Cryptology ePrint Archive: Report 2011/219

A Standard-Model Security Analysis of TLS-DHE

Tibor Jager, Florian Kohlar, Sven Schäge, and Jörg Schwenk

Abstract: TLS is the most important cryptographic protocol in use today. However, up to now there is no complete cryptographic security proof in the standard model, nor in any other model. We give the first such proof for the TLS ciphersuites based on ephemeral Diffie-Hellman key exchange (TLS-DHE), which include the cipher suite TLS DHE DSS WITH 3DES EDE CBC SHA mandatory in TLS 1.0 and TLS 1.1. Due to subtle problems with the encryption of the final Finished messages of the TLS handshake, this proof cannot be formulated in the Bellare-Rogaway (BR) or any other indistinguishability-based model. Therefore we only prove the security of a truncated version of the TLS handshake (which has been the subject of all previous papers on TLS except [34]) completely in the standard BR model. We then define the notion of authenticated and confidential channel establishment (ACCE) as a model in which the combination of TLS handshake and TLS Record Layer can be proven secure.

Category / Keywords: cryptographic protocols / Authenticated key agreement, SSL, TLS, provable security, ephemeral Diffie-Hellman

Date: received 6 May 2011, last revised 30 Sep 2011

Contact author: tibor jager at rub de