Internet to TLS 1.3: Where have you been all my life

March 28 2018, by Nancy Owano

Credit: CC0 Public Domain

The Internet Engineering Task Force (IETF), which is the premier Internet standards body, has given its nod of approval for something that will make the Web more secure. It is called Transport Layer Security version 1.3.

Criminals, at least for now, and until the more persistent troublemakers start trying out workarounds, should feel badly. But good luck to them if they do persist. They will need it.

"All in all, TLS 1.3 is a serious boost to Internet security, being considered nigh impossible to crack, at least with today's resources," said Catalin Cimpanu in *Bleeping Computer*. (TLS stands for Transport Layer Security – works by creating a secure connection between client and server.)

Jon Fingas in *Engadget* pointed out that "Old encryption algorithms are no longer options, so a hacker can't force the use of a legacy format to break security. Evildoers also can't reuse decryption keys for future transactions."

Kieren McCarthy, *The Register*, called TLS 1.3 "A much-needed update to internet security" that finally passed at the IETF.

TLS Protocol Version 1.3 is a new protocol, a security layer, and its purpose is to protect the web from unauthorized access. TLS 1.3, then, becomes the standard method in which a client and server establish an encrypted communications channel across the Internet, said *Bleeping Computer*, aka HTTPS connections.

Christina Cardoza, news editor of *SD Times*, said, "The latest version is more than four years in the making with 28 versions created during that time."

More specifically, the decision, said Cimpanu, came after four years of talks and 28 protocol drafts. The 28th was selected as the final version. The document "The Transport Layer Security (TLS) Protocol Version 1.3 draft-ietf-tls-tls13-28" is dated March 20 and the expiration date is September 21.

The abstract stated, "This document specifies version 1.3 of the Transport Layer Security (TLS) protocol. TLS allows client/server applications to communicate over the Internet in a way that is designed

to prevent eavesdropping, tampering, and message forgery."

McCarthy reported that "TLS 1.3 won unanimous approval (well, one 'no objection' amid the yeses), paving the way for its widespread implementation and use in software and products from Oracle's Java to Google's Chrome browser."

TLS 1.3 is secure in what ways?

First, "The new protocol aims to comprehensively thwart any attempts by the NSA and other eavesdroppers to decrypt intercepted HTTPS connections and other encrypted network packets," said *The Register*.

Second, "it ditches many of the older encryption algorithms that TLS 1.2 supports that over the years people have managed to find holes in," said McCarthy. "The older crypto-systems potentially allowed miscreants to figure out what previous keys had been used (called "non-forward secrecy") and so decrypt previous conversations."

Fingas in *Engadget* weighed in on the benefits of the new protocol, in that it "involves both shrinking the window of opportunity for intruders and preventing them from recycling code."

Fingas wrote, "To begin with, the handshake between your client and the server will invoke encryption sooner, reducing the amount of unprotected data both sides send. Old encryption algorithms are no longer options, so a hacker can't force the use of a legacy format to break security. Evildoers also can't reuse decryption keys for future transactions."

Then there are the counterarguments. What if "good guys" need to break in? That is the sort of argument behind those who were unhappy. McCarthy reported, "banks and businesses complained that, thanks to

the way the new protocol does security, they will be cut off from being able to inspect and analyze TLS 1.3 encrypted traffic flowing through their networks, and so potentially be at greater risk from attack."

McCarthy said, "An effort to effectively insert a backdoor into the protocol was met with disdain and some anger by internet engineers."

The backdoor proposal did not move forward.

Bleeping Computer's Catalin Cimpanu said another plus about TLS 1.3 is that it is "faster at negotiating the initial handshake between the client and the server, reducing the connection latency that many companies cited when justifying not supporting HTTPS over HTTP."

Check out *The Register*'s walk-through of what the process has been like, compared with what it will be like in the new 1.3.TLS. In short, the 1.3 speeds up the process. Steps are bundled.

What's next? Cimpanu said that "Browsers like Chrome, Edge, Firefox, and Pale Moon have already rolled out support for earlier versions of the TLS 1.3 draft, and are now expected to update this support to the official standard."

Placing all this in perspective, Fingas said that "This certainly won't put an end to online threats, but it could stop attacks that take advantage of basic flaws in how the internet works."

More information: The Transport Layer Security (TLS) Protocol Version 1.3, tools.ietf.org/html/draft-ietf-tls-tls13-28