Global Information Assurance Certification Paper

"How to Secure Your Website for E-commerce using (SSL) Secure Sockets Technology,"
Ervin Daniels
February 17, 2003
GSEC Practical: Option 1 – Research on Topics in Information Security (v.1.4b)

Introduction

E-commerce stands for Electronic Commerce. E-commerce is the buying and selling of products and services over the internet. The emergence of the internet has changed the way of conducting business. E-security has become one of the biggest issues with businesses. There are several challenges that E-commerce businesses must deal with such as customer trust, security issues, internet threats and ways of reducing many risks. After addressing those challenges, implementing a security infrastructure using (SSL) Secure Socket Layer technology can help resolve those issues.

Businesses must address the customer trust issue by making the customers feel comfortable with submitting there credit card information or making financial transactions on there web sites over the internet. In order for the E-commerce business to succeed, they must take advantage of the very competitive marketplace and use the current technology to protect there customers. The merchants who can build confidence of the customers will gain their loyalty and enormous opportunity for expanding the market share.

Security issues are very important. It's difficult to provide safety over the internet because you can't physically protect your website from threats. E-commerce sites that become aware of the risks from the Internet –based transactions can acquire technology solutions that overcome those risks. E-commerce is vulnerable to Cyber crimes. Hackers can cause damage to an e-commerce business. Hackers can gain unauthorized access to your web site. Hackers can duplicate, steel, alter and erase sensitive financial data. Database servers that hold credit card information are susceptible to hackers. However, the programs that hackers use to access sites are created by humans, therefore those tools have flaws. It takes skilled knowledge about how to use them to keep hackers at bay oddly enough, but the most skilled security gurus are former participants of cyber crimes.

Internet security threats are performed in several ways. The following tactics are Spoofing, Unauthorized disclosure, Unauthorized action, eavesdropping and Data altercation. Spoofing is performed when hackers can easily duplicate legitimate websites. Hackers can create a site that's identical, feels and operates like a well known site. This is an easy trap for vulnerable on-line shoppers to fall into which allows hackers to obtain credit card information. Secondly, another tactic is unauthorized disclosure. This tactic is performed when a hacker intercepts the data when it's transmitted from one's computer through the internet

to the E-commerce server. Unauthorized action is a tactic that is performed when a competitor or disgruntled customer can alter a web site so that it refuses service to potential clients or causing the website to malfunction. Eavesdropping is when unprotected private data is intercepted en route over the internet. Data Alteration is when unprotected and private data is intercepted and also altered intentionally or inadvertently. Financial sensitive data such as credit card numbers that are sent in the clear are the most vulnerable to data alteration.

Given the issues surrounding E-commerce security, it must be imperative that E-commerce businesses implement an E-commerce security infrastructure to avoid the risks of on-line transactions. Companies should address the confidence of on-line customers and answer the problems of about privacy and security. The goals of implementing a secure infrastructure should be authentication, confidentiality, data integrity and non-repudiation. Authentication security must allow customers to ensure that they're exchanging private information with a real on-line business and not a spoof site pretending to be a legitimate e-commerce business. Confidentiality must be enforced to ensure that during internet transactions, financial and credit card information must be kept private and secure. Also, Data integrity must in placement to protect undetectable alteration by hackers during transmission on the internet. It should not be possible for a sender to reasonably claim that her or she did not send a secured communication or did not make an online purchase. This is called nonrepudiation.

Implementing a complete E-commerce security infrastructure is the solution for your E-commerce web site. Applying PKI cryptography and digital signature technology via Secure Sockets Layer (SSL) digital certificates can provide authentication, data integrity and privacy necessary for E-commerce. The process is implemented by installing SSL certificates on your E-commerce web server.

How to Build a Secure Infrastructure using SSL Technology

Secure Sockets Layer (SSL) technology is the industry standard method for protecting web communications developed by Netscape Communications Corporation. The SSL security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection. Because SSL is built into all major browsers and web servers, simply installing a digital certificate turns on their SSL capabilities.

