SSL Fingerprint

An SSL fingerprint

GRC has created HTTPS Fingerprints. This service allows you to check whether or not your enterprise is performing MITM on the SSL secured site that you are trying to reach.

It compares the certificate fingerprint to what you would receive to the fingerprint that they receive by going direct. If they are the same, the certificate is authentic and you have no problem. If they are different, then it is likely that someone is performing MITM on your SSL connection.

Anyone examining an SSL certificate (like this page or your web browser) can create a “cryptographic hash” or “digest” of the certificate's contents. Cryptographic hashes are complex mathematical algorithms which carefully process every single bit of what they “digest.” They have the amazingly property that if even one bit inside the certificate is changed, an average of half of the fingerprint's hash bits will change in response! In other words, when such a cryptographic hash is used to “fingerprint” a certificate any change, no matter how small, will result in a COMPLETELY different fingerprint.

Fingerprints offer incredibly sensitive and strong detection of anything changed anywhere in a security certificate. Certificate fingerprints were originally based upon the “MD5” (Message Digest 5) hashing algorithm. But over time researchers found MD5 to be a bit weak in some special cases which might have been exploitable. So the entire industry (and this web site) has switched over to using the newer, stronger and even more secure “SHA1” (Secure Hashing Algorithm 1) hashing algorithm.

GRC has created HTTPS Fingerprints. This service allows you to check whether or not your enterprise is performing MITM on the SSL secured site that you are trying to reach. It compares the certificate fingerprint to what you would receive to the fingerprint that they receive by going direct. If they are the same, the certificate is authentic and you have no problem. If they are different, then it is likely that someone is performing MITM on your SSL connection.

From:
http://docs.intenogroup.com/glossary/ - **Inteno Glossary**

Permanent link:
http://docs.intenogroup.com/glossary/s/ssl_fingerprint

Last update: **2018/08/10 18:16**