YANKEE GROUP

Building Blocks of Transparent Web Security: Server-Gated Cryptography

Security Solutions & Services
by Phebe Waterfield CISSP
September 2005

Executive Summary

Secure Sockets Layer (SSL) is the de facto standard for securing e-commerce transactions. SSL encrypts personal information such as credit card numbers, social security numbers, passwords, names and addresses sent to an e-commerce vendor via its web site. Therefore, SSL is a critical component in the protection of consumer privacy and a necessity to reduce the risks of fraud and identity theft.

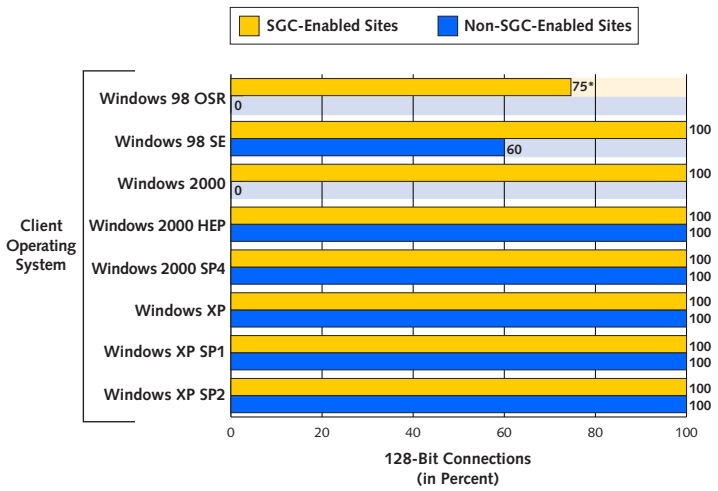
Yankee Group research shows that between 1% and 2% of e-commerce transactions are related to fraud. Losses totaling $2 billion in 2004 are growing at the same rate as e-commerce revenue and eroding consumer confidence. SSL encryption is a key component in protecting consumers' online transactions. Its transparency to users will be a critical factor in reducing fraud.

SSL lacks transparency in a key area: the strength of encryption used for a given session. Browsers, web servers and operating systems all play a role in determining the level of encryption used: 40 bit, 56 bit or 128 bit. Some PC systems can't take advantage of full 128-bit SSL encryption. Server-gated cryptography (SGC)-enabled certificates address this issue.

E-commerce web sites using SGC can assure customers of stronger encryption, greater privacy and reduced risks of fraud and identity theft.

This special report, commissioned by VeriSign, tests SGC- and non-SGC-enabled certificates in 92 common environments to determine under what conditions users benefit from strong encryption. As Exhibit 1 illustrates, SGC-enabled certificates enable more Windows 2000 users to connect with 128-bit encryption. This difference means tens of millions more internet users worldwide would get 128-bit encryption or higher if all e-commerce vendors used SGC-enabled certificates.

Exhibit 1
Summary of SGC Testing Results by Operating System
Source: Yankee Group, 2005



**Windows 98 OSR SGC results reflect anomalous test failures involving Sun ONE (25% of the tests). The anomalies have limited impact on the internet population—Sun ONE is run on less than 3% of all web sites.*

Table of Contents

I. Introduction

In this report, Yankee Group investigates the circumstances under which a user benefits from strong encryption; specifically, which combinations of clients and servers successfully negotiate strong 128-bit encryption and above instead of weaker 56-bit or lower encryption. We tested four certificate products from VeriSign with and without SGC capability on 23 combinations of client configurations and four typical web servers to determine the encryption level that is actually negotiated. We performed 368 separate tests, including video capture on the client side, to verify the level of encryption used. The results illustrate SGC SSL certificates' ability to make strong encryption available to users regardless of the web server, operating system or browser they use. We outline the results of this testing here and offer advice for consumers and e-commerce vendors on how to manage this important aspect of internet security.

II. Transparent Web Security

Early attempts to harness the power of public key cryptography using protocols such as SSL for encryption revealed one clear conclusion: The ideal user experience with public key cryptography is one of transparency. Users need to know whether they are using a secure channel, but shouldn't have to ensure that they are protected with 128-bit or 256-bit keys. For users who visit multiple secured sites each day, SSL ideally provides strong encryption transparently in ways that limit the possibility of users unknowingly connecting with weak encryption.

Computer operating system and browser capabilities have a lot to do with determining whether connections occur at the 128-bit or higher encryption level. Even new browsers that support 128-bit and higher encryption may only do so if the operating system also allows it. Many Windows 2000 systems will fail to step up to 128 bits unless the web site SSL certificate supports SGC.

Importance of Encryption Strength

Consumers and e-commerce vendors often view encryption as too complex for the average hacker to exploit. Surely any sort of encryption provides enough security to do online banking and shopping, right? Unfortunately, the answer is no. Low-level encryption, using 56 bits or less, is universally deemed too weak for safe financial transactions. With the computing power available today, it's not cost prohibitive for hackers to attack 56-bit encryption using brute force—which involves trying every possible key combination until they find the one that converts ciphertext into plaintext.

