White Paper

Spoofing Server-Server Communication: How You Can Prevent It

By Larry Seltzer
Security Analyst and Writer

Spoofing Server-Server Communication: How You Can Prevent It

CONTENTS

Executive Summary 3

Introduction 3

Weaknesses of SSL in Practice 4

SSLStrip – A New Type of Man-in-the-Middle Attack 4

EV SSL – The Antidote for SSLStrip Attacks 6

EV Certificates Enable Strong Authentication 7

Implementation Considerations 8

Call to Action 8

Conclusion 8

Appendix A 9

Appendix B 10

Appendix C 11

Executive Summary

Advances in attacks on network security over the last few years have led to many high-profile compromises of enterprise networks and breaches of data security. A new attack is threatening to expand the potential for attackers to compromise enterprise servers and the critical data on them. Solutions are available, and they will require action by company officers and administrators.

"SSLStrip" and related attacks[1] were among the highlights of the July 2009 Black Hat show in Las Vegas[2]. Researcher Moxie Marlinspike[3] combined a number of discrete problems, not all related to SSL, to create a credible scenario in which users attempting to work with secure websites were instead sent to malicious fake sites. One of the core problems described by Marlinspike is the ability to embed null characters in the common name field of a certificate, designating a domain name. This can be used to trick software, web browsers for example, into recognizing a domain name different from the complete field name. The result is that software, and users, are misled as to the actual domain with which they are communicating.

SSLStrip has not lacked for press coverage, but the analysis has focused on the consumer or end user with a browser. The use of SSL in embedded applications, including server-server communications, presents an even more ominous scenario. This is because SSLStrip attack could be used against server-server communications with the potential for mass-compromise of confidential data.

This spoofing problem is solved by proper use of Extended Validation (EV) SSL certificates for authentication. Moving certificate-based enterprise authentication to EV SSL would therefore protect an organization against this form of attack.

SSLStrip attack could be used against server-server communications with the potential for mass-compromise of confidential data.

Introduction

SSL authentication is most famous for providing secure web access to sites with sensitive information, such as banks, but it has many applications. It is commonly used, for example, as a means for parties in a machine-to-machine, typically server-server conversation to verify each other's identity; see Figure A for an illustration.

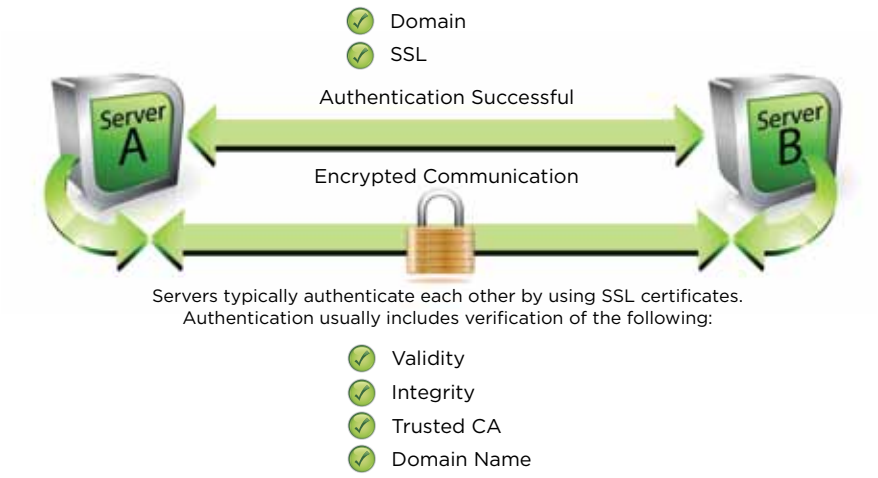
The recent revelation of a new attack against SSL threatens these server-server communications. An attacker who gains access to the network could use the attack to spoof the identity of a critical server and thereby gain unauthorized access to critical data.

Since EV SSL certificates contain only authenticated organization information, businesses can employ EV SSL and require the organization information to match the expected values before allowing access to mission critical applications. In this scenario the intruder using the new attacks will fail to gain access because it will lack the presence of the EV certificate, the correct organization information, or both.

