Cryptology ePrint Archive: Report 2011/050

Authenticated Key Exchange with Synchronized States

Zheng Yang

Abstract: Nowadays, most of sensitive applications over insecure network are protected by some authenticated secure channel which is highly relies on specific authenticated key exchange (AKE) protocol. Nevertheless, the leakage of authentication credential used in AKE protocol somehow result in unauthorized exploitation of credential information via identity impersonation (IDI) attack. To address the problem of IDI, we introduce a new dynamic authentication factor for AKE protocols, i.e., the secret execution states, to either prevent IDI attack by detecting attempts thereof, or limit its consequences by on-line detecting situations of previously unidentified IDI. In this paper, we model the security for authenticated key exchange with synchronized states (AKESS) based on Bellare-Rogaway model, and we particularly formalize the IDI and IDI detection. We propose a generic execution states synchronization framework for AKE, in which we utilize the session key to generate the secret execution states on both sides, and present a new AKESS protocol which is provably secure in the standard model. Our goal is to enhance the security of existing authenticated key exchange with long-lived key (AKELL) protocols by equipping them with the capabilities of both IDI prevention and detection without modifications on those protocols.

Category / Keywords: authenticated key exchange, impersonation detection, state synchronization, security model

Date: received 26 Jan 2011, last revised 10 Jun 2011

Contact author: Zheng Yang at rub de