Abstract

Providing security over open and large distributed networks has always been both intriguing and challenging. There is a great chance for malicious individuals to perform disruptive and unethical tasks. Malicious users may attempt to obtain valuable information. So we require "secure channel" over insecure network. The secure communication channel should achieve primary security goals like confidentiality, integrity, authentication and non-repudiation and shared session keys are incorporated for the purpose. Therefore, it is of great interest and most challenging to devise effective mechanisms to establish these shared session keys, called key distribution problem. Much work has been done in recent years on mechanisms for key establishment. Many cryptosystems rely on cryptographically secure keys and therefore have to deal with issues like key management. A number of key establishment protocols have been proposed by different researchers as solutions to the key distribution problem and password based scheme is one of them. A password is shared between the entities in password based schemes. However, because users choose small and frequently used words as passwords, these schemes are suffered from password guessing attacks. Especially these schemes are subject to offline dictionary attacks. This work focus on password based key establishment. Even though there are a lot of password based schemes, the LDH, enhanced LDH, and PP-TAKE seems to be widely accepted mechanisms. In this context, this study includes
performance evaluation of the above mentioned protocols.

References

- Jablon David P., Strong password-only authenticated key exchange, ACM, 1996.

Index Terms

Computer Science  Security
Keywords

LDH  CAPTCHA  PP-TAKE  RSA  key establishment protocols.