Why Use TLS 1.3? | SSL and TLS Vulnerabilities

TLS 1.3 improves over previous versions of the TLS (SSL) protocol in several important ways.

TLS 1.3 Learning Objectives

After reading this article you will be able to:

- Understand why TLS 1.3 is faster and more secure than TLS 1.2
- Learn about TLS vulnerabilities

Related Content

How SSL Works

Keyless SSL

SSL Certificate Types

SSL Handshake

What is an SSL Certificate?

What is the difference between TLS 1.3 and TLS 1.2?

TLS 1.3 is the latest version of the TLS protocol. TLS, which is used by HTTPS and other network protocols for encryption, is the modern version of SSL. TLS 1.3 dropped support for older, less secure cryptographic features, and it sped up TLS handshakes, among other improvements.

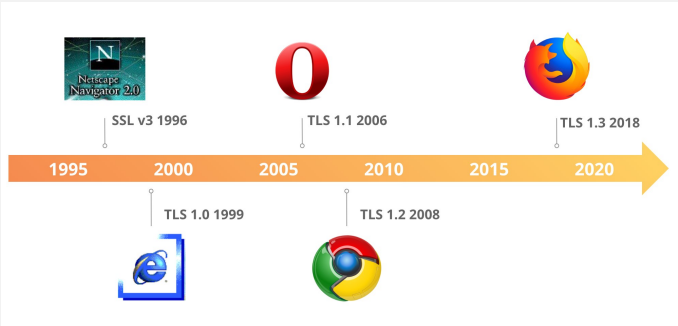
For context, the Internet Engineering Task Force (IETF) published TLS 1.3 in August 2018. TLS 1.2, the version it replaced, was standardized a decade previous, in 2008.

What are the advantages of using the latest TLS version?

In a nutshell, TLS 1.3 is faster and more secure than TLS 1.2. One of the changes that makes TLS 1.3 faster is an update to the way a TLS handshake works: TLS handshakes in TLS 1.3 only require one round trip (or back-and-forth communication) instead of two, shortening the process by a few milliseconds. And in cases when the client has connected to a website before, the TLS handshake will have zero round trips. This makes HTTPS connections faster, cutting down latency and improving the overall user experience.

Many of the major vulnerabilities in TLS 1.2 had to do with older cryptographic algorithms that were still supported. TLS 1.3 drops support for these vulnerable cryptographic algorithms, and as a result it is less vulnerable to cyber attacks.

Why are there different TLS versions?



Updates are a natural part of software development. Computer systems are so complex that it is inevitable that they'll need repairs or improvements to be more efficient or more secure. Any software is going to have vulnerabilities – flaws that an attacker can exploit.

In the case of TLS, parts of the protocol carried over from its early days in the 1990s resulted in several high-profile vulnerabilities persisting in TLS 1.2. Additionally, those who work on developing the protocol are continually identifying inefficiencies that can be eliminated.

How do new versions of TLS get developed?

The IETF is in charge of developing TLS, codifying feedback and ideas via a document known as a "Request For Comments," or an RFC. Most protocols on the Internet are defined via RFCs. All RFCs are numbered; TLS 1.3 is defined by RFC 8446.

Once a new version of a protocol is released, it's up to browsers and operating systems to build support for those protocols. All operating systems and browsers should want better performance and security, so they have incentive to do so. However, it can still take some time for support for updated protocols to be widespread, especially because private businesses and consumers may be slow to adopt the latest versions of browsers, applications, and operating systems.

What is a vulnerability?

A software vulnerability is a flaw in the design of a computer program that an attacker can take advantage of to perform malicious activity or gain illicit access. Essentially, vulnerabilities are inevitable in computer systems, just as it is practically impossible to build a bank that is impregnable to highly determined bank robbers.

The security community documents and catalogues vulnerabilities as they are discovered and described. Known vulnerabilities are assigned a number, like CVE-2016-0701. (The first number is the year when it was discovered.)

What are some important SSL and TLS vulnerabilities?

A number of outdated cryptography features resulted in vulnerabilities or enabled specific kinds of cyber attacks. Here is a non-exhaustive list of TLS 1.2 cryptography weaknesses, and the vulnerabilities or attacks associated with them.

- RSA key transport: Doesn't provide forward secrecy
- CBC mode ciphers: BEAST and Lucky 13 attacks
- RC4 stream cipher: Not secure for use in HTTPS
- Arbitrary Diffie-Hellman groups: CVE-2016-0701
- Export ciphers: FREAK and LogJam attacks

A lot of TLS 1.2 features have been removed in addition to those listed above. The idea is to make it impossible for someone to enable the vulnerable aspects of TLS 1.2. This is somewhat like when the government made it illegal to manufacture new cars without seatbelts: The goal of the regulations was for seatbelt-less cars to be phased out so that everyone would be safer. For a while, drivers could still choose to use older car models and be less safe, but eventually those more dangerous cars disappeared from the roads.

Does Cloudflare support TLS 1.3?

Cloudflare prioritizes supporting all the latest, most secure versions of networking protocols. Cloudflare immediately offered support for TLS 1.3; in fact, Cloudflare supported TLS 1.3 back in 2016, before the IETF finished fine-tuning it.

For more technical details on TLS 1.3 and how it differs from TLS 1.2, see this detailed look at TLS 1.3 by Cloudflare Head of Cryptography Nick Sullivan.

About SSL
What is SSL?
What is TLS?
How SSL Works

Contact Sales:

+1 (888) 99 FLARE

About HTTPS
What is HTTPS?
Why Use HTTPS?
HTTP Security Gaps
Connection Not Private

About Encryption
What is Encryption?
Public Key Encryption
Asymmetric Encryption
Lava Lamp Encryption
Cryptographic Key
What is a Session Key?

SSL Glossary
What is Mixed Content?
SSL Handshake
What is an SSL Certificate?
SSL Certificate Types
Why Use TLS 1.3?
What is SNI?
What is Encrypted SNI?
What is Domain Spoofing?

Learning Center Navigation
Learning Center Home
DDoS Learning Center
CDN Learning Center
DNS Learning Center
Performance Learning Center
Security Learning Center
Serverless Learning Center
Bots Learning Center
Cloud Learning Center
Access Management Learning Center
Network Layer Learning Center
Privacy Learning Center
Video Streaming Learning Center