White Paper

The State of SSL Security

Why Secure Sockets Layer Certificates Remain Vital to Online Safety

Symantec

Norton SECURED powered by VeriSign

The State of SSL Security

Contents

Without adequate security, online transactions—and the Internet as we know it—could not serve as a feasible platform for global commerce, transmission of data, or the sharing of reliable information. SSL security is the easiest, most cost-effective way to provide that strong protection.

Yet high-profile SSL hacking incidents have filled the news headlines recently. Poor security practices by secure sockets layer (SSL) Certificate Authorities (CAs), coupled with persistent outcries from industry detractors that the CA model is no longer viable, caused the digital certificate to have a challenging year in 2011. But SSL itself is not the problem. Rather, the culprits tend to be weak validation, lax oversight of third-party authenticating entities, failure to use best practices to secure facilities, or other factors that are less a matter of the technology than of operator error. SSL itself is still critical to keeping online transactions safe. The real issue is that businesses considering SSL should remember that their choice of vendor matters—significantly.

What SSL is—and why it matters

To transact business securely online, we need to transmit information between web sites and customers in such a way that other people—or systems—can't easily intercept and read it. Most web traffic goes over the Internet in an unencrypted form. This means that anyone with sufficient technical expertise and tools can easily "eavesdrop" on the conversations between two parties. SSL security prevents this eavesdropping in two ways. First, it encrypts the data moving between a web server and a browser, making it extremely difficult to intercept and decode the information. Second—and more significantly—it uses "certificates" to ensure that both members of an online conversation know who they are communicating with.

Say a customer is attempting to buy a costly piece of computer equipment from an online retailer. The customer wants to make sure that he or she is really talking to the retailer before typing in a credit card number. Even if the credit card data is encrypted while in transit across the internet, if someone is "spoofing" the retailer's web site—pretending to be the retailer by putting up a false web site, for example—the credit card could fall into the hands of a criminal.

This is where SSL certificates come in. SSL certificates provide the digital proof that each party in a transaction is who they say they are, and that the transaction is secure and authentic.

Here's how it works: The SSL vendor gives a web site a unique credential identifying that it is a certificate owner. When a customer tries to access the web site, his or her browser immediately asks for the server's SSL certificate. The browser then verifies the authenticity of the certificate by checking whether it has been signed by a "root" CA that the browser has been instructed to trust. However—and this has been the cause of some of SSL's recent woes—the browser may in fact be relying on third-party Registration Authorities (RAs) to validate the certificate. An RA is essentially a local reseller for a CA that validates identities on behalf of the root CA. In theory, the CA tightly monitors and controls the quality of its RAs, so that everyone in the transaction can trust that that the RA has done its job properly—and the CA can safely issue the certificate. This "web of trust" that starts

with a trusted root CA and extends to trusted authorities is critical for SSL success. If any thread in this web is vulnerable or compromised in any way, hackers could get false certificates that could be used to trick browsers into trusting them. This makes the whole system vulnerable to so-called "man-in-the-middle" attacks.

Different levels of validation, different levels of trust

SSL vendors provide three types of certificates, ranging from the most basic (a domain validation certificate) to the most sophisticated (an extended validation certificate). Below you will find brief descriptions of each.

- **Domain validation (DV) certificate.** This certificate simply validates an organization's domain name and ensures that it controls the domain in question. It then applies a 256-bit encryption to any information transmitted. According to Frost and Sullivan, 39.4 percent of SSL certificates issued fall into this most rudimentary category.[1] Many industry insiders find this number—which is growing—alarming, as a DV certificate provides minimal protection. After all, when a DV certificate has been issued, the CA merely checks the right of the applicant to use a specific domain name. The CA doesn't investigate the company identity, and no information is given to the customer's browser other than the encryption information. Because of this, DM certificates are the easiest—and least expensive—certificates for web sites to obtain. They're also the easiest for hackers to acquire fraudulently.
- **Organization validation (OV) certificate.** This type of certificate goes several steps further than a DV certificate, and validates the organizational data and the administrator in addition to the domain. This is the most popular kind of certificate requested, with 44.6 percent of all certificates falling into this category, according to Frost and Sullivan. The additional organizational information provided is available to customers by clicking on the Secure Site Seal, given them a greater sense of trust that the web site is authentic. OV certificates are popular because they provide more assurances than DV certificates, yet aren't as complex or costly as extended validation certificates.
- **Extended validation (EV) certificate.** Currently the highest level of validation, this certificate requires a CA to do extensive validation before authenticating a certificate. After the certificate has been authenticated, the customer's browser bar turns green to assure him or her that the web site is indeed secure. Specifically, the CA checks the right of the web site to use its domain name, plus it does a much more thorough evaluation of the organization itself, including verifying that the organization in fact does exist legally, physically, and operationally, and that the organization's identity matches official records. Acquiring an EV certificate is both more time-consuming (up to two weeks) and costly than obtaining either DV or OV certifications, and sales of EV certificates have disappointed industry observers. As of 2011, only 16 percent of certificates released fell into this category.

