39-40.*

Alejandro Bravo
Abravo@oas.org
W 202-458-6162
H 301-263-0391
5703 Wilson Lane
Bethesda, MD 20817

True and False Questions

1. The SSL (Secure Socket Layer) protocol is an application layer protocol. (T or F) Answer is: F
2. Netscape and Internet Explorer provide support for the SSL protocol. (T or F) Answer is: T
3. One of the most important advantages of the SSL protocol is mixing the better of two encryption key techniques symmetric and asymmetric algorithms. (T or F) Answer is: T
4. The SSL protocol only uses symmetric key algorithms. (T or F) Answer is: F
5. The HTTP protocol is considered a secure communication protocol. (T or F) Answer is: F

Multiple Choice Questions

1. Which of the following protocols is not an application layer protocol.

a. HTTP
b. FTP
c. TELNET
d. SSL
The answer is (d).

2. Which of the following is a security threat of performing web e-commerce transactions:

a. Information disclosure
b. Information tempering
c. Information destruction
d. Denial of services
e. All of the above
The answer is (e).

3. Which of the following choices is not an associated risk with an insecure Internet communication?

a. Financial Risk
b. Life threatening
c. SPAM mail
d. Reputation
The answer is (c).

4. Which of the following protocols is not supported by SSL.

a. HTTP
b. FTP
c. TELNET
d. NNTP
e. Non of the above.
The answer is (e)

5. Which of the following is not a feature of the SSL protocol.

a. Privacy, Authentication
b. Encryption
c. Integrity
d. Non-repudiation
e. Control over the distribution of personal information when visiting a web site.

The answer is (e).

Last Updated: July 28th, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event