WHITE PAPER: SECURITY AND TRUST: THE BACKBONE OF DOING BUSINESS OVER THE INTERNET

White Paper

Security and Trust: The Backbone of Doing Business Over the Internet

Symantec™

Norton™ SECURED
powered by VeriSign

Security and Trust: The Backbone of Doing Business Over the Internet

CONTENTS

Introduction

Gaining the trust of online customers is vital for the success of any company that requires sensitive data to be transmitted over the Web. In e-commerce, consumers are very concerned about identity theft, among other things, and are justifiably leery of providing their personal information to untrusted sources. People are reluctant to provide information like their credit card and social security numbers, passwords, health details, and other confidential data. The concern is that this sensitive information will be intercepted in-transit, or perhaps the destination website is manned by imposters with malicious intent.

The result is often an abandoned transaction – the bane of e-commerce. According to a study on this topic, 21 percent of users have not concluded an online purchase due to security concerns over credit card data[1]. Others may make small purchases but limit the size of their transactions for fear that the transaction will be compromised.

Such consumer fears are well founded. The "11th Annual Online Fraud Report" estimated 2009 fraud losses to U.S. and Canadian online retailers to be $3.3 billion[2]. The total number of unique phishing reports submitted to the Anti-Phishing Working Group (APWG) in December 2009 was 46,190[3].

Online businesses have much to gain by taking steps to assuage customer fears. Concern about Internet fraud, particularly identity theft, is a major inhibitor of online sales. Since fears of online scams limit not only the number of transactions conducted but also their size, the potential incremental business that can be generated through development of customer trust is significant. Consumers too have much to gain. The convenience and affordability of online shopping is unsurpassed. Often a consumer looking for a particular item is shopping across multiple websites – some trusted and some not.

The ability for the consumer to shop on a wide range of trusted e-commerce sites gives them the ability to make the best choice, while protecting their private information. Fortunately, there is technology available that helps online businesses protect sensitive customer data, authenticate their websites, and build consumer trust – technology that helps customers differentiate trustworthy websites from clones produced by scam artists with malicious intent.

This paper explores the current state of website security and the contributions Symantec is making to help organizations protect critical data and build trust with customers. It begins with Secure Sockets Layer (SSL) encryption, the technology that addresses the most obvious and oldest problem in online business – the susceptibility of sensitive data in-transit to interception by cyber criminals. This paper covers the need for data encryption offered by SSL, and the need for additional measures like authentication of website legitimacy and trust building with one's customer base.

[1] "Security Concerns Hinder Online Shopping, Survey Finds," June 2009. www.eweek.com/c/a/Midmarket/Security-Concerns-Hinder-Online-Shopping-Survey-Finds-288359/
[2] http://www.marketingcharts.com/direct/e-commerce-fraud-losses-drop-12308/cybersource-online-revenue-loss-fraud-mar-2010.jpg
[3] Anti-Phishing Working Group, December 2009; www.apwg.org

Encryption Technology and SSL Certificates

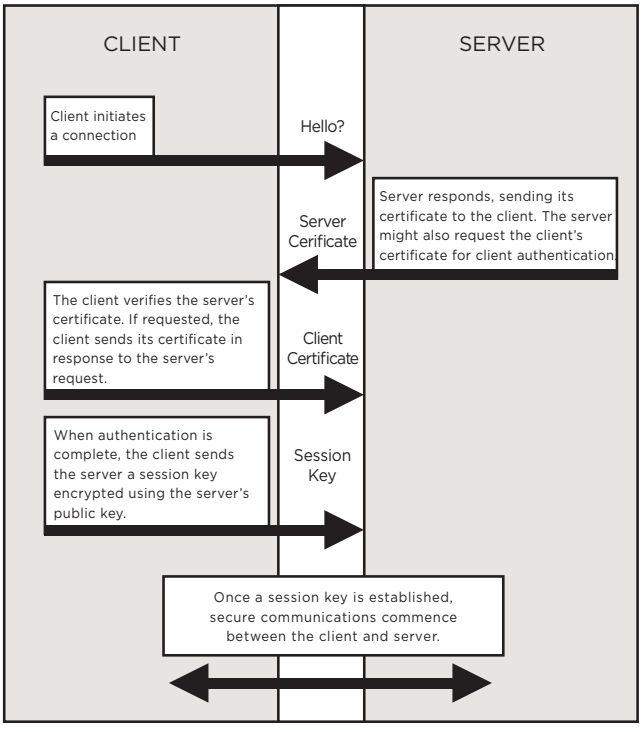
Customers know that any information they submit to an unsecured website is at risk. To survive in the market, online businesses need to incorporate the use of SSL certificates to encrypt and protect sensitive customer information.