1. "Analysis of the SSL Market." Frost and Sullivan, November 2011.

SSL under siege

2011 was a tough year for SSL, and 2012 is shaping up to offer more of the same challenges.[2] First, in March 2011, a hacker obtained fraudulent digital certificates after breaching an Italian RA for Comodo, a known CA. The rogue SSL certificates were generated to impersonate Google, Yahoo!, Skype, and other major web sites. A week after the initial attack, Comodo admitted that two additional RAs in their network had also been compromised.[3] This was a case where one or more of the threads in the web of trust had snapped, possibly because of a lack of RA oversight. In May 2011, another reseller for Comodo, Comodo Brasil, was compromised via SQL injection. Although Comodo does not own Comodo Brasil, the reseller relatioship and the shared name did not help the embattled CA's reputation.[4]

Then, near the end of August, it became known that a rogue *.google certificate had been issued by a Dutch CA, DigiNotar.[5] The certificate in question was used in a number of attacks against Google services and was immediately revoked. The same attacker who had gained mild notoriety from breaches at Comodo, dubbed "ComodoHacker," claimed to have been the perpetrator of this breach as well.[6] An investigation of the DigiNotar breach uncovered that the attacker gained access to the Dutch CA's certificate authority servers in mid-July 2011. Over the course of two weeks, the attacker was able to install malware across DigiNotar's network and generate over 500 rogue certificates. In August, multiple Internet service providers (ISPs) in Iran began having certificate problems. Only at that point did DigiNotar admit that the hacker had created dozens of fraudulent certificates, including certificates for Yahoo!, Mozilla, WordPress, and even other CAs. To make matters worse, DigiNotar was unable to ensure that the fraudulent certificates had been revoked. An independent audit of DigiNotar's network identified a number of severe security flaws that ranged from critical servers that lacked basic malware detection software and weak administrator keywords, to the fact that their CA servers were accessible via LAN.[7] By the end of September 2011, the Dutch CA's roots were removed from all browsers' trusted root stores and DigiNotar was forced into bankruptcy.[8]

In September 2011, in another blow to the SSL industry's reputation, researchers discovered a critical vulnerability in virtually all websites protected by SSL. The browser exploit via SSL/TLS, dubbed "BEAST," could allow hackers to decrypt data passing between a web server and a customer's browser. The problem was traced to vulnerabilities in versions 1.0 and earlier of transport layer security (TLS), the predecessor to SSL. Although Versions 1.1 and 1.2 of TLS were deemed safe from this vulnerability, these versions aren't yet supported by most browsers or websites. This meant that, in theory, anyone engaged in transactions on major commercial web sites—including PayPal and Gmail—couldn't trust that their information was secure from criminals. BEAST proved to be more of an academic threat than a genuine one, as it required a specific computer to be infected with a specific piece of Java malware and intercepted while visiting a targeted website within the attacker's network. Oracle has since released a security update to eliminate the Java exploit.

---

2. "Internet Security Threat Report, Volume 17," Symantec, April 2012.
3. "Comodo: Web Attack Broader Than Initially Thought," CNET, March 2011.
4. "Comodo Brazil Breached, Sensitive Data Leaked," Help Net Security, May 2011.
5. "Interim Report: DigiNotar Certificate Authority Breach 'Operation Black Tulip," Fox-IT, September 2011.
6. Ibid.
7. Ibid.
8. Ibid.

2011's SSL woes were far from over. In November, a Malaysian CA, DigiCert Sdn. Bhd. (Digicert Malaysia), was caught issuing certificates with weak 512-bit keys. Entrust, Inc., the CA that had issued an intermediate root certificate to DigiCert Malaysia, revoked the Malaysian CA's certificate on November 8, 2011. The issuance of 512-bit certificates is considered poor practice, and DigiCert Malaysia roots have been pulled from both the Internet Explorer and Mozilla trusted root stores.[9]

Amidst these various incidents, the SSL industry itself was changing. Consolidation of major market players means that approximately 15 major SSL vendors are left, with Symantec holding approximately 39 percent of the market.[10] At the same time, the steadily growing number of CAs and RAs—the Electronic Frontier Foundation estimates that as of 2012 more than 650 CAs were in existence—means that the web of trust is being stretched, perhaps too far, as some experts believe. On a global scale, the CA business today is highly fragmented, with many local and regional players jumping into the market to meet the needs of businesses adhering to local laws, regulations, and accreditation processes to produce legally binding digital signatures.

