Attacking and Proving TLS 1.3 implementations

Karthikeyan Bhargavan

December 2, 2015

The Transport Layer Security (TLS) protocol is widely used to provide secure channels for the Web (`https`), email, and Wi-Fi networks. In recent years, several high-profile attacks on the TLS protocol and its implementation have been published. Many of these attacks were discovered by a collaborative research effort between Microsoft Research and INRIA called miTLS.

The primary goal of the miTLS project (`mitls.org`) is to build a verified implementation of TLS [BFK+13] with strong cryptographic proofs of security [BFK+14]. A key focus of miTLS has been to verify the protocol as it is used in practice, and hence to account for all the dirty details and corner cases of the protocol. The miTLS library is probably the largest cryptographic protocol implementation to have a security theorem.

Aside from developing cryptographic proofs, miTLS has also led to the discovery of important attacks such as the Triple Handshake attacks on the protocol [BDLF+14] and the SKIP and FREAK attacks on TLS implementations [BBDL+15]. These attacks have had significant real-world impact; they led to security updates to all major TLS libraries and web browsers.

All these published results of miTLS are for TLS versions up to 1.2, but now a new and substantially different version of the protocol is in the process of being standardized as TLS 1.3. The next major goal of the miTLS project is to build a verified reference implementation of TLS 1.3 in the F* programming language [SHK+16] and to develop an analysis framework that can find attacks in the new protocol and its fresh implementations. Our goals are ambitious and we have a large team of researchers from INRIA and Microsoft Research who will work on it. We expect to have many sub-projects suitable for masters internships, and some long-term projects for PhD students.

We seek brilliant students who are interested in learning new software verification techniques and applying them to develop new security theorems and to discover new attacks on real-world cryptographic protocols such as TLS 1.3. The student intern will be expected to contribute to a clearly defined sub-task, hopefully leading to a publication in a leading research conference. Students with a strong background in programming languages, or formal verification, or cryptography are particularly encouraged to apply.

References

[BBDL+15] Benjamin Beurdouche, Karthikeyan Bhargavan, Antoine Delignat-Lavaud, Cédric Fournet, Markulf Kohlweiss, Alfredo Pironti, Pierre-Yves Strub, and Jean Karim Zinzindohoue. A messy state of the union: Taming the composite state machines of tls. In *IEEE Symposium on Security & Privacy 2015 (Oakland'15)*, 2015. Distinguished Paper Award.

[BDLF+14] Karthikeyan Bhargavan, Antoine Delignat-Lavaud, Cédric Fournet, , Alfredo Pironti, and Pierre-Yves Strub. Triple handshakes and cookie cutters: Breaking and fixing authentication over tls. In *IEEE Symposium on Security & Privacy (Oakland)*, 2014.

[BFK+13] Karthikeyan Bhargavan, Cédric Fournet, Markulf Kohlweiss, Alfredo Pironti, and Pierre-Yves Strub. Implementing tls with verified cryptographic security. In *IEEE Symposium on Security & Privacy (Oakland)*, 2013.

[BFK+14] Karthikeyan Bhargavan, Cédric Fournet, Markulf Kohlweiss, Alfredo Pironti, Pierre-Yves Strub, and Santiago Zanella-Béguelin. Proving the tls handshake secure (as it is). In *CRYPTO*, 2014. Long version at Cryptology ePrint Archive, Report 2014/182: `https://eprint.iacr.org/2014/182`.

[SHK+16] Nikhil Swamy, Ctlin Hricu, Chantal Keller, Aseem Rastogi, Antoine Delignat-Lavaud, Simon Forest, Karthikeyan Bhargavan, Cdric Fournet, Pierre-Yves Strub, Markulf Kohlweiss, Jean-Karim Zinzindohoue, and Santiago Zanella-Bguelin. Dependent types and multi-monadic effects in F*. In *ACM Symposium on Principles of Programming Languages (POPL'16)*, 2016.