Abstract

Proving an identity over a public link is complex when there is communication between Client and Server. Secure Shell protocol is deployed, to determine a client’s identity through Password-based key exchange schemes, over a public network, by sharing a (short) password only, with a session key. Most of the existing schemes are vulnerable to various dictionary attacks. SSL is the de facto standard today for securing end to end transport. While the protocol seems rather secure there are a number of risks which lurk in its use. The focus of the paper is on the analysis of very efficient schemes on password-based authenticated key-exchange methods. In this paper analysis of AuthA key exchange scheme and DH-EKE is done and complete proof of its security is generated. Evidences are generated to show that the AuthA and DH_EKE protocol and its multiple modes of operation are secure under the computational Diffie-Hellman intractability assumption and help in fortification of transport layer security protocol.
Reference


Index Terms

Computer Science
Security

Key words

Password Authentication

Diffie-Hellman Key Exchange
Secured Socket Lock