[1] SSLStrip, description and code download. http://www.thoughtcrime.org/software/sslstrip/index.html
[2] Black Hat USA 2009, Welcome page - http://www.blackhat.com/html/bh-usa-09/bh-us-09-main.html
[3] Moxie Marlinspike, home page - http://www.thoughtcrime.org/

See Appendix A for an explanation of how SSL authentication works.

Figure A: Typical Server-Server Communication



Weaknesses of SSL in Practice

The main weakness with conventional SSL certificates is that there are no standards for their issuance, nor any rules for what the fields in them are supposed to mean and which are required for authentication.

One implication is that client applications, called relying parties, cannot have confidence that the organization listed as the owner of the certificate is in fact that owner. This follows all the way up the chain until the relying party reaches a trusted root.

In fact, the least expensive SSL certificates, domain-authenticated certificates, don't even authenticate an organization, merely an internet domain. Users can tell precious little from them about those with whom they are doing business.

SSLStrip – A New Type of Man-in-the-Middle Attack

Marlinspike's SSLStrip attack demonstrated the combination of several attack techniques to exploit the above weaknesses and fool users/client applications into thinking they were using a trusted site/server, when in fact they were using a fake version of that site/server. He combined a number of techniques, including "man-in-the-middle," fake leaf node certificates and the null character attack.

It is possible to trick the client into seeing the name it expects, when the actual domain name in the certificate is that of a malicious site.

Null characters in a domain name

The key threat Marlinspike discloses is the use of null (zero value, often designated '\0') characters embedded in a domain name.

Online purchase of inexpensive "domain-validated" SSL certificates is so automated that it's often possible to buy one with an embedded null character. For example - \0thoughtcrime.org. In the attack, the domain name of the certificate is

combined to the right of the domain name to be spoofed, for example, "www.symantec.com\0thoughtcrime.org". (Thoughtcrime.org is a domain owned by Marlinspike and used by him in his examples.)

Most software treats the null character as a string terminator. So when SSL client software reads the certificate domain name in the example it will stop at the null and treat the certificate as valid for www.symantec.com as issued by the Certificate Authority (CA).

For more detail on how this attack works see Appendix B.

Null-Stripping

Two SSL implementations, the Opera and Safari browsers, defeat this specific attack by stripping null characters from the Common Name. Thus, in the example above, the comparison will be to www.symantec.com.thoughtcrime.org and it will fail.

But Marlinspike claims that some CAs can be tricked with the same vulnerability in a way that makes null-stripping itself a vulnerability.

In his example, he buys a certificate for sitekey.ba\0nkofamerica.com. Presumably he owns nkofamerica.com. When this name is presented to Opera or Safari it will display his attack site as sitekey.bankofamerica.com, the login page for that bank.

Man-in-the-Middle

If you're on the same local network as the server you are compromising, Marlinspike's techniques make it very possible to perform the man-in-the-middle attack; see Figure B for an illustration. A number of popular techniques exist for this: A rogue wireless access point is one, or DNS or AARP cache poisoning.

If you're not on the same network then you need to get there, which you can do most likely by installing malware on a relatively less-secured system on the same network. The attacks which make this possible are legion.

Figure B: Man-In-The-Middle (MITM) Attack Using SSLStrip

SSLStrip attack demonstrated the combination of several attack techniques to exploit the weaknesses of authentication based on domain names in SSL certificates.
The attacker can fool users/client applications into thinking they were using a trusted site/server, when in fact they were using a fake version of that site/server.

Damage Potential in Server-Server Environments

The damage potential of this attack in a server-server communication scenario, such as database servers synchronizing across a WAN, is substantial.

Such servers commonly use SSL to authenticate each other. A malicious user on the network could spoof that authentication using the techniques described above. One that authenticated as a database mirror could capture the entire database including, if it's stored on the server, privileged information and confidential customer data.

EV SSL – The Antidote for SSLStrip Attacks

We saw that with conventional certificates, especially domain-validated certificates, there is no reliable information to back up the authentication of the domain name. To address this critical problem, CAs and software companies joined to form the CA/Browser Forum[4] and promulgate a new standard called EV SSL for Extended Validation SSL.