Installing Digital Certificates on your web servers and implementing an online payment system are the two essential components for a secure infrastructure. Digital certificates for Web servers provide authentication, data integrity and privacy through encryption. Also, implementing a secure online payment system will allow your e-commerce website to process payments online. However this paper is not to focus on the payment system.

Cryptographic Systems: Symmetric or Asymmetric

SSL is made up of a cryptographic system that includes symmetric and asymmetric (PKI) or Public Key Cryptography, the system underlying (SSL). The following section presents an overview and background technical information on cryptographic system.

Secure Sockets Layer (SSL) is based upon two cryptography systems. The two systems are symmetric and asymmetric (Public Key) cryptography. Cryptography is the science that includes encryption which is the transformation of information or data (plaintext) into a form (cipher text) that conceals the original meaning to prevent it from being known or used to all but the intended.

Symmetric cryptography or commonly known as ("Secret-key cryptography") is when two parties communicate secretly over the internet by using an algorithm that uses the same key to encrypt and decrypt data. With symmetric cryptography, the two parties first have to agree in advance on a single secret key before communicating. However, Symmetric cryptography has some drawbacks because it requires both parties to trust each other based on a shared secret. In modern day Cryptography systems, symmetric is hardly used as a means of agreeing upon the necessary secrets to begin communicating because it causes a key management problem. The problem with key management will be explained later.

Currently, Asymmetric or "Public-Key" cryptography systems have been used more often because of its improved technology. Asymmetric allows two parties to exchange secured information in case of eavesdroppers, without previously agreeing on a "shared-secret." This is no longer a simple shared secret used by symmetric cryptography; instead it uses two sub keys, the private key and the public key.

When an asymmetric cryptography system is being used, the person who wishes to receive encrypted information must generate a private and public keys, or key pair. The private key is to be kept as a secret and the public key is the publishing key that goes out to the internet so that all parties that would like to encrypt data for that participant is available. The public key encrypts the data and the private key decrypts the same message. This is the reason why this is better than symmetric cryptography because it resolves the complexity in the key management problem since no share secret has to be exchanged.

Many of today's cryptography systems use the hybrid approach. Hybrid systems simultaneously use both the asymmetric "Public Key" and the traditional symmetric cryptography. However, the asymmetric key has a more complex mathematical algorithm, but the symmetric key is much faster for encrypting huge data. Therefore, asymmetric is used first to solve the key distribution problem first, and then the symmetric key cryptography is used for speed of data flow.

The key management for both asymmetric and symmetric has its problems and raises questions about the overall confidence in the confidentiality features of the system. However, the techniques of both asymmetric and symmetric are sufficient in handling the privacy and security features of the system, but how can we be so sure? Web browsers of today use the public key of the web sites in order to send financial information such credit card numbers over the web and one protect access to files and data using a private symmetric key to scramble the information before it's saved. Therefore, this problem requires a certified public key in order to function correctly without third parties being able to interfere which causes two more questions. How can we ensure that the public key that your browser uses to send credit card information is in fact the correct one for that web site, and not a bogus one? Secondly, how can you reliably communicate your public keys to your correspondents so that they can rely on it to send you encrypted communications? The answer is the combination of digital signatures and X.509 digital certificates (which employ digital signatures), including SSL certificates.

Digital Signatures

Digital Signatures is an asymmetric cryptographic algorithm that produces a digital signature in the form of a pair of large numbers. The signature is computed using rules and parameters such that the identity of the signer and the integrity of the singed can be verified. Digital signatures are based upon data hashing with public key based encryption. Hashing is done by grabbing a block of data at a time and repeatedly using simple scrambling algorithm to modify the bits. If the scrambling is done repeatedly, the there is no known practical way to predict the outcome. The digital signature process is part of the process for a digital certificate, therefore digital certificates is the primary tool to ensure E-commerce security.

The following diagram illustrates the Digital signature process.