The difference in security between 40 bit, 56 bit and 128 bit is significant. The progress made in computing technology means that weaker encryption using 40-bit or 56-bit keys can be attacked by brute force and broken in a matter of hours using an average-speed PC. As recently as 1997, the same exercise would have taken days and required the effort of multiple computers and people. As illustrated in Exhibit 2, at current computing speeds, 128-bit encryption will take more than a trillion years to attack using brute force, an obstacle that would deter any financially motivated attacker. By contrast, breaking shorter 40-bit or 56-bit encrypted sessions is a relatively small investment for attackers harvesting personal information.

Businesses using SSL encryption to secure e-commerce sites need to keep on top of the need for sufficient encryption key lengths. The current recommended 128 bits will not be sufficient forever. As computing speeds improve, breaking 128-bit encryption will get faster and therefore cheaper.

Exhibit 2
Time to Break Encryption by Brute Force
Source: Yankee Group, 2005

Key Length	Time to Break 1997*	Time to Break 2005*	Number of Key Combinations
40-Bit DES	4 hours	Seconds	1x10*12 or 1 trillion
56-Bit DES	140 days	Days	7x10*16 or 70 quadrillion
128-Bit TripleDES	10*21 sextillion years	0.25 sextillion years	300 septillion

**Estimated assuming distributed computing network of high-end desktop computers*

Strong Encryption with Server-Gated Cryptography

In the 1990s, the US government imposed restrictions on exporting strong cryptography to other countries. The restriction meant that software implementing SSL, such as web browsers, operating systems and web servers, had to limit encryption to weak algorithms and shorter key lengths if it was sold for use outside the United States. Lawmakers included an exception for financial transactions to ensure that customers worldwide could safely transact online using strong encryption.

SGC was created as an extension to SSL for consumers with export versions of web browser software to use strong cryptography for financial transactions. US export laws were upheld by issuing SGC certificates only to eligible financial institutions, creating an enforcement point at the server without any impact to the client. The restrictions on export of strong encryption have since been lifted, and SGC certificates may be issued to any institution.

Restrictions on encryption are evident in old versions of Windows 2000 running Internet Explorer that are still in use. Consumers and e-commerce vendors, particularly those outside the United States, are still using weak encryption, despite the fact that safer, stronger alternatives are available. Although newer versions of Windows 2000 provide these features, millions still use old versions. Users who are still using old browser versions that only provide weak 40-bit or 56-bit encryption can gain full-strength 128-bit encryption when conducting business with SGC-enabled web sites. With SGC, browser and operating system versions—whether exports or domestic—that would otherwise connect with weak encryption are afforded much stronger security. Until older versions of browser and operating systems disappear completely, SGC certificates can protect this portion of the user population.

III. SSL Encryption Strength Test

We performed systematic testing on four typical web server configurations using SSL certificates and the most commonly used web browser and operating system combinations to validate that SGC-enabled certificates result in stronger 128-bit SSL encryption.

Hardware and Software Setup

Testing of SGC certificates took place at a facility with four web servers running in typical configurations: Sun ONE 6.1 on Solaris 10; Apache 2.0.46 on Red Hat ES 3; IIS 5.0 on Windows 2000; and IIS 6.0 on Windows 2003. Each web server was configured to host two SSL-enabled web sites—with and without SGC capability—for a total of eight distinct web server environments.

Client configuration was more complex due to the links between operating system and browser versions. We tested a total of eight operating system versions and 17 browsers in 23 combinations. Operating systems included Windows 98 through Windows XP, with and without service and high-encryption packs. After a particular version of a web browser was installed and tested against each of the four certificate-enabled web sites, the desktop was re-imaged with a fresh copy of the operating system and browser. Conducting each of the 23 tests on a fresh installation ensured accuracy in results and avoided the possibility of cached certificates affecting the test results.

We handled certificate enrollment and signing requests for each server using the system's default configuration options and native tools—except in the case of Red Hat's bundled Apache, where we used the supplied makefile to build a single certificate for the site. We used the 1,024-bit key option specified in this makefile to generate the RSA key pair and certificate request.

The common names used for each certificate included the platform being tested and the certificate type for that server, enabling a check and balance for the entire testing process.

Testing Methodology

Each test followed these steps:

- Enabled tcpdump on the router with switches to capture pertinent HTTPS traffic
- Booted the system and launched video recording software
- Verified the operating system version using msinfo32.exe
- Launched Internet Explorer and verified its version using the "About" option on the Help menu
- Loaded an SSL-enabled web site, visited each link and accepted all the security warnings indicating entry to a secure site
- Recorded SSL session information using the "Properties" option on the File menu
- Recorded details of the certificate by opening the certificate button (padlock icon)
- A custom server script also recorded specific details about the connection including the common name (CN) of the certificate and SSL- or HTTPS-related information to verify the client's connection
- Stored and archived video for later reference
- Suspended the system and saved its running state for later use

This testing methodology takes advantage of several indicators available to users and web site administrators to highlight the encryption level used for a specific session:

- Web browsers will display the certificate, its issuing authority and key length
- Network traffic will demonstrate characteristics of a 128-bit SSL handshake
- Web browsers will issue warnings on entering and leaving an encrypted web site

IV. Conclusions and Recommendations

The number of people still subject to weak encryption because they are using older versions of Windows and Internet Explorer is in the tens of millions. Users running the Windows 2000 operating system without Service Pack 4 or the high-encryption pack are most likely to be affected. Tested browsers released earlier than March 2000 also return higher rates of connection at low encryption levels. Our testing results show that when using SGC certificates, virtually all combinations of Windows operating system, Internet Explorer and server are able to step up to 128-bit encryption. Wide-scale deployment of SGC-enabled SSL certificates would reduce the actual number of users exposed by weaker encryption dramatically and make it possible for virtually every internet user to enjoy the protection of 128 bit or stronger encryption.