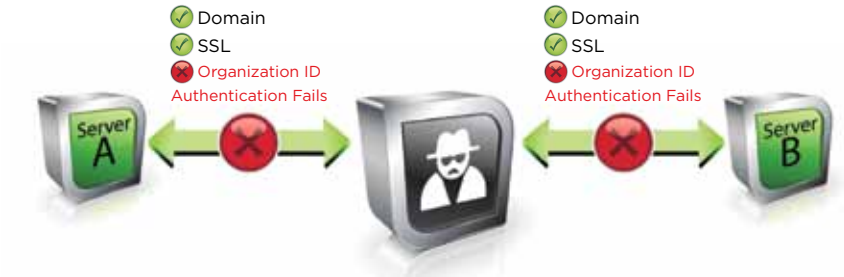
EV SSL allows software to authenticate strongly in ways which defeat the SSLStrip attack.

EV SSL defines rules for who can qualify for such a certificate and the procedures a CA must follow in order to validate the information supplied by an applicant[5]. For instance, they must validate that the organization exists as a legal entity, that any organization names are legal names for that organization, and that the applicant is authorized to apply for the certificate. For some details of the requirements of different types of organizations applying for an EV SSL certificate, see Appendix C.

EV SSL allows software to authenticate strongly in ways which defeat the SSLStrip attack.; see Figure C for an illustration The fields in the certificate generally ignored by conventional SSL implementations, such as organization name, are required in EV SSL and can be checked every time. This second-level of authentication ensures that the parties know exactly with whom they are communicating.

Since certificates contain organization names that have been verified, users and applications that rely on EV SSL certificates can verify the actual owner of the certificate with confidence.

Figure C: Usage of Extended Validation (EV) SSL Certificates Defeats SSLStrip Attack



EV SSL enables software to authenticate strongly in ways which defeat the SSLStrip attack. In addition to the domain name, the fields generally ignored by conventional SSL implementations, such as organization name, are required in EV SSL and can be checked reliably every time. This second-level of authentication ensures that the parties know exactly with whom they are communicating.

[4] CA/Browser Forum website - http://www.cabforum.org/index.html
[5] EV SSL Certificate Guidelines Version 1.1 - http://www.cabforum.org/EV_Certificate_Guidelines_V11.pdf

The specification is also clear about the information that must be provided by the applicant. Other rules are more restrictive than with conventional SSL. For instance, wildcard certificates, the type that make null character attacks even more dangerous, are not allowed in EV SSL.

EV certificates are also limited in lifetime relative to conventional certificates: the maximum validity period is 27 months. This ensures "freshness" of the information in the certificate.

In addition to collecting a proper EV certificate request, containing much organization information including the jurisdiction of incorporation, and a signed subscriber agreement, the CA is required to verify that the organization exists and operates at the locations specified in the request. They may go to government sources for this. They have to verify that the entity exists at the physical address they specify. For business organizations a face-to-face verification of the principal individual in the entity is required.

The requirements go on and on for 93 pages. It would be very hard to get a fake EV certificate.

EV Certificates Enable Strong Authentication

Standards also specify what software needs to do in order to authenticate a party based on a certificate. Unlike the loose conventions which developed around conventional SSL, these rules must be followed for EV.

The added costs of EV SSL and requisite software modifications are negligible compared to the potential damage.

When encountering an EV certificate, a program must confirm first that the CSP (Certificate Service Provider), meaning the CA who issued the EV certificate, is authorized to issue such certificates. Each CSP has a unique EV policy identifier associated with it which must be compared to the identifier in the end-entity certificate.

Applications that use EV certificates properly need to embed CSP root certificates in order to confirm that certificates they encounter are issued by trusted roots. Required procedures for CSPs to work with application developers, including providing test facilities, are defined by the CA/Browser Forum.

"Relying applications [clients authenticating certificates] must provide adequate protection against malign threats to the integrity of the application code and the CSP root." This is the sort of requirement that needs some history to fully-define itself, but basically it puts the onus on application developers to take care to write secure code.

