GeoTrust

TechnologyBrief

The Truth About SSL Encryption Strengths

One of the common misconceptions in a Public Key Infrastructure (PKI) is that the strength of an SSL encryption session is a function of the digital certificate.

The fact is that the length of the Secure Sockets Layer (SSL) encrypted session is a function of the encryption algorithms contained in the browser and server. By applying an SSL certificate to a server (and associated domains), SSL is enabled via a series of communications and encryption/decrypting routines that already exit on browser programs and servers. The function of SSL certificates is to provide authentication of the identity of the server and to allow access to the security functionality of the web server itself.

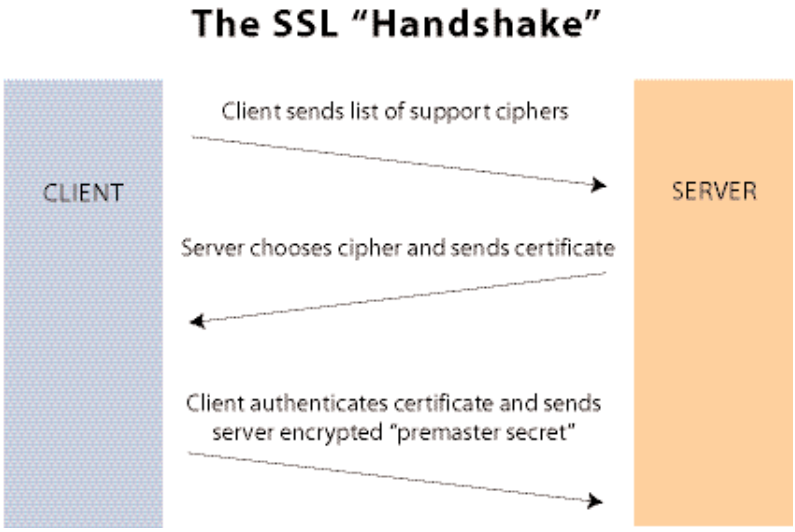
HOW DOES SSL ENCRYPTION WORK?

During an SSL transaction, the client browser sends a list of algorithms that it is willing to support to the server. The server chooses one of these algorithms (as long as one of these algorithms meets the server's minimum security requirements) and sends it back to the client browser along with a certificate containing the server's public key. The certificate serves the purpose of authenticating the server to the client. It then provides the public key that the client can then use to encrypt a pre-master-secret that is ultimately used to help create a symmetric key that is shared by both the client and server to encrypt traffic between themselves. The key item of note here is that the SSL encryption strength is not determined by the certificate, but is a function of the algorithms supported by the browser and server software.

During this SSL "handshake" -- the browser and web agree to use the strongest supporting cipher suite that meets the minimum requirements set-up on the application server -- whether it be 40-bit, 128-bit or even 256-bit. So, if both the browser and server support the AES-256 cipher suite, then the session will be encrypted at 256-bit. And, if both the browser and server support 128-bit encryption, the session will then be encrypted at 128-bit.

WHY DO CERTIFICATE PROVIDERS MARKET "PREMIUM" CERTIFICATES SUCH AS 256-BIT OR SERVER GATED CRYPTOGRAPHY (SGC) CERTIFICATES?

Certificate Authorities (CAs) have traditionally marketed SSL certificates as either 40-bit encryption strength or 128-bit encryption strength. This was due to the fact that prior to 2000, there were export restrictions on encryption software. Many of the browsers only supported 40-bit encryption. The US government recognized the fact that financial institutions would benefit from increased encryption strength, and allowed certain CAs to sell certificates that supported Server Gated Cryptography (SGC) technology. These types of certificates were designated as 128-bit encryption certificates by these CAs and certificate providers, and SGC support became synonymous with the 128-bit encryption capability.



However, in 2000, encryption export restrictions were removed and all of the major browser and software vendors began supporting 128-bit encryption in their browsers. Over time, the need for SGC became obsolete, and today, less than 1 percent of browsers need to be "bumped up" to 128-bit sessions (for more information see our Technology Brief -- *The Myth of Server Gated Cryptography*)."

Yet, despite the lifting of export restrictions, many CAs who supported SGC have continued to utilize the outdated naming convention in an effort to continue charging a premium for SGC or “step-up” certificates.

Today, this type of deceptive behavior now has some certificate providers introducing “premium” certificates at inflated prices that claim to support 256-bit encryption. Again, the truth of the matter is that if both the browser and server support the AES-256 cipher suite, then the session will be encrypted at 256-bit -- regardless of the certificate type.

HOW CAN I ENSURE THAT I’M USING THE “RIGHT” CERTIFICATE?
There really is no “right” kind of certificate -- since the certificate does not determine the encryption strength of the session between the browser and the server. When implementing certificates you should however make sure that your clients are using the latest modern browser versions and that your organization is using newer server operating systems that support at least 128-bit encryption.

Equally important is the trustworthiness of the certificate provider and the certificates they sell. A certificate from a trusted Certificate Authority provides a “stamp of approval” that says: "I stand by this User with this public key XYZ, and he is who he says he is because I've verified him." You should use certificates from trusted Certificate Authorities that:

- **Have certificates with 99% or higher browser compatibility and server recognition.** If a certificate is not recognized, the result is that the recipient may receive an error message or complaint from the browser, and consequently not trust either the server or the source.

- **Own their own root certificates.** Certificate providers who don’t own their own root certificates and issue certificates off chained roots or license roots from third parties may not be able to offer customers assurances of root stability during the lifetime of a certificate.

- **Are WebTrust compliant.** WebTrust is a comprehensive third-party auditing process which signifies that a CA meets the highest standards for issuing and managing digital certificates.

- **Have trustworthy domain and/or organizational ownership authentication procedures.** A certificate provider should conduct all the necessary checks to ensure that the identity data contained within a certificate is authentic and accurate.

- **Practice fair and accurate marketing and advertising of SSL certificates.** Take note of certificate providers that try to justify inflated prices for “premium” certificates that provide no added value in terms of encryption strength.

ABOUT GEOTRUST.
GeoTrust is a leader in identity verification and trust services for e-business. Its products include web security services for secure e-commerce transactions, identity verification, managed security services and TrustWatch (www.trustwatch.com), a free toolbar and search site that helps consumers recognize whether a site has been verified and is safe for the exchange of confidential information. With more than 100,000 companies in over 140 countries using its technology for online security, GeoTrust has rapidly become the second largest Certificate Authority in the world.

Visit www.geotrusteurorope.com or call +44 1622 764789 option 3 for more information.

GeoTrust®
6 Kings Row, Armstrong Road
Maidstone, Kent, UK
Phone: +44 1622 764789
E-mail: info@geotrusteurope.com
www.geotrusteurope.com