Cryptology ePrint Archive: Report 2011/276

Analysis of the SSH Key Exchange Protocol

Stephen C. Williams

Abstract: We provide an analysis of the widely deployed SSH protocol's key exchange mechanism. We exploit the design of the SSH key exchange to perform our analysis in a modular manner. First, a shared secret key is obtained via a Diffie-Hellman key exchange. Next, a transform is applied to obtain the application keys used by later stages of SSH. We define models, following well-established paradigms, that clarify the security provided by each type of key. Previously, there has been no formal analysis of the SSH key exchange protocol. We provide a modular proof of security for the SSH shared secret and application keys. We show that although the shared secret key exchanged by SSH is not indistinguishable, the transformation then applied yields indistinguishable application keys. Our proofs use random oracles to model the hash function used within SSH.

Category / Keywords: cryptographic protocols / SSH, key exchange, security proof

Date: received 28 May 2011

Contact author: williams at cs bris ac uk