The rules state that applications must be able to handle key strength of symmetric algorithms of at least 128 bits.

Applications are required to check for revocation of the certificate before accepting it. The application should support both CRL and OCSP, although OCSP is clearly the wave of the future and the only scalable approach. (In his presentation Marlinspike suggests a method for bypassing OCSP by returning a "Try again later" code, in

which case the application typically gives up and authenticates. The EV rules state: "If the application cannot obtain a response using one service, then it should try all available alternative services." This precludes the lazy behavior described by Marlinspike.)

Once all of these requirements have been met and the fields in the certificate match those expected by the application, then it may proceed.

Implementation Considerations

Adopting EV SSL is not simply a matter of buying and using an EV SSL certificate. Client software has to know to look for an EV SSL certificate and to follow the rules for implementing EV SSL authentication .

Fortunately, it's not difficult programming, but it needs to be done potentially with in-house as well as with 3rd party client software code. But the work is the same in all places. If you are well-organized about your certificates then it will be straightforward work. And many products, including current Windows versions, support EV SSL out of the box.

Call to Action

CIOs, CSOs and compliance officers need to consider the risk potential of exposing data at the server level to attackers through a generic SSL certificate that only cost them a few dollars. Such incidents can be ruinous to a company. The added costs of EV SSL and requisite software modifications are negligible compared to the potential damage.

Network administrators need to identify and document SSL uses in their networks where their use may be unobvious. Many enterprises don't have clear records of their uses of digital certificates, and these applications could represent serious vulnerabilities given the realities of these attacks. To address the issue, enterprises can leverage automated certificate discovery and management tools to bring all SSL certificates under management.

Independent software vendors need to adapt their programs to use EV SSL authentication where available. Vendors of libraries and open source implementations need to provide easy support for developers.

Conclusion

EV SSL is designed to fix a critical broken piece with SSL and the work shows its value in this instance. An attack which has broad application across a variety of implementations, even though it's an implementation error, is defeated by the design of EV SSL.

However, neither EV SSL nor any other particular security mechanism is a magic bullet, stopping any attack dead. Marlinspike's presentation is proof enough that security mechanisms frequently are imperfect, or at least imperfectly

[6] Guidelines for the Processing of EV certificates - http://www.cabforum.org/Guidelines_for_the_processing_of_EV_certificates%20v1_0.pdf

implemented. EV SSL is therefore properly considered as a defense-in-depth mechanism, reinforcing other techniques used in what is always a complex set of transactions.

It's a good example of how keeping systems secure often follows from modernizing implementations to newer versions of products and standards which implement the lessons learned from prior ones. Migrating secure applications to require more authentication information is a winning proposition for applications which need to be secure.

Appendix A

How SSL Authentication Works

Digital certificates are documents that combine a public key and an identity. You can use them to verify that the public key belongs to the group or individual that purports to hold them.

Certificates can be generated by freely available software and issued by anyone to anyone, but their real value in the marketplace comes when they are issued by a trusted authority. These are generally companies known as CAs, which are entrusted with verifying the identity information on the certificate. These companies sign the certificates, so that third parties can verify their authenticity. If the party trusts the authority and its verification procedures, they can trust the certificate itself.

Digital certificates viewed by a user also include information on the authority that issued them, because that is an important element of a trust decision. There is also a date range for which the certificate is valid, and the user agent will normally warn the user when a certificate is out of this range.

The most common use of digital certificates is in secure web browsing. When you surf to a website with an https:// link, your browser reads the certificate stored on the server and verifies that the certificate is valid, current, and signed by a trusted CA (browsers and other Internet software contain lists of "trusted roots," which are the public keys of trusted CAs). And since https encrypts the data transmitted by the web server, the browser uses the public key in the certificate to create session keys to decrypt that data, as well as to encrypt data sent back.

