J Cryptol (2021)34:24
https://doi.org/10.1007/s00145-021-09386-z

Journal of
CRYPTOLOGY

Introduction to the Special Issue on TLS 1.3

Colin Boyd
NTNU, Trondheim, Norway
colin.boyd@ntnu.no

Communicated by Kenny Paterson

Received 29 December 2020 / Revised 31 December 2020 / Accepted 1 January 2021
Online publication 24 May 2021

The Transport Layer Security (TLS) protocol is known as one of the most important and widely-used security protocols. It emerged in the 1990s from the proprietary SSL protocol, originally designed for securing web traffic in the Netscape browser. Since its first version the TLS protocol has seen a series of evolutions and a great deal of scrutiny from both cryptographers and security practitioners. As well as remaining the standard method to protect channels between web browsers and servers, TLS is now widely used to secure many other network services.

The latest version of the TLS protocol, TLS 1.3, was published as an Internet Proposed Standard in 2018 [3]. Development of the standard progressed in a way that differed from earlier TLS versions, in what Paterson and van der Merwe [2] call a *proactive* process in contrast to a *reactive* process. What they mean by this is that TLS 1.3 was developed in cooperation with the academic community, employing formal models to obtain high assurance of security *before* the standard was published. Earlier updates to the standard were mainly focussed on fixing security problems that had been discovered *after* publication.

It is something of a paradox that as technology advances, providing us with ever increasing computational capabilities, the demand for more efficient protocols increases as well. Thus, in addition to providing a scientific basis for security, a driving goal for the TLS 1.3 standard was to improve efficiency of the protocol in a number of ways. These ways included measures such as simplifying the negotiation of protocol versions and cipher suites, reducing the number of handshake messages, and allowing faster resumption of previously used channels.

Three of the five papers in this special issue on TLS 1.3 are concerned with security analysis of the published standard.

– *A Cryptographic Analysis of the TLS 1.3 Handshake Protocol* by Dowling et al., gives us proofs that the handshake protocol is secure in a computational model based on the well-established cryptographic security models for authenticated key exchange which emerged in the 1990s, starting with Bellare and Rogaway [1].

– An attack on the TLS 1.3 handshake protocol is described in *Selfie: reflections on TLS 1.3 with PSK* by Drucker and Gueron. The attack does not invalidate the above security proofs because it applies in a scenario ruled out in the analysis model. Nevertheless, this chink in the armour does show the importance of comprehensive analysis, a challenge for a protocol as complex as TLS 1.3.
– *On the Tight Security of TLS 1.3: Theoretically-Sound Cryptographic Parameters for Real-World Deployments* by Diemert and Jager shows what size of parameters are necessary in order to give concrete security bounds. In other words, this work allows us to trade security against efficiency in a measurable way.

Are there ways to improve on the security or the efficiency of TLS 1.3 without making unreasonable compromises? The other two papers in this issue look at such possibilities.

– *Session Resumption Protocols and Efficient Forward Security for TLS 1.3 0-RTT* by Gellert et al. explores the use of puncturable PRFs to provide forward secrecy for resumed protocol sessions without using any additional message passes.
– In *Secure Communication Channel Establishment: TLS 1.3 (over TCP Fast Open) versus QUIC*, Chen et al. consider the security of TLS 1.3 as a channel establishment protocol and compare it with another protocol with similar goals, namely the QUIC protocol. They reveal some subtle differences connected with the interplay of the protocols and the underlying communication layers.

The papers in this special issue provide insight into the current understanding of TLS 1.3 as well as showing directions for enhanced security and efficiency. Future versions of TLS must be anticipated. Experimental usage of post-quantum secure cipher suites is already well under way. New attack methods and new cryptographic technologies will inevitably lead to improvements and new standards. We can expect the cryptographic research community to play a significant role in the development of such standards.

Funding Open access funding provided by NTNU Norwegian University of Science and Technology (incl St. Olavs Hospital - Trondheim University Hospital).

References

[1] M. Bellare, P. Rogaway, Entity authentication and key distribution, in D.R. Stinson (ed.) *Advances in Cryptology—CRYPTO '93, Lecture Notes in Computer Science*, vol. 773 (Springer, 1993), pp. 232–249. https://doi.org/10.1007/3-540-48329-2_21

[2] K.G. Paterson, T. van der Merwe, Reactive and proactive standardisation of TLS, in L. Chen, D.A. McGrew, C.J. Mitchell (eds.) *Security Standardisation Research—Third International Conference, SSR 2016, Lecture Notes in Computer Science*, vol. 10074 (Springer, 2016), pp. 160–186. https://doi.org/10.1007/978-3-319-49100-4_7

[3] E. Rescorla, The Transport Layer Security (TLS) protocol version 1.3. *RFC* **8446**, 1–160 (2018). https://doi.org/10.17487/RFC8446