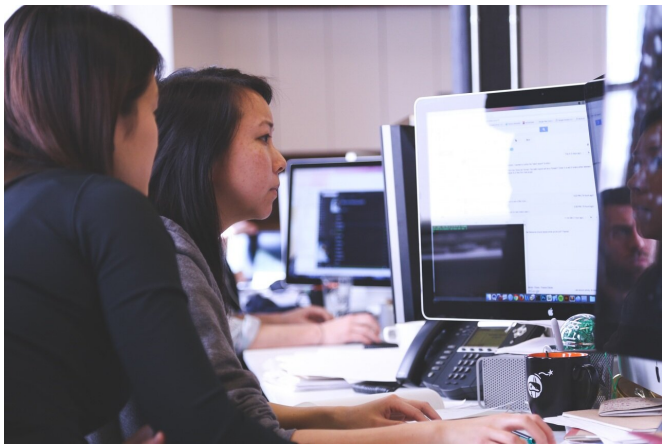
The story behind that little padlock in your browser

24 March 2020, by Jon Cartwright, From Horizon Magazine



'Transport layer security' means your internet activities are secure on three fronts - authentication, encryption and integrity. Credit: Pxhere, licensed under CC0

Whenever you see a little padlock in the address bar of your internet browser, as well as when you use apps, email and messaging, you're relying on something called 'transport layer security' or TLS. It's a protocol that keeps us safe online.

Behind that little padlock is cryptographic code that guarantees the security of data passing between you and, for example, the website you are looking at.

In fact, TLS guarantees security on three fronts: authentication, encryption and integrity. Authentication, so that your data goes where you think it is going; encryption, so that it does not go anywhere else; and integrity, so that it is not tampered with en route.

"It's the most popular security protocol on the internet, securing essentially every e-commerce transaction," Eric Rescorla, chief technology officer at US technology company Mozilla, told Horizon over email.

In the two decades leading up to 2018, there were five overhauls of TLS to keep pace with the sophistication of online attacks. After that, many experts believed that the latest incarnation, TLS1.2, was safe enough for the foreseeable future, until researchers such as Dr. Karthikeyan Bhargavan and his colleagues at the French National Institute for Research in Digital Science and Technology (INRIA) in Paris came along.

Scaffold

As part of a project called CRYSP, the researchers had been working on ways to improve the security of software applications. Usually, software developers rely on TLS like a builder relies on a scaffold—in other words, they take its safety for granted.

To improve security at the software level, however, Dr. Bhargavan and colleagues had to thoroughly check that the underlying assumptions about TLS1.2—that it had no serious flaws—were justified.

"At some point, we realised they weren't," he said.

After discovering some shaky lines of code, the researchers worked with Microsoft Research and took on the role of hackers, performing some simulated attacks on the protocol to test the extent of its vulnerability. The attacks revealed that it was possible to be a 'man in the middle' between an internet user and a service provider, such as Google, and thereby steal that user's data.

"It would have to be a fairly complex sequence of actions," explained Dr. Bhargavan. "Typically, the person in the middle would have to send weird messages to each actor to lure them into a buggy part of the code."

"If, as the person in the middle, I was successful, I could potentially steal someone's payment details," he continued. "Or I could pretend to be Apple or

Google, and download (insert) malware via a software update to get access to people's computers."

Serious threat

Such a hacker would need great expertise and computational power, that of a government agency, for example, as well as access to some of the physical infrastructure close to the key actors. Nevertheless, the Internet Engineering Task Force (IETF), an international organisation promoting internet standards, judged the threat to be sufficiently serious to warrant a new version of the cryptographic protocol.

Dr. Bhargavan points out that he was far from the only computer scientist to prompt the revision. There were four or five other research groups unearthing problems with the current protocol, pushing one another along, he says, in a healthy rivalry.

Still, he says that his group discovered some of the most surprising flaws in TLS1.2, which he believes may have been the 'final nails in the coffin' for the protocol.

His group was also part of a broad collaboration within the internet community, overseen by an IETF working group, to construct the more secure, and man-in-the-middle-proof successor that is TLS 1.3, using modern algorithms and techniques. "Dr. Bhargavan was a key player in that effort," said Rescorla who oversaw TLS at the IETF at the time of the work.

TLS 1.3 was officially launched in August 2018. Since then it has been implemented by major internet browsers such as Mozilla Firefox and Google Chrome.

So how much safer are internet users as a result?

Human error

It is true that for most online security breaches, TLS is not to blame. Usually, personal data gets into the wrong hands because of bugs in software—what Dr. Bhargavan's group was working on to begin with—or human error.

But Dr. Bhargavan believes there is reassurance in knowing that the underlying protocol is secure. "It's not everything, but so long as you click that padlock you have some confidence about safety—it's the most basic thing," he said.

Besides, internet users are not only worried about hackers. Since 2013, and the leaks of Edward Snowden, a former employee of a US National Security Agency contractor, many people are concerned about the amount of personal data amassed by state intelligence and large enterprises.

Designed with the Snowden revelations in mind, TLS 1.3 closes the door to some types of this pervasive network-based monitoring through its encryption of both user data and metadata. It also prevents retrospective decryption—one of the previous version's weaknesses.

There was a long discussion in the IETF working group about whether preventing surveillance was one of the goals of TLS, says Dr. Bhargavan. "And the answer was ultimately in the positive," he said.

Now Dr. Bhargavan is returning to the issue of software security. He believes the majority of remaining vulnerabilities can be eliminated at the design stage.

Verified

To do this, he and his colleagues are constructing a library, HACL*, of fully verified cryptographic code, which other developers can draw on when building new software. In this project, known as CIRCUS, they are also creating an easy-to-follow reference paradigm that tells developers how to put software together without introducing security glitches.

The resultant high-assurance software has already been taken up by developers at Mozilla and Microsoft, among others. "We want everyone to be following these techniques," Dr. Bhargavan said.

Ultimately, his goal is not to secure everything online, but to find the safest spots within our highly

complex computer systems. "I don't think we will ever get to a point where everything is verified," he said, 'but we can find the most secure basket in which we can put our keys and passwords and financial data."

Provided by Horizon: The EU Research & Innovation Magazine