How Triple Handshake, Freak and Logjam discoveries contributed to a broader effort to safeguard the Internet

November 19 2015, by Allison Linn

When researchers from Microsoft and the French research organization INRIA discovered and helped fix three serious security vulnerabilities in a popular system for enabling secure Internet transactions, many people assumed that finding those flaws had been their primary goal.

That wasn't exactly the case. Instead, the discovery of the Triple Handshake, Freak and Logjam vulnerabilities was a beneficial byproduct of a much larger ambition. The researchers have for several years been working through the Microsoft Research-Inria Joint Centre to create a much more secure method for implementing the Transport Layer Security, or TLS.

That's a system that most of us are using many times a day – whether we realize it or not – to securely do things like buy a book, pay a bill or connect to a corporate network.

"We did not find them because we were looking for attacks. We found them as a side effect," said Cedric Fournet, a principal researcher at Microsoft Research Cambridge and one of the project's lead researchers.

This week, the Microsoft and INRIA researchers are making public two sets of code that are part of that more extensive Internet security project, which is called MiTLS.

The long-term goal of MiTLS is to create a system they can mathematically prove to be secure, because of an absence of attacks against it.

The code releases are aimed at helping academic and security experts create their own more secure implementations of TLS.

In addition, the researchers also have been working closely with security experts from throughout the industry who are building the next

generation of the overall TLS protocol, which serves as the basis for the implementations that companies use to secure communications between servers and web browsers. That version of the protocol, which is due out sometime next year and will be implemented over the next several years, is expected to do a much better job of safeguarding our data and personal information from prying eyes.

"To me that's the most exciting aspect of this," said Karthikeyan Bhargavan, a research team leader at INRIA who is a key researcher on MiTLS project. "We're actually influencing the next generation."

A short-term project gets bigger

When Bhargavan and Fournet first started work on the project that would eventually become MiTLS, Bhargavan said they expected to do a short-term academic research project looking at how some of academic security implementations of TLS might work on real systems that people were actually using on the Internet.

The idea, Fournet said, was to address the difference between the theoretical security models that were being created in research labs and the practical applications that actual consumers were using every day.

"What we really wanted to do was bridge the gap between the two," Fournet said.

The researchers soon found that the security issues were much bigger than they expected, and Bhargavan said what they thought would take six months turned into a much larger and more ambitious project.

The researchers have now been working together for several years. Along the way, they've uncovered several major vulnerabilities that could have allowed bad actors to access personal data, including the

Triple Handshake, Freak and Logjam attacks.

The vulnerabilities the Microsoft/INRIA team discovered and helped fix highlighted the fact that many companies were using outdated cryptographic algorithms in their TLS implementations, leaving their customers more open to attack. Fournet said that's because upgrading to a new set of algorithms can be costly and time-consuming, and may result in elements of a system not working properly or running more slowly.

In addition, Bhargavan said, many companies didn't see the benefits of upgrading until some of the larger vulnerabilities were exposed.

Fournet and Bhargavan are hoping that the work they have done to improve TLS, and to offer more secure ways of implementing it, will allow companies to more proactively protect people from attacks. That's much better than having to retroactively patch vulnerabilities that are found in the older versions.

"The general goal is to improve the overall trust in web security," Fournet said.

More information: Download the MiTLS open source tools, which are available on GitHub under Apache 2.0

Provided by Microsoft