GeoTrust®

Technology Brief

The Myth of Server Gated Cryptography (SGC)

What is Server Gated Cryptography?

Some Certificate Authorities (CAs) market 128-bit certificates as a differentiator to sell "special" certificates known as "step up" or Server Gated Cryptography (SGC) certificates. At one time, SGC certificates served a purpose, but that purpose has since waned.

Today, almost all CAs support 128-bit certificates as the standard.

A Brief History

When the first CAs appeared in the 1990s, the US government had strict laws governing the export of strong cryptography, which was defined as anything over 40-bit encryption. That definition was later extended to include anything over 56-bit encryption. For the commercial world, strong cryptography was defined as a 128-bit encrypted SSL session. Commercial users of this technology were acutely aware that 128-bit SSL sessions were significantly stronger cryptographically than 40-bit SSL sessions and wanted to offer strong encryption to their customers, vendors, and employees. The following table shows the dramatic difference between the cipher strength of a 40-bit SSL session and a 128-bit SSL session based on the attackers' ability.

Key Length	Individual Attacker	Small Group	Academic Network	Large Company	Military Intelligence Agency
40-bit	weeks	days	hours	milliseconds	microseconds
56-bit	centuries	decades	years	hours	seconds
128-bit	infeasible	infeasible	infeasible	infeasible	millennia

Table: Average times needed to search half the symmetric key-space based on 1997 estimates using a brute force attack method (worse case scenario would be twice as long.

A Solution to the Problem - Server Gated Cryptography

During the 1990s the US government allowed selected companies to enable strong cryptography with a new technology called Server Gated Cryptography (SGC). Server Gated Cryptography allowed selected 40-bit and 56-bit web browsers to automatically increase, "bump up", their web sessions to the stronger 128-bit SSL sessions. SGC was the perfect technology given the US government's export policy at the time.

A Change in U.S. Export Policy

In early 2000, the Bureau of Export Administration (BXA) dropped most of the restrictions that prohibited US companies from shipping high grade encryption products. This new policy allowed both web server and web browser vendors to ship 128-bit SSL enabled products both domestically and internationally.

The Irrational Need for Server Gated Cryptography (SGC)

After the BXA dropped the 128-bit SSL enable software restrictions, the need for SGC began to fade away. As of January 2004, an estimated 85% of browsers in use were shipped with strong encryption by default [IE 5.5, IE 6.0, Mozilla 1, Opera 7.0, Safari] (http://www.onestat.com/html/aboutus_pressbox26.html).

Additionally, conservative figures would suggest that 2/3 of the remaining 15% of browsers were shipped with the ability to enable 128-bit SSL. That leaves only 5% of the current web browsers unable to connect with a strong 128-bit SSL connection. Finally, the upgrade rate for these (15%) older browsers should maintain the current trend of 5.3% for the next two years. This will result in a SGC having almost 0% marginal value with in the next several months.

A more fundamental problem, however, is that these older browsers have security flaws. Since the primary point of SGC is to strengthen the security of the SSL session, this object is completely defeated if a potential attacker can exploit a security weakness in the browser. In fact, if commercial entities want strong security, they must upgrade to the latest browser versions; there are literally hundreds of security vulnerabilities in IE 5.01 and IE 5.5 that have been fixed in subsequent versions of the browsers. IE 5.0 also only supports SSLv1 and SSLv2 (since TLS did not exist at the time of development).

These protocols have at least two known flaws (http://www.meer.net/~ericm/papers/ssl_servers.html#1.2):

1. The downgrade attack allows an active attacker (one who can change bits in the messages between client and server) to force an SSLv2 session to use weaker cipher suites than would ordinarily be negotiated.

2. The truncation attack allows an attacker to stop the SSLv2 session without the server or client knowing that the session was stopped by an attacker instead of by the other party. If the attacker knows something about the structure of the message and how it is sent in the SSLv2 packets, he can use the truncation attack to change the meaning of the message.

Conclusion

In summary, for the sake of security it is best for us to encourage the migration to more modern browsers to facilitate truly secure web experiences; continuing to offer SGC simply maintains the illusion that web sessions using these certificates are secure when, in fact, the older browsers that use SGC represent a significant security risk. It is recommended that customers using IIS 5 and up, detect a browser connection's strength by exposing an https key size variable with an ASP server object. As such it is possible to include an ISAPI or ASP page on a server that would re-direct the customer to a site helping them get updated.

GeoTrust®
European Headquarters
6 Kings Row
Armstrong Road, Maidstone
Kent, ME15 6AQ, United
Kingdom
Phone: +44 1622 764789
Fax: +44 870 1322080
E-mail: info@geotrusteurope.com
www.geotrusteurope.com