What Is TLS 1.2 and why should we still care?

The internet is the most ambitious communication and data transference technology ever created, but Gigamon cautions that with its advance come several challenges.

“As we improve our ability to share large amounts of information between computers, servers and other digital devices, the risk of that data falling into unauthorised hands increases significantly,” says George Tsoukas, Gigamon’s ANZ Country Manager.

To prevent eavesdroppers, hackers and other cyber criminals from accessing sensitive data as it moves through the internet, various cryptographic protocols have been introduced. The most famous of these are Secure Socket Layers (SSL) and Transport Layer Security (TLS).

SSL has long been defunct, replaced by TLS and its subsequent versions. And with TLS 1.0 and 1.1 deprecated as of the end of 2020, organisations and web hosts wishing to ensure data safety need to move to support TLS 1.2 across all of their deployments.

But what is TLS 1.2, and how does it work? To answer that, let’s first take a quick look at the history of cryptographic protocols.

SSL 1.0, 2.0, and 3.0

Back in 1995, when the internet was still figuring itself out, Netscape decided to address growing concerns over security by creating a form of encryption that would allow data to travel safely without the risk of being intercepted. SSL 1.0 was flawed, and never saw general release, but SSL 2.0 followed shortly afterwards, and was then superseded by the much improved SSL 3.0.

This final SSL version became the standard for internet encryption for nearly two decades. Unfortunately, as technology improved, so did the capabilities of various online threat actors. In late 2014, the Google Security Team detected a major security flaw in SSL 3.0, necessitating a new approach to communication encryption. TLS was the solution.

TLS

Originally envisioned as another SSL protocol upgrade, TLS instead grew into something unique enough to deserve its own designation. And while TLS 1.0 was different enough from SSL as to make interoperability impossible, it was designed with a mechanism allowing it to fall back on SSL 3.0 when needed — at reduced security effectiveness.

TLS 1.0 was followed by TLS 1.1, improving its security offering and addressing a number of newly discovered weaknesses in the previous version. And TLS 1.1 was an effective cryptographic protocol for several years. But as with all of the previous protocols, eventually it became outdated and incapable of supporting modern cryptographic algorithms.

TLS 1.2 addressed these issues while also including increased protection against newly discovered security vulnerabilities.

What Is TLS 1.2?

TLS 1.2 is simply an upgraded form of TLS 1.1. It was released in 2008, offers improved security, and was designed for both high performance and improved reliability. To accomplish this, it relies on a combination of symmetric and asymmetric cryptography.

More specifically, TLS 1.2 replaces the MD5/SHA-1 combination in the digitally signed element with a single hash, ensuring increased security in negotiation during the handshake.

At the same time, it provides improvements to both the client’s and the server’s ability to designate algorithms for the hash and the signature. TLS 1.2 also supports increased authentication encryption and adds TLS extensions and AES cipher suites.

TLS 1.2 was a definite improvement over its predecessors. But, as anyone who works with technology knows, you can’t stop progress.

In 2018, the Internet Engineering Task Force (IETF) finalised and published TLS 1.3, making it the most advanced and secure cryptography protocol available. TLS 1.3 improved web performance and security by increasing TLS handshake speed, improving load times, and removing obsolete and insecure TLS 1.2 cipher suites, such as the RSA key exchange algorithm, the RC4 stream cipher, the CBC mode cipher, and others.

Simply put, TLS 1.3 is designed to secure against every known TLS 1.2 vulnerability and simplify the configuration process. So, with TLS 1.3 currently the obvious best choice for online data encryption, why should you still care about TLS 1.2?

The TLS 1.2 deadline

By the end of 2020, TLS versions 1.0 and 1.1 were no longer supported. That means that websites that don’t support TLS 1.2 or higher are now incapable of creating secure connections.

Attempting to access those sites using a mainstream web browser (such as Google Chrome, Apple Safari, Mozilla Firefox or Microsoft Edge) will return a “Secure Connection Failed” error message. Similarly, e-commerce sites required to accept credit card payments and remain PCI compliant must use TLS 1.2 or higher.

The overwhelming majority of websites currently support TLS 1.2 and will not be affected by the loss of TLS 1.0 and 1.1. That said, there may still be a handful of sites that have not yet upgraded. By delaying support for TLS 1.2, these sites put themselves, and their clients, at significant risk.

Dangers of not upgrading to TLS 1.2

TLS 1.2 isn’t simply the obvious next step for Transport Layer Security, it’s an actual solution to serious security threats.

In recent years, both TLS 1.0 and 1.1 have become vulnerable to various advanced cryptographic threats, including BEAST and POODLE. Both of these threats allow attackers to take advantage of TLS security weaknesses to recover potentially sensitive data.

These are by no means the only threats facing outdated TLS protocols. Organisations that resist upgrading put themselves and their users at risk of data theft.

Beyond the dangers of insecure data, non-1.2-compliant sites will also suffer significant traffic loss. As visitors attempt to use standard browsers to access these sites, they will encounter the aforementioned error message, essentially deflecting them away from accessing the desired content.

This means that these sites will be unable to interact with potential customers, or negatively impact on an organisation’s credibility. Those who see ‘Secure Connection Failed’ are much less likely to trust that particular site, or the organisation behind it, in future sessions. Outdated TLS versions have also been linked to lower rankings in Google search-engine results pages.

Finally, e-commerce sites that do not have TLS 1.2 support risk up to $US100,000 in non-compliance fines and will likely be unable to process payments.

How to upgrade to TLS 1.2

Unfortunately, there is no single button or process to ensure TLS 1.2 compatibility; depending on the platform and software solutions currently in use, the process may be extremely simple or unnervingly complex.

Start by identifying which systems may need to be upgraded and which don’t. Reviewing local software, legacy systems, and online stores and payment gateways may reveal TLS vulnerabilities.

Platforms and connections that may need to be upgraded to TLS 1.2 include internet information services, web servers, e-commerce applications, and .Net Framework. Thankfully, e-commerce third-party support will likely have already been upgraded.

Working closely with IT and security teams is vital, as is creating a detailed migration plan. Upgrading to support TLS 1.2 is essential, particularly as TLS 1.0 and 1.1 are deprecated. But for the best possible protection, upgrade to TLS 1.3 and regularly patch and upgrade TLS software to ensure protection against new threats.

As internet information technologies evolve, so do the threats that they face. The coordinated move to TLS 1.2 is an effective solution to help ensure optimal data security, both for organisations and customers.

Gigamon has a number of tools that help to keep information secure, specifically when it comes to SSL/TLS decryption. Learn how our bundled GigaSMART® SSL/TLS Decryption apps will help you to efficiently decrypt and re-encrypt traffic and meet privacy and compliance requirements — meaning not only greater security, but fewer headaches for everyone.

###

Contacts

David Frost
(02) 7903 9567
mailto: david.frost@prdeadlines.com