Encryption is the process of transforming data to make it unintelligible to all but the intended recipient. It is the basis of data integrity and privacy necessary for e-commerce. Customers and business partners will submit sensitive information and transact on websites only when they are confident that it can be done so securely. The solution for businesses that are serious about e-commerce is to implement a trust infrastructure based on encryption technology.

Secure Sockets Layer (SSL), the world standard for Web security, is used to encrypt and protect information transmitted over the Web with the ubiquitous HTTP protocol. SSL encryption protects data in transit that could otherwise be intercepted and tampered with if unencrypted. Support for SSL is built into all major operating systems, Web browsers, Internet applications, and server hardware platforms.

An SSL certificate is an electronic file that uniquely identifies individuals and websites, and enables encrypted communications. SSL certificates serve as a kind of "digital passport," or credential. Typically, the "signer" of an SSL certificate is a third-party Certificate Authority (CA). Symantec is the world's leading CA with more than one million Web servers secured worldwide[4].

The following diagram illustrates the process that guarantees protected communications between a Web server and a client. All exchanges of SSL certificates occur within seconds and require no action by the consumer.



[4]Includes Symantec subsidiaries, affiliates, and resellers.

Levels of Encryption and SGC

Data encryption comes in various strengths, determined by the number of bits used in the encryption algorithm. The current minimum standard is 128-bit, which is considered for all intents and purposes unhackable at current computing speeds. Certain old versions of some operating systems and browsers, in certain combinations, do not support more than 40- or 56-bit encryption. These lower levels of encryption could be easily hacked, rendering users of those operating system and browser combinations vulnerable to attack.

A technology called Server-Gated Cryptography (SGC), available with certain Symantec SSL Certificates, overcomes this problem for 99.9 percent of website visitors. Websites equipped with SGC "step up" to 128-bit encryption for communications with systems that normally can perform only 40- or 56-bit encryption.* Therefore, businesses that employ SGC SSL certificates can guarantee a sufficient level of encryption to all of their customers. Symantec™ Secure Site Pro with EV supports SGC 128-bit encryption and all Symantec SSL Certificates support up to 256-bit encryption on all connections where both the client and the server are capable of encrypting at this level.

Levels of Authentication and Trust

One of the key purposes of SSL certificates is to help assure consumers that they are actually doing business with the website they believe they are accessing – i.e., the legitimacy of the website has been authenticated by a trusted third-party. There are three commonly recognized categories of SSL authentication:

- Domain
- Organization
- Extended Validation (EV)

The differences in the level of security provided, and related customer trust engendered, are vitally important. Even within a level specific authentication processes vary from CA to CA – a key reason for choosing a widely known, respected, and trusted CA. Symantec is the world's leading provider of SSL certificates and maintains more EV SSL certificates than any other Certificate Authority[5].

Domain Authentication

A domain authenticated SSL certificate provides the lowest form of authentication available. With this category of validation, CAs conduct a process to verify that an entity requesting a domain authenticated SSL certificate either owns the domain requested or has the right to use that domain name. The CA may also verify that the email address for the contact requesting the certificate is either listed in the WHOIS directory or meets the CA's predetermined email alias requirements. All websites secured with Symantec SSL Certificates submit to a higher level of authentication beyond domain authentication.

* Users with the following browser versions and operating systems will temporarily step-up to 128-bit SSL encryption if they visit a website with an SGC-enabled SSL certificate: Internet Explorer export browser versions from 3.02 but before version 5.5; Netscape export browser versions after 4.02 and up through 4.72; Windows 2000 systems shipped prior to March 2001 that have not downloaded Microsoft's High Encryption Pack or Service Pack 2 and that use Internet Explorer. Internet Explorer browser versions prior to 3.02 and Netscape browser versions prior to 4.02 are not capable of 128-bit encryption with any SSL certificate.

[5]Includes Symantec subsidiaries, affiliates, and resellers.

