Abstract

Recently, Tsai et al. proposed dynamic ID based smart card authentication scheme. This paper demonstrates that Tsai et al.’s scheme fails to provide early wrong password detection, secure password change and protection against insider attack. To overcome, we propose a secure SCAM (Smart Card based Authentication Mechanism) which keeps all previous merits and achieves security and functionality requirements. The performance of both the schemes has been analyzed in terms of various metrics. Comparing with Tsai et al.’s scheme, our scheme provides higher security with nearly same cost. For network where clock synchronization is tough, nonce based scheme is additionally offered.
A Secure SCAM (Smart Card based Authentication Mechanism)

References

- H. Zhang, M. Li, Security vulnerabilities of an remote password authentication scheme with smart card, 2011 International Conference on Consumer Electronics, Communications and

Index Terms

Computer Science
Security

Keywords
Authentication  Nonce  Password  Security  Smart card