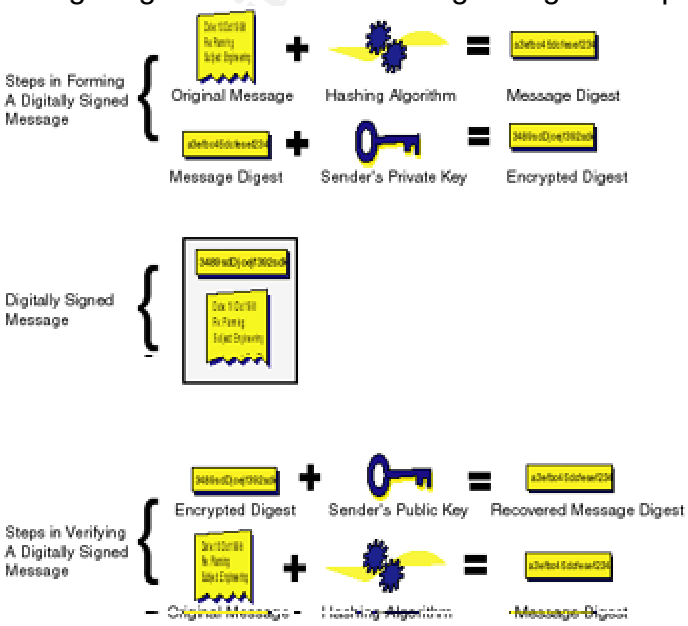

Figure1: Steps in forming and verifying a digitally signed message

http://www.verisign.com/resources/gd/buildEcommerce/index.html

Sending Outgoing Message

1. The first step is to take the original message and compute a "digest" of the outgoing message using a hashing algorithm. The result is a "message digest." At this point you have the original message in tact along with digest.
2. The sender uses his private key to encrypt the outgoing message digest
3. The original message + encrypted message digest = digitally signed message. Now, it's ready to be delivered to the recipient.

Receiving Incoming Message

4. The recipient receives and verifies the digitally signed message using the inverse set of steps by decrypting the encrypted message digest using the sender's public key.
5. The results of the decrypted message digest are compared to an independent computation of the message digest value using the hashing algorithm. If the two values are the same, the message has been successfully verified.

How do you know that the digital signature was signed by the original sender? If a third-party had intercepted and the original message had been changed it, then no need to be worried. If so, the decrypted original message digest would not match the recomputed one for the changed data in the message (see step 5). Therefore, the verification of the digital signature would fail. No hacker can create a fake signature because the hacker would not have the appropriate private key.

Digital Certificates

Digital certificate is an electronic identification card that establishes your credentials for individuals when doing business or other transactions on the web. The digital certificates are issued by a trusted third-party called a Certificate Authority (CA). In this case VeriSign is one of the most popular CA's. The certificate authority issues, creates and sign certificates. The electronic identification card contains your name, expiration dates, serial number and a copy of the certificates holder's public key. Also, digital certificates contain the digital signature of the CA so that the recipient can verify that certificate is legitimate.

Digital certificates are very important to web cryptography systems. When you access a secure E-commerce website and you are ready to make a financial transaction with your credit card, your browser client has already been issued a public key from the secure e-commerce site. This process is transparent to the

user and it's browser during the secure connection. The digital certificate is the X.509 form. The browser trusts the certificate because it is signed by a digital signature, and the browser trusts the signature because the signature can be verified because the (CA) or signer's public key has been embedded in the browser. To confirm that your browser has the embedded public key by a Certificate Authority issuer depends on what browser and it's version. The two most dominate browser's are Netscape and Internet Explorer. The following steps will show how to check your browser's settings.

For Netscape versions 4.05 or later please follow these steps:

1. Click on the security icon from the main toolbar
2. Select Certificates and Signers
3. Select the certificate and click the Edit button

For Internet Explorer 6.0 follow these steps:

1. Go to the exact website you want to check
2. Right click on the web sites' page
3. Select properties
4. Click the Certificates button

This is the most commonly known representation of an X.509 digital certificate in cryptography systems. However, X.509 digital certificates come in three different versions. This particular certificate identifies the owner of the certificate including the trusted Certificate Authority that issued the certificate. The certificate entails the version, serial number, signature algorithm ID, issuer name, validity period, subject (user) name, subject public-key information, issuer unique identifier (versions 2 and 3 only), subject unique identifier (versions 2 and 3 only), extension (version 3 only), digital signature for the above fields. A more detailed display of information can be viewed by dumping the raw certificate content which includes more detailed information about the certificate.

