Abstract

Various security attacks may cause unauthorized access, misuse, modification, or denial of a computer network and network accessible resources. To prevent these attacks various authentication means can be used to provide authenticated key exchange protocols. Authenticated key exchange protocol allows the exchange of session key and also authenticates the identities of parties involved in the key exchange. It mathematically binds the agreed key to other agreed upon data such as shared secret keys, passwords and public/private key pairs. The reliability and security of the authentication protocol can be increased by combining two factors in the same authentication protocol. Many two-factor authenticated schemes have been proposed due to its usefulness. The main focus of this paper is to propose an enhanced two-factor authenticated scheme that can resist various security attacks in network by eliminating the attack races by matching it with knowledge available in the network as well as provide user anonymity.

References

- Abdalla M., Bellare M. and Rogaway P. "The Oracle Diffie-Hellman
- Sklavos N., Alexopoulos E., and Koufopavlou O. Networking Data Integrity: High Speed Architectures and Hardware Implementations in The International Arab Journal of
Security Analysis and Performance Evaluation of an Enhanced Two-Factor Authenticated Scheme


Index Terms

Computer Science

Security
Keywords
  Key exchange  Symmetric key  WSN  Authentication.