Although the total number of issued certificates is growing, primarily due to increased online commerce, vendors are seeing less revenue growth because of price erosion for low-end DV certificate vendors and SSL resellers. Typically priced at USD49 to USD150 by major SSL vendors, DV certificates are being sold for as little as USD12 per certificate. OV certificates have a broad range of cost, from USD60 to USD1,000 a year, and EV certificates have a wide USD100 to USD1,500 per year price spread.[11]

This is mixed news. On the one hand, more certificates means that more web sites are protected with SSL. On the other hand, much of this growth is at the very low end of the scale, with demand for DV certificates growing at a faster rate than for either OV or EV certificates. Commoditization appears unavoidable—but many experts believe that the SSL market could suffer further declines in reputation if commoditization continues, as the decreasing margins could put CAs or RAs under financial pressure, tempting many smaller CAs to cut corners on security and infrastructure investments that could ultimately put consumers at risk.

Emerging SSL trends: protecting the fragile trust ecosystem

SSL security breaches spell trouble for the entire security community. But SSL itself is not the problem. Rather, poor validation and lax oversight of third-party authenticating organizations are the primary culprits. Leading CAs are still capable of providing the greatest assurance possible that their certificates—and the web sites that use those certificates—are authentic and safe for online business.

As SSL Adoption Continues to Rise, Symantec Remains the Global Market Leader

The number of sites using SSL has more than doubled between 2005 and 2012, and today more than 4.5 million sites are using SSL certificates issued by a Certificate Authority.[1] Symantec remains the dominant CA in the marketplace, with a 65.1 percent global market share and 41.3 percent year-over-year growth in EV SSL certificates.[2]

1. Netcraft, February 2012 SSL Survey
2. Netcraft, April 2012 SSL Survey

9. "Firefox and Internet Explorer Pull Trust in DigiCert Malaysia SSL Certificates," TechWorld, November 2011.
10. Netcraft, SSL Survey, April 2012.
11. Ibid.

To bolster the fragile trust ecosystem that is essential to the success of SSL, leading SSL vendors are already taking steps to address many of these issues.

- **Apply best-practice standards for DV and OV certificates.** Not all SSL certificates are issued equally. There are currently no industry standards within the SSL vendor market to ensure an appropriate level and rigor of authentication and security. However, leading CAs publish their policies to show that they have the necessary security infrastructure in place. At minimum, that infrastructure should include specifically designed physical facilities that are secure against access by non-authorized personnel, hardware-based cryptographic signature systems, and regular audits by trusted third parties. Other best practices should include enforcing dual control certificate issuance, use of authentication/registration best practices to identify ownership, and documented CA employee background investigations to protect against insider threats.
- **Expand use of EV certificates.** EV certificates were introduced in 2007. But growth has been slower than expected. To obtain an EV certificate, an organization must be thoroughly validated, which can take from two days up to two weeks. Plus, the certificates are substantially more costly than either DV or OV certificates. For these reasons, organizations seem reluctant to obtain them, despite the fact that they provide the highest level of SSL security. But the sooner more web sites obtain EV certificates, the more secure online transactions will be.
- **Adopt always-on SSL across high-traffic websites.**[12] The growth of Web 2.0 and social media provides users with highly personal and interactive online experiences. Many of these new services rely on browser "cookies" to remember users as they move from site to site or between different sections of a single site. But insecure cookies make users vulnerable—not least Facebook CEO Mark Zuckerberg, whose Facebook fan page was hacked in January 2011. Just one day later, Facebook announced that the world's largest social network would move to always-on SSL.[13] Always-on SSL encrypts all pages on a website, not just the log-in page. This protection is especially required for users who log in using an SSL secured page but then move on to unsecured pages, because the cookie that established the initial session can be sent without encryption and intercepted by a criminal who could use the information to compromise the account. According to the Online Trust Alliance, so-called "sidejacking" is easier than ever with plug-ins like Firesheep, a Firefox add-on that enables attackers to take advantage of unprotected HTTP connections on open Wi-Fi networks.[14] With always-on SSL, users can rely on site-wide SSL/TLS and HTTP Secure (HTTPS) to protect their entire experience, no matter what Wi-Fi network they've joined. As a proven and practical security measure, it should be deployed on all websites where users share sensitive data about themselves.

SSL in the cloud

With the emergence of cloud computing, SSL is more complicated than ever.