(SSL) Secure Socket Layer Server Certificates

SSL digital certificates for Web servers can provide security for e-commerce web sites under a cryptographic system. Implementing (PKI) Public Key Infrastructure and digital signatures via Web server certificates enable authentication and SSL encryption. SSL certificates allow e-commerce sites to offer safe and secure data transactions to their customers. SSL is the basic ingredient of an Internet trust infrastructure. SSL server can ensure non-repudiation, authentication, integrity and confidentiality.

SSL server authentication is very important for secure e-commerce transactions. Server certificates allow users to confirm a web server's identity. When internet users access a web site, the browser will check that e-commerce website for it's certificate and public ID that have been issued by a certificate authority, such as VeriSign.

Websites with SSL make sure that they create a secure channel for transaction between the user's web browser and the e-commerce web server. By doing this, the user's browser sends encrypted information while protecting against hackers, detecting tampering and data alteration in transit. This ensures that users confidently can send sensitive data over the web such as credit card information.

How SSL Server Certificates work

SSL certificates use SSL to effectively communicate between e-commerce sites and visitor's web browsers. SSL allows the storefront's server to authenticate itself to the user's browser and then permits the server and the browser to create symmetric keys used for encryption, decryption and tamper detection. When SSL is working, it goes through a series of steps to indicate that SSL certificates are working. The following process runs unnoticeable and there is no interaction between the user and the browser.

1. A visitor hits a website and the site indicates that it's secured by SSL if the URL begins with "https:" instead of "Http." Or, the browser may display a message.
2. The visitor's browser sends the server its SSL information which includes version number, cipher settings and other important information.
3. Automatically, the server responds and sends the visitor's browser the site's digital certificate including the server's SSL version number and other important information.
4. The visitor's browser carefully processes the information from server's certificate and verifies each of the following:
    a. Valid server certificate and date
    b. The CA that issued the server been signed by a trusted CA whose certificate is embedded into the browser.
    c. That the issuing CA's public key that's built into the browser validates the issuer's digital signature
    d. Domain name indicated by the server certificate is identical to the server's domain name. If authentication fails, the user is notified that an authenticated connection cannot be established.

5. If authentication fails, then the user is warned with a message that an authenticated and encrypted connection can be established. If the authentication is a success, the user's web browser builds a unique "session key" which is going to encrypt all communication between the site and the browser using asymmetric encryption.
6. The session key is encrypted by the browser with the site's public key. Therefore, the site can only read the key and sends it to the server.
7. The session key is decrypted by the server and it uses it own private key.
8. A message is sent by the browser to the server informing the server that any future message from the client will be encrypted with the session key.

9. At this point, an established SSL session uses the symmetric encryption to encrypt and decrypt message with the secured channel.
10. The session is terminated once the session is complete.

Security mechanisms are embedded in the Netscape Navigator and Microsoft Internet Explorer to help prevent users from carelessly submitting their personal financial information over a channel that is not secure. If a user tries to enter his personal data at an insecure site, or a site without a SSL server certificate the browsers will by default will display a message, "Any information you submit is insecure and can be observed by a third-party while in transit. If you are submitting passwords, credit card numbers, or any other information you would like to keep private, it would be safer to cancel the submission." On the other hand, if a user submits financial information at a secure site, no message will appear. However, here are some things a user can look for before submitting information on a website to insure security.

Steps to check

1. The URL starts with "https" instead of "http."
2. The padlock in the lower left corner of the Netscape Navigator Communicator will be closed and not open.
3. Internet Explorer will have a padlock icon in the bar at the bottom of the IE Window.

SSL 40-bit & 128-bit encryption

There are two kinds of encryption transactions using SSL which are measured by its strength. You have the 40-bit and 128-bit which refer to the length of the session key when generated by every encrypted transaction. The strength of the key is determined by the length of the key. The 128-bit is stronger that the 40-bit key. With today's technology, the 128-bit key is the world's strongest and it would be very difficult to break the encryption transaction, according to RSA labs.

Not only do you have two different levels of strength for SSL, but there are two different levels of encryption provided from each of the two browsers, Microsoft and Netscape. The different levels of encryption will depend on the type of SSL server certificate that the browser is communicating with.

