Abstract

This paper proposes an efficient and robust multi-server authentication scheme using smart cards. Security of this scheme depends upon cryptographic one-way hash function. This scheme allows remote users to access multiple servers without any need of separately registering with each server. Also, it gets rid of the use of verification table, permits users to select and update the password securely without taking help from the server or registration center, achieves mutual authentication and establishes a session key that is common between user and the server. Moreover, the proposed scheme withstands user impersonation attack, reflection and parallel session attacks, server impersonation attack, replay attack, password guessing attack, smart card loss attack, insider attack, and stolen verifier attack.

References

An Efficient and Secure Multi-server Smart Card based Authentication Scheme

- Cheng Hsiang and Wei-Kuan Shih, 2009 "Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment," Computer Standards & Interfaces, vol. 31, no. 6, pp. 1118-1123.
- Y. M. Tseng, T. Y. Wu, J. D. Wu, 2008 "A pairing-based user authentication

Index Terms

Computer Science & Security

Keywords

BAN logic Hash function Multi-server Nonce Session key Smart card