SGC and its Limited Value

Evaluating the near irrelevance of Server Gated Cryptography

Contents

Summary

Server Gated Cryptography (SGC) was created to step up weak encryption levels in browsers exported from the US from the mid-90s through 2000. While the need for the technology was clear at the time, those browsers are no longer in use today. Yet SGC is still seen by some in the industry to have value. The reality is SGC is not necessary with modern browsers and is merely a Band-Aid over the more serious vulnerabilities of the outdated browsers it is designed to help. Instead of using SGC to facilitate the use of outdated, insecure software, we should be encouraging users to use the latest, patched software.

Origins of SGC

SGC was introduced in response to United States federal legislation on the restrictions surrounding the export of strong cryptography (anything above 40 bit) in the 1990s. The legislation affected the major US incorporated browser vendors at the time – Microsoft and Netscape – whose browser software was being exported outside of the US. However recognizing a legitimate need for strong encryption for international financial transactions, an exemption was created to allow strong encryption to be permitted for SSL Certificates for financial organizations, delivered through a technology called SGC (Server Gated Cryptography). The encryption export legislation was relaxed in 2000, and today no longer exists. 2000 also marked the start of all new browsers, including export versions, being capable of supporting strong encryption levels of 128 bit and above without the need for SGC.

What does SGC actually do?

The US cryptography export restrictions of the mid-1990s to 2000 meant some old export versions of the Internet Explorer and Netscape browsers were only capable of 40 bit SSL encryption levels. 40 bit encryption is breakable with today's computation power. SGC, or Server Gated Cryptography, was designed to force these weak encryption browsers versions to use stronger 128 bit encryption. The browsers that can benefit from SGC are limited to the exported versions of:

- Internet Explorer export browser versions from 3.02 to 5.01
- Netscape export browser versions from 4.02 to 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

For ease of reference the above list will be referred to as 'SGC browsers' in the remainder of this article.

Why SGC can be bad

1. Supporting the use of insecure software

Certificate Authorities, browser vendors, and responsible website owners should encourage clients to use the latest, patched software and not to facilitate the use of unsafe, insecure software. SGC will upgrade weak encryption but does not address the many security vulnerabilities that are present in the SGC browsers. Such exploits leave the SGC browsers vulnerable to attack via man in the middle attacks, botnet infection, keylogging exploits, and malware infection.

Major e-commerce providers such as PayPal actively speak out about the continued support for unsafe browsers being used for financial transactions, stating that it "is equal to a car manufacturer allowing drivers to buy one of their vehicles without seat belts."[1]

Encouraging users and encouraging website owners to educate their visitors to use the latest patched browser is not a new concept and has been pushed heavily for many years: https://www.thepaypalblog.com/wp-content/uploads/2008/07/__a_practical_approach_to_managing_phishing_april_2008.pdf

2. SGC browsers do not support the latest revisions to the SSL/TLS Protocols

By their very nature, SGC browsers are outdated and will not be able to support the ongoing revisions to the client side implementation of the SSL protocol, including fixes to new vulnerabilities and ongoing improvements to the protocol itself.

[1] PayPal Chief Information Security Officer Michael Barrett, http://www.eweek.com/index2.php?option=content&task=view&id=47667&pop=1&page=0&hide_js=1

The Need for SGC?

SGC supports the use of outdated, unsecure software.

SGC browsers do not support the latest revisions to the SSL/TLS protocols.

SGC browsers do not support the latest classification of SSL Certificates.

The usage of the browsers SGC is designed to help is negligible.

About GlobalSign

GlobalSign has been a trust service provider since 1996. Its focus has been, and always will be, on providing convenient and highly productive PKI Solutions for organizations of all sizes. Its core Digital Certificate solutions allow its thousands of authenticated customers to conduct SSL secured transactions, data transfer, distribution of tamper-proof code, and protection of online identities for secure email and access control. Vision and commitment to innovation led to GlobalSign being recognized by Frost & Sullivan for the 2011 Product Line Strategy Award. The company has local offices in the US, Europe and throughout Asia. For the latest news on GlobalSign visit www.globalsign.com or follow GlobalSign on Twitter (@globalsign).

3. SGC Browsers do not support the latest classification of SSL Certificates

In 2007 a new standard for SSL was ratified by members of the CA/B Forum – Extended Validation, or EV SSL. The new standard incorporates a number of specific identity verification requirements, which are represented in a different SSL Certificate structure. Browsers are able to identify EV SSL Certificates and represent the enhanced certificates by turning the browser address bar green and offering the user more trustworthy identity assurance. EV SSL was introduced some 7 years after the last SGC browser; as such, SGC browsers cannot offer the user the enhanced benefits of encountering an EV SSL Certificate. Website owners investing in EV SSL should also be encouraging visitors to upgrade to browsers capable of delivering the extra benefits they've invested in.

4. So few browsers now need SGC

SGC is only beneficial if the client is still utilizing a pre-year 2000 version of the SGC browser. In browser revision schedules, this represents archaic versions of the browsers. For example:

- In July 2012, Internet Explorer is on version 9. Microsoft has ceased all support and distribution of Internet Explorer 5.01 and previous versions for many years. As of December 2008, IE5 usage was down to 0.3% (www.w3schools.com).
- In 2007 Netscape discontinued its Netscape browser. As of September 2009, Netscape usage was down to 0.07% (www.statowl.com).
- Neither Netscape browsers nor IE 5.01 (or below) are available for download from their parent organizations.

While it is difficult to quantify, website owners should also consider the likelihood of a customer using an SGC browser being a serious customer. Consider how likely is it that a browser that's 10 years out of date is being used for legitimate transactions. And more importantly, do you want to do business / exchange sensitive information with a browser that is known to contain many security vulnerabilities and is not capable to using the latest SSL/TLS revisions?

GlobalSign's Stance on SGC

GlobalSign is one of the original trust providers on the Internet, and we take our role very seriously. We make significant contributions to the SSL ecosystem through tools, information and guidance, and our stance on SGC is in line with our mission to improve the security and usage of SSL for everyone.

We firmly believe that SGC Band-Aids over more serious vulnerabilities. The object of SGC is defeated if a potential attacker can exploit a security weakness in the browser or the protocol that is not related to encryption strength. Users who want stronger security must keep their software up to date, and if possible, upgrade to the latest browser versions so as to benefit from the security improvements offered in these more recent versions.

GlobalSign does not believe that SGC provides any real value in today's Internet ecosystem, and we discourage its use.

Some CAs charge a premium for SGC. This pricing policy suggests that historically there may have been a widespread market view that SGC was worthwhile and due to the limited number of CAs permitted to offer SGC, used it as a competitive advantage over non-SGC enabled CAs. We believe this period has now ended.

As we do not believe SGC gives any significant value and more importantly to adhere to security best practices, we no longer offer SGC as an option with our certificates. Instead we suggest partners and customers spend their time and effort encouraging upgrades to fix major security flaws. We also encourage you to enforce server side SSL best practices as this is much more effective at providing strong security than using SGC.

Check back frequently to the GlobalSign SSL Information Center as we'll be adding new resources and tools to help you achieve SSL implementation best practices.