Recommendations for E-Commerce Vendors

- **Implement the strongest security available: SGC-enabled 128-bit or higher SSL encryption.** Aim to guarantee security for end users, but don't burden customers with too much information. Consumers only want to know whether they are secure. Professionals may understand the subtleties of public key cryptography, but consumers may not check key lengths. With SGC certificates, it's less important for users to understand these technical aspects of using SSL.
- **Recognize that weak client security imperils your brand.** Use consumer encryption levels as a measure of your own brand security. Consumers that visit your web site using weak encryption risk their personal information and reputation as well as yours. Ensure that all your customers are protected with strong encryption enabled through the use of SGC certificates.
- **Raise user awareness of safety online, particularly of the safe and correct use of SSL-enabled web sites.** Although steps are needed to improve the transparency and usability of SSL encryption for consumers, much can be achieved through education to reduce the risk of fraud, such as phishing.

V. Further Reading

Yankee Group Security Solutions & Services Report
Application Gateways Secure Business Communications, August 2004

Yankee Group

Yankee Group has research and sales staff located in North America, Europe, the Middle East, Africa, Latin America and Asia-Pacific. For more information, please contact one of the sales offices listed below.

Corporate Headquarters

31 St. James Avenue
BOSTON, MASSACHUSETTS 02116-4114
T 617.956.5000
F 617.956.5005
info@yankeegroup.com

EMEA

55 Russell Square
LONDON WC1B 4HP
UNITED KINGDOM
T 44.20.7307.1050
F 44.20.7323.3747
euroinfo@yankeegroup.com

North America

260 Terence Matthews Crescent, Suite 200
KANATA, ONTARIO, CANADA K2M 2C7
T 613.591.0087
F 613.591.0035
canadainfo@yankeegroup.com

Decision Services

Yankee Group Decision Service annual memberships offer clients access to research and one-to-one expert guidance.

Decision services represent our best value for clients. The services help our members understand industry, regulatory, competitive and market-demand influences, as well as opportunities and risks to their current strategies.

Membership includes an invaluable in-person strategy session with Yankee Group analysts, direct access to a team of analysts, DecisionNotes[sm] and regular online decision forums on relevant topics.

We offer Decision Services on almost 30 selected topics in Telecommunications; Wireless/Mobile Communications; Consumers, Media & Entertainment; and Information Technology Hardware, Software & Services.

Decision Instruments

Yankee Group offers a full portfolio of technology and market forecasts, trackers, surveys, and total cost of ownership (TCO), return on investment (ROI), selection and migration tools. Decision Instruments provide our clients the data required to compare, evaluate or justify strategic and tactical decisions—a hands-on perspective of yesterday, today and tomorrow—shaped and delivered through original research, in-depth market knowledge and the unparalleled insight of a Yankee Group analyst.

Trackers
Trackers enable accurate, up-to-date tactical comparison and strategic analysis of industry-specific metrics. This detailed and highly segmented tool provides discrete proprietary and performance data, as well as blended metrics interpreted and normalized by Yankee Group analysts.

Surveys
Surveys take the pulse of current attitudes, preferences and practices across the marketplace, including supply, delivery and demand. These powerful tools enable clients to understand their target customers, technology demand and shifting market dynamics.

Forecasts
Forecasts provide a basis for sound business planning. These market indicators are a distillation of continuing Yankee Group research, interpreted by our analysts and delivered from the pragmatic stance our clients have trusted for decades.

Signature Events

Yankee Group's Signature Events provide a real-time opportunity to connect with the technologies, companies and visionaries that are transforming Telecommunications; Wireless/Mobile Communications; Consumers, Media & Entertainment; and Information Technology Hardware, Software & Services.

Our exclusive interactive forums are the ideal setting for Yankee Group analysts and other industry leaders to discuss and define the future of conversable technologies, business models and strategies.

Consulting Services

Yankee Group's integrated model blends quantitative research, qualitative analysis and consulting. This approach maximizes the value of our solution and the return on our clients' consulting investment.

Each consulting project defines and follows research objectives, methodology, desired deliverables and project schedule. Many Yankee Group clients combine Decision Service memberships with a custom-consulting project, enabling them to augment our ongoing research with proprietary studies.

Thousands of clients across the globe have engaged Yankee Group for consulting services to hone their corporate strategies and maximize overall return.

www.yankeegroup.com