Cryptology ePrint Archive: Report 2011/278

Comparing Different Definitions of Secure Session

Can Zhang

Abstract: We first propose a definition of session protocol where two parties exchange information using a shared key. The notion of security based on our definition of session protocol requires the secure transmission of a sequence of message pieces rather than a single message piece. We then propose several definitions of secure session protocol depending on how powerful we allow the adversary to be. The main goal of this paper is to compare those definitions and show a hierarchy of definitions of secure session protocol.

Category / Keywords: foundations / secure session, session protocol, private key cryptography

Date: received 26 May 2011

Contact author: canzhang work at gmail com

Available formats: PDF | BibTeX Citation

Version: 20110530:160912 (All versions of this report)

Discussion forum: Show discussion | Start new discussion