But SSL is not used only by browsers and websites. It is used widely in less-visible applications. SSL is popular as a protocol for VPNs (virtual private networks); it can be used to secure FTP file transfers and is used by numerous companies to

---

Larry Seltzer has been writing software for and English about computers ever since he graduated from the University of Pennsylvania in 1983. He was one of the authors of NPL and NPL-R, fourth-generation languages for microcomputers by the now-defunct Desktop Software Corporation. His work at Desktop Software included programming the UCSD p-System, a virtual machine-based operating system with portable binaries that pre-dated Java by more than 10 years. For several years, he wrote corporate software for Mathematica Policy Research and Chase Econometrics, before being forcibly thrown into the consulting market. He worked in the Philadelphia consulting and contract-programming scenes for a year or two before taking a job at NSTL (National Software Testing Labs) developing product tests and managing contract testing for the computer industry, governments and publication. In 1991 Larry moved to Massachusetts to become Technical Director of PC Week Labs (now eWeek Labs). He moved within Ziff Davis to New York in 1994 to run testing at Windows Sources. In 1995, he became Technical Director for Internet product testing at PC Magazine and stayed there till 1998. Since then, he has been writing for numerous other publications, including Fortune Small Business, Windows 2000 Magazine (now Windows IT Pro), ZDNet and Sam Whitmore's Media Survey. He is a Contributing Editor at PC Magazine where he writes the Security Watch blog. He is co-author of Linksys Networks: The Official Guide, author of ADMIN911: Windows 2000 Terminal Services.

secure proprietary protocols. In such cases the authentication mechanisms are the same, perhaps simpler. A custom application may look for a specific certificate or a specific digital signature.

Appendix B

Null Characters in Domain Name Attack

The heart of the attacks demonstrated by Moxie Marlinspike at Black Hat 2009 was the use of null characters in a domain name in a digital certificate[7].

When a client connects to a server in an attempt to use SSL the server responds, in part, with its certificate. The client then looks at the Common Name field of that certificate, which should contain the name of the server, and will then compare that name to the name of the server it expects, such as www.symantec.com.

It is possible to trick the client into seeing the name it expects, when the actual domain name in the certificate is that of a malicious site belonging to an attacker.

Marlinspike begins the explanation of this attack by noting that when you buy a low-cost certificate from a CA these days the process is automated. If an unauthorized party requests a domain-validated certificate for a.b.c.symantec.com, the CA will parse the base domain name (symantec.com) from the request, do a whois lookup on that domain and send a request for authorization to the Administrative Contact for the domain. Whoever is in charge of that for symantec will turn down Marlinspike and other unauthorized parties.

The Common Name field is one component of the Distinguished Name data grouping in X.509 certificates. Other fields include an organization, organizational unit, country, state, and locale. But most SSL implementations don't care about anything but the Common Name. It has become convention, in conventional SSL, to ignore the other fields with respect to authentication. Browsers may display those fields when you click the lock icon, but they are not used for authentication.

X.509 certificates are formatted using a notation system called ASN.1[8] which allows many string types. One of them is called an IA5String and is formatted with a byte length prefix, in the style of programming in Pascal, a language popular in the 1980s: The string is prefixed with a byte that defines the length of the string, followed by the string data itself[9].

Pascal-style strings are not common in conventional programming these days, as C language-style strings have predominated along with C-influenced languages. Thus it is common for programs which read certificates to do so with C or another language that handles strings the way C does.

C strings have no length indicator and, instead, are null-terminated. One major advantage of this is that strings can be larger than 255 characters, which is a limit for Pascal in using a single byte. It also means that strings cannot contain a null

[7] Null Prefix Attacks Against SSL/TLS Certificates - http://www.thoughtcrime.org/papers/null-prefix-attacks.pdf
[8] Wikipedia, Abstract Syntax Notation One - http://en.wikipedia.org/wiki/ASN.1
[9] In fact, strings were not part of the original Pascal language at all but are an extension defined as part of the popular UCSD Pascal. (Wikipedia, UCSD Pascal - http://en.wikipedia.org/wiki/Ucsd_pascal)

character (a zero byte, often written as \0), because the string reading code stops when it reaches that character.

This is the problem on which Marlinspike relies.

He then buys a certificate (for example) for www.symantec.com\0.thoughtcrime.org (Marlinspike legitimately owns thoughtcrime.org). The CA contacts the owner of thoughtcrime.org – him – and checks to see that he wants to buy this certificate. He says yes.

