Cryptology ePrint Archive: Report 2013/139

Rethinking Definitions of Security for Session Key Agreement

Wesley George and Charles Rackoff

Abstract: We consider session key agreement (SKA) protocols operating in a public key infrastructure, with pre-specified peers, that take no session ID as input, and output only a session key. Despite much work on SKA, we argue that there is no good definition of security for this (very natural) protocol syntax. The difficulty is that in this setting the adversary may not be able to tell which processes share a key, and thus which session keys may be revealed without trivializing the security condition.

We consider security against adversaries that control all network traffic, can register arbitrary public keys, and can retrieve session keys. We do not attempt to mitigate damage from hardware failures, such as session-state compromise, as we aim to improve our understanding of this simpler setting. We give two natural but substantially different game based definitions of security and prove that they are equivalent. Such proofs are rare for SKA. The bulk of this proof consists of showing that, for secure protocols, only compatible processes can be made to share a key. This property is very natural but surprisingly subtle. For comparison, we give a version of our definition in which processes output session IDs and we give strong theorems relating these two types of definitions.

Category / Keywords: foundations / Key Exchange, Definitions, Public Key Infrastructure

Date: received 7 Mar 2013

Contact author: wgeorge at cs toronto edu

Note: A very similar version of this paper was submitted to and rejected from TCC 2011 and TCC 2012. We had hoped to quickly create a revised version, but since we didn't, we present this version as is.