Abstract

In a single server environment, one server is responsible for providing services to all the authorized remote users. However, the problem exists if a user wishes to access several network services. To overcome this weakness, various multi-server authentication schemes have been proposed. Though, these schemes are exposed to one or the other network security attack. This paper suggests robust multi-server authentication scheme using smart cards. Its security is based on cryptographic one-way hash function and the discrete logarithm problem. This scheme allows remote users to access multiple servers without separately registering with each server. Furthermore, it eliminates the use of verification table, allows users to choose and change the password securely without taking any assistance from the server or registration center, provides mutual authentication and establishes a common session key between user and the server. Additionally, the proposed scheme withstands user impersonation attack, server impersonation attack, replay attack, reflection and parallel session attacks, password guessing attack, insider attack, smart card loss attack and stolen verifier attack.
References

Remote User Authentication Scheme in Multi-server Environment using Smart Card


**Index Terms**

Computer Science

Computer Communication

**Keywords**

Authentication  Multi-server  Nonce  Session key  Smart card