Then he installs this certificate on his server. Assuming he can get a client to reach his server after attempting to reach www.symantec.com, something he can do with other well-known attacks, the SSL tests will pass and his site will authenticate as www.symantec.com. This is because most SSL implementations will compare the two names and stop at the null embedded in his Common Name.

But it gets worse: having to buy targeted certificates for each site you attack can be cumbersome and expensive. You can buy wildcard certificates instead that allow you to match to anything: *\0.thoughtcrime.org.

Marlinspike provides a long list of SSL client programs which are vulnerable to this attack, including Firefox, Internet Explorer, Outlook, AIM, Citrix VPN, and more.

On October 13, 2009, Microsoft issued an update to their CryptoAPI that addresses this situation[10]. On systems which have the update applied CryptoAPI rejects certificate names that contain null terminators.

Appendix C

CA/Browser Forum Rules for Validating an Applicant for a Certificate

Private organizations, business entities, non-commercial entities (international organizations) and government entities may apply for certificates, and there are rules for validating each.

For Private Organizations:

1. The Private Organization must be a legally recognized entity whose existence was created by a filing with (or an act of) the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration (e.g., by issuance of a certificate of incorporation) or is an entity that is chartered by a state or federal regulatory agency;
2. The Private Organization must have designated with the Incorporating or Registration Agency either a Registered Agent, or a Registered Office (as required under the laws of the Jurisdiction of Incorporation or Registration) or an equivalent facility;

[10] Microsoft Security Bulletin MS09-056 - Vulnerabilities in Windows CryptoAPI Could Allow Spoofing. http://www.microsoft.com/technet/security/Bulletin/MS09-056.mspx

3. The Private Organization must not be designated on the records of the Incorporating or Registration Agency by labels such as “inactive,” “invalid,” “not current,” or the equivalent;
4. The Private organization must have a verifiable physical existence and business presence;
5. The Private Organization’s Jurisdiction of Incorporation, Registration, Charter, or License, and/or its Place of Business must not be in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA’s jurisdiction; and
6. The Private Organization must not be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA’s jurisdiction.

For Business Entities:

1. The Business Entity must be a legally recognized entity whose formation included the filing of certain forms with the Registration Agency in its Jurisdiction, the issuance or approval by such Registration Agency of a charter, certificate, or license, and whose existence can be verified with that Registration Agency;
2. The Business Entity must have a verifiable physical existence and business presence;
3. At least one Principal Individual associated with the Business Entity must be identified and validated;
4. The identified Principal Individual must attest to the representations made in the Subscriber Agreement;
5. Where the Business Entity represents itself under an assumed name, the CA must verify the Business Entity’s use of the assumed name pursuant to the requirements of Section 15 herein;
6. The Business Entity and the identified Principal Individual associated with the Business Entity must not be located or residing in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA’s jurisdiction;
7. The Business Entity and the identified Principal Individual associated with the Business Entity must not be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA’s jurisdiction.

For Non-Commercial Entity Subjects (international organizations):

1. The Applicant is an International Organization Entity, created under a charter, treaty, convention or equivalent instrument that was signed by, or on behalf of, more than one country’s government.
2. The International Organization Entity MUST NOT be headquartered in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA’s jurisdiction; and

3. The International Organization Entity MUST NOT be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction. Subsidiary organizations or agencies of qualified International Organizations may also qualify for EV certificates issued in accordance with these guidelines.

And for Government Entities:

1. The legal existence of the Government Entity must be established by the political subdivision in which such Government Entity operates;
2. The Government Entity must not be in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction;
3. The Government Entity must not be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.

More Information

Visit our website

http://www.symantec.com/ssl

To speak with a Product Specialist in the U.S.

1-866-893-6565 or 1-650-426-5112

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our website.

About Symantec

Symantec protects the world's information and is the global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device to the enterprise data center to cloud-based systems. Our industry-leading expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at: go.symantec.com/socialmedia.

Symantec World Headquarters

350 Ellis Street
Mountain View, CA 94043 USA
1-866-893-6565
www.symantec.com

UID: 080/10/13