The 40-bit SSL Server Certificates Encryption is enabled with its being used with the export version of Navigator Netscape or Microsoft Internet Explorer. The 40-bit SSL encryption can get stronger and be a 128-bit SSL when being used with the domestic version of both browsers. 128-Bit SSL Server Certificates enables the 128-Bit encryption with the export and domestic version with Microsoft Internet Explorer and Navigator Netscape browsers.
During the process of obtaining a SSL certificate, it's important to build the correct kind of private key. That process is generating a Certificate Signing Request from the server's web software. In order to obtain the CSR, web server

administrators carefully select a 1024-bit private key, which allows the Global Server ID to 128-bit encryption instead of a 512-bit private key, which enables only 40-bit encryption.

There are ways to check your level of encryption is protecting your transactions from a site that uses SSL certificates. Netscape users and Internet Explorer can check their browsers to indicate if the site uses SSL certificates. However, most E-commerce businesses may choose to have an automatic way for visitors to see if their site has been secured by providing a security and privacy statement or post a site seal on their home page. This depends from which Certificate Authorities company you have obtained your SSL certificates.

Vulnerabilities of SSL

Now that the technology of SSL has been explained, we know exactly how SSL is supposed to perform and protect the client and the server. Although, SSL is designed to prevent sensitive data of internet users from being intercepted by unintended third parties, there are vulnerabilities with SSL. Normally, when an SSL connection is established, the browser alerts the user that the connection is safe by displaying a secured padlock, or the browser alerts if the web server has the potential to be a malicious web site.

A padlock icon in the user's web browser may result in a false sense of security. Users will assume that the SSL connection is secure whereas it may not be safe because SSL is vulnerable to several attack vectors. It's easy for a virus, trojan, worm, malicious web site, malicious e-mail or any other attack vector to add a malicious SSL certificate to the victim's user's list of trusted root CAs.

A malicious SSL certificates could be injected to the user's list of trusted root CAs through several attach vectors such as including vulnerabilities and viruses. The malicious SSL certificates are more likely to attack when the browsers are exposed to vulnerabilities because that has not been properly patched. If an internet user's CA list is infected, this can betray to the users and redirect them to malicious web sites, or spoof sites. Researchers believe that vulnerabilities can be detected by certain anti-virus packages. A fast propagating virus could have a payload such as performing a certificate injection attach against infected users and redirecting them to a malicious server which proxies SSL requests. The certificate injection attacks can be restricted by software policies are by desktop hardening during the workstation builds.

Conclusion

E-commerce has become one of the biggest ways of doing business. Securing E-commerce sites has become so important that it's very important to properly protect your website against the evil of the internet. SSL continues to be the standard protocol for securing a connection between the client and the server.

Although, SSL is secure it can also be vulnerability. Attack vectors ranging from viruses to software can betray internet users by redirecting them to malicious sites rather that protecting them for unintended third parties. When using SSL technology make sure you've properly researched the technology and know the benefits and vunlerablities.

8 Sources

Nickels, G. William, James M. McHugh and Susan M. Mchugh. Understanding Business. The McGraw-Hill Companies, New York, NY: 2002. 12 – 15.

"Building and E-commerce Trust Infrastructure SSL Server Certificates and Online Payment Services."
URL: http://www.verisign.com/resources/gd/buildEcommerce/index.html

"Secure Sockets Layer." URL: http://wp.netscape.com/security/techbriefs/ssl.html

"How SSL Works."
URL: http://developer.netscape.com/tech/security/ssl/howitworks.html

"Securing Online Payments." SC Online Magazine. December 2002.
URL:
http://www.scmagazine.com/scmagazine/sc-online/2002/article/55/article.html

"E-commerce/Security: Frequently Asked Questions."
URL: http://www.html.com/faq/e-commerce-security.html#q1

"How Encryption Works."
URL: http://wp.netscape.com/security/basics/encryption.html

McLeod, Steven and Dr. Michael Cohen. "SSL Vulnerabilities."
http://www.dsd.gov.au/talks/Auscert2002.pdf

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event