Abstract

A key exchange protocol enables two parties to share a common key for encrypting a large amount of data. Authentication is an essential requirement prior to the key exchange process in order to prevent man-in-the-middle attack. It is important to understand the capabilities and performance of the existing key exchange protocols before employing the protocols in our applications. In this paper, we compare Secure Socket Layer, Secure Shell, and Identity-based key exchange protocols by quantifying the performance, complexity, and level of security of each protocol. Detailed experiments and observations are conducted to examine the protocols in terms of disk usage, computation time, and data transmission time. The analysis shows that the identity-based key exchange maintains similar security level as the other protocols, while conveying better performance.
A Comparison Study on Key Exchange-Authentication protocol

Reference

- The libssh project, http://www.libssh.org/
- The openssl project, http://www.openssl.org/
- The pbc library, http://crypto.stanford.edu/pbc/

Index Terms

Computer Science       Security

Key words

Key exchange protocol       Performance
Security
Complexity