Organization Authentication

Organization authentication is the validation process that Symantec and other CAs employ for common (i.e., non-EV) SSL certificates. CAs begin by verifying the organization's existence through a government-issued business credential, normally by searching government and private databases. If necessary, they may request such items as Articles of Incorporation, business licenses, and Fictitious Business Name statements. Before issuing an SSL certificate with Organization Authentication, CAs verify a company's identity and confirm it as a legal entity, validate that it has the right to use the domain name included in the certificate, and verify that the individual who requested the SSL certificate on behalf of the company was authorized to do so.

Extended Validation Authentication

Extended Validation authentication (EV), offers the highest level of authentication available with a SSL certificate. EV authentication adds structure and controls to the authentication process. It includes an in-depth validation of an entity's authenticity starting with a signed acknowledgement of agreement from the corporate contact. A company registration document may also be required if the CA is unable to confirm the organization's details through a government database.

A legal opinion letter may be requested to confirm the following details about the organization:

- Physical address of the place of operation
- Telephone number
- Confirmation of the exclusive right to use the domain
- Additional confirmation of the organization's existence (if less than three years old)
- Verification of the corporate contact's employment

The process represents little burden for legitimate organizations, but is a substantial obstacle for a fraudster.

Earning Trust Marks

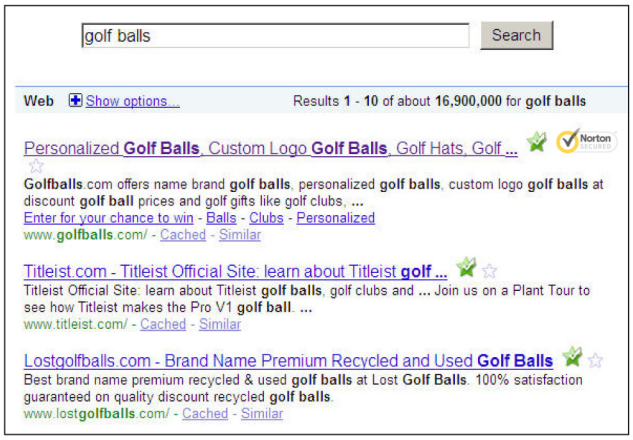
To earn trust and maximize online business, e-commerce sites need to not only protect their customers' online transmissions, but clearly communicate that concrete measures have been taken to enable this security. To convey this investment in security, with the goal of building customer trust, CAs display seals bearing their trust mark. These seals are commonly posted prominently on a website.

The Norton™ Secured Seal is the world's most used and most recognized Internet trust mark. In tests, 40 percent of consumers trust Norton Secured Seal, more than our competitors' trust seals[6]. Clicking on the Norton Secured Seal brings up a display showing the name of the certificate owner, the validity period, information about the security services provided, and details on the owner validation process Symantec conducted prior to issuing the certificate.

[6]Symantec Consumer Research Study, January 2011

Symantec Seal-in-Search: Communicating Trust Early and Often

Whereas SSL assures customers that their transactions are secure and that the website is authentic, look for advanced solutions that can establish customer peace of mind at multiple points in the customer experience – the earlier that a trust message can be communicated, the better. To engender trust at all phases of the customer's interaction, Symantec bundles SSL with other trust functionality, including malware scanning of websites and, subject to results of the scan, the related display of a trust mark in conjunction with search results.



This capability, known as Symantec™ Seal-in-Search, enables online businesses to convey a sense of trust prior to customer navigation to their website. The ability of an online business to reach a potential visitor with a positive trust message so early in their process helps differentiate them from competitors that employ other brands of SSL certificates that do not include website malware scanning or the ability to display a trust mark in conjunction with search results.

Extended Validation SSL: Enabling Trust

In the past, indicators of an SSL session such as "https" in the URL or the gold lock icon were sufficient to quell most consumer fears of malicious activity on the Internet. They provided assurances that sensitive data transmission was protected by sufficient levels of encryption. Today, even the strongest encryption is no longer enough because of a very different problem – phishing. Internet thieves have become adept at posing as genuine online businesses. They purchase SSL certificates – which, unfortunately, are all too available from lower quality CAs that perform inadequate authentication – and use them to trick customers into sending them sensitive information.

Encryption is necessary, but no longer sufficient – it does no good if the recipient of the encrypted transmission is a falsified business and proceeds to use confidential data for identity theft, or some other form of malfeasance. The ability to convey trust to users is a significant challenge. Even if a site appears to be a known and trusted online business, how are people to know that it is not a clone from a clever imposter with malicious intent?