To begin with, cloud business models vary considerably: for some, it's a pay-as-you-go model, while others offer subscriptions by the month or year. Yet SSL certificates are valid for one or more years. Also, some CAs are working on SSL certificates that allow a single certificate to work for many users' on-demand requests for certification. Others are working on developing certificates that meet the high-level encryption capabilities of the powerful physical servers behind the cloud. All of these considerations are likely to make SSL more, not less, critical in coming years.

12. For more information about always-on SSL, see the Online Trust Alliance white paper "Protecting Your Website with Always On SSL," March 2012.
13. "Facebook Rolls Out Always-On Encryption in Wake of CEO's Fan Page Being Hacked," InfoWorld, January 2011.
14. "Protecting Your Website with Always On SSL." Online Trust Alliance, March 2012.

- **Offer solutions-based offerings that supplement SSL and ensure more trust.** Many SSL vendors are moving towards solutions-based offerings to add value to the customer experience and ensure greater trust. For example, some SSL vendors are offering web site malware and vulnerability scanning in addition to basic encryption and confidentiality assurances. These features verify that a web site is not vulnerable to hackers or other kinds of attacks—a benefit to both SSL vendors and businesses alike.

Why working with a trusted, industry-leading vendor is critical

As consumer and business use of the Internet continues, especially for e-commerce, so does demand for SSL certificates. Recent setbacks for the SSL industry don't detract from the value of SSL; rather, they point to the importance of choosing an SSL provider carefully.

Trust is a critical aspect of SSL. Without trust, SSL doesn't function as a security mechanism. Both customers and internal users will feel more comfortable providing their personal data if they see that a site has been certified by a reputable vendor.

Some organizations issue self-sign certificates, primarily in the hopes of saving money. But this is not recommended. In many cases, the security infrastructure is not in place, and the expense of managing it more than outweighs any cost savings on the certificates themselves.

What to look for in an SSL vendor:

- **Consumer brand recognition and trust.** A certificate is only as good as the consumer believes it is. Choose an SSL vendor with an impeccable reputation—one that has the unwavering trust of everyone who spends any significant time online.
- **A comprehensive portfolio of solutions.** By offering a full range of solutions, leading CAs enable their partners to address all customer segments and requirements so that they don't have to deal with multiple vendors. Symantec's family of dominant SSL brands includes Symantec SSL, GeoTrust, Thawte, and RapidSSL, commanding nearly 40 percent of all active SSL certificates in use today.[15]
- **Best-of-breed authentication infrastructure and practices.** A vendor like Symantec has military-grade infrastructure and practices in place to ensure that data remains protected. This, combined with years of experience in the industry, makes Symantec a superior choice for SSL. Price certainly influences many organizations' SSL buying decisions, but simply looking at the number of CA breaches in 2011 should remind you that price should be but one of many factors in selecting a CA.

15. Netcraft, SSL Survey, April 2012.

- **Ease of doing business.** Many corporations and SMBs are highly challenged to manage the tens to thousands of certificates they purchase. A CA like Symantec provides customers with tools—including an easy-to-use web portal—that offer much-needed visibility into their certificate data. Additionally, leading CAs allow customers to purchase additional certificates and check which certificates are expiring. Some CAs like Symantec even provide an overview of all certificates installed on an organization's server regardless of the issuing CA. This is essential for corporations handling large numbers of certificates, as it enables them to quickly purchase a certificate and achieve validation.
- **Support.** As with any technology product or service, you need to know that your vendor will be there to support you when the chips are down. You should pick a vendor that is responsive, completes the authentication process in a timely manner, and is able to offer quick, effective remediation for any issues that arise, anywhere in the world, 24/7. Global support capabilities are increasingly important in an increasingly "flat" business world, including localized help available across all geographies from native language speakers. Make sure that your SSL vendor offers the resources necessary to assess an emerging security situation, design and deploy a remediation plan, and monitor your vulnerability going forward.

Conclusion

Although the only way to achieve comprehensive security is to secure *all* traffic to and from web sites, the fact is that many web site owners are choosing minimal SSL measures rather than spending the extra time and money to ensure that their customers—and their internal users—are safe.

Still, advances in technology—coupled with promoting a better understanding of the importance of moving beyond minimal SSL security to OV or EV certificates—will help promote more (and more judicious) use of SSL as online commerce becomes ever more important to people throughout both their personal and business lives. The SSL model is still sound. However, understanding the importance of choosing a truly trusted SSL vendor is key to the web of trust that makes e-commerce possible.

Companies have depended on SSL technologies to secure customer communications and transactions for more than a decade now. As the world moves into more of an interconnected and social way of interacting online, and as mobile access to the internet becomes an imperative, this will only continue.

More Information

Visit our website

go.symantec.com/ssl-certificates

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

Call 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 is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

Symantec Corporation World Headquarters

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