To earn trust, there needs to be an easy, reliable way to show customers that not only are their transactions secure, but that the website where the consumer is performing the transaction is a legitimate and owned by a verified business entity. To meet this need, security vendors and developers of Internet browsers combined forces to establish the Extended Validation (EV) standard, the first fundamental change in the world's secure e-commerce backbone in over ten years. Symantec adheres to this standard with its Extended Validation SSL certificates.

When customers using high-security browsers visit a webpage secured with an EV SSL certificate, the address bar turns green and a special field appears with the name of the legitimate site owner along with the name of the security provider that issued the EV SSL certificate. The browser and the security vendor control the display to deter phishers and counterfeiters from hijacking website's brand and customer information. Fraudsters are becoming adept at mimicking almost everything about a website, but without the legitimate company's EV SSL certificate there is no way they can display its name on the address bar because the information displayed is outside of their control. The ability for someone other than the legitimate site's owner to obtain the company's EV SSL certificates is not possible because of the stringent authentication process conducted by the CA.

EV SSL is Comforting to Consumers

- Online customers can see the visual display of the certificate owner's name on the address bar to make sure the website is indeed authored by the intended source and not an imposter.
- CAs conduct additional levels of validation of an organization's legitimacy and authenticity before issuing them EV SSL certificates to keep fraudsters from posing as legitimate Internet businesses.
- In order to operate, CAs must satisfy rigorous criteria to be eligible to issue EV SSL certificates. CAs must pass regular third-party WebTrust audits that confirm compliance with the standards of the CA/Browser Forum, a consortium of CAs and browser suppliers. This eliminates the use of feeble background checks by inadequate CAs that enable malicious imposters to operate unimpeded. With EV SSL, customers can feel confident that the organization has been properly vetted as the legitimate owner of the website.
- The color change to green appears to create a positive association for consumers. Even customers who are not familiar with the "real" reasons why EV protects them are more inclined to convert to sales and buy more per sale if they see a green bar.

Evidence that EV SSL works is overwhelming. Dozens of tests conducted by companies around the world have demonstrated that the use of Symantec EV SSL increases transactions, on average, by 17.8 percent[7]. Customer use cases of this type demonstrate the value and importance of EV SSL and the Symantec brand name with respect to recognition, trust, and preferences.

[7]Based on 32 case studies in 11 countries

Furthermore, the Norton™ Secured Seal, included with all Symantec SSL Certificates, allows a company to display the number one sign of trust on the Internet. In tests, 77 percent of consumers recognized the Norton Secured Seal, more than our competitors' trust seals[8]. The Norton Secured Seal also allows visitors to check the SSL certificate's information and status in real time – increasing customers' trust in the online business.

Symantec: The #1 Provider of Online Security

Symantec is the world's leading provider of SSL certificates and maintains more EV SSL certificates than any other Certificate Authority. 97 of the world's top 100 SSL-using banks, over 97 percent of the Fortune 500 companies, and 81 percent of the 500 biggest e-commerce sites in North America use SSL certificates sold by Symantec[9]. Web users are accustomed to seeing commercial e-commerce websites display the Norton Secured Seal – prominently featured to assure online users that their online business is authentic and that their site is capable of securing their confidential information with SSL encryption.

Conclusion

With the skyrocketing rise in Internet fraud, security of personal data transmissions has never been more critical to e-commerce. The prevalence – and consequences – of identity theft are all too well known and documented. With the increased level of Internet data theft, potential customers have become more savvy, more skeptical, and frankly, more scared. They expect to be protected, and they want more assurance that their information is secure.

Establishment of customer trust makes all the difference. Investment in technology to protect customers and earn their trust is trivial when compared to the overall cost of doing business. When the costs are dwarfed by the potential upside, it's clear that enhancing e-commerce site security, with technologies like SSL, is an obvious choice for online businesses looking to be successful.

To ensure that current and future customers are fully aware of security investments being taken by e-commerce businesses, it is critical to go with a security vendor whose brand name is the best known and the most trusted. Symantec has earned its industry-leading brand name recognition, and related customer trust, by delivering the state-of-the-art in online security and trust solutions.

[8]Symantec Consumer Research, January 2011
[9]Includes Symantec subsidiaries, affiliates, and resellers.

More Information

Visit our website

http://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

Symantec

Norton SECURED
powered by VeriSign