Cryptology ePrint Archive: Report 2011/676

Enhanced Biometrics-based Remote User Authentication Scheme Using Smart Cards

Jian-Zhu Lu, Shaoyuan Zhang, Shijie Qie

Abstract: Authentication and key exchange are fundamental techniques for enabling secure communication over mobile networks. In order to reduce implementation complexity and achieve computation efficiency, design issues for efficient and secure biometrics-based remote user authentication scheme have been extensively investigated by research community in these years. Recently, two well-designed biometrics-based authentication schemes using smart cards are introduced by Li and Hwang and Li et al., respectively. Li and Hwang proposed an efficient biometrics-based remote user authentication scheme using smart card and Li et al. proposed an improvement. The authors of both schemes claimed that their protocol delivers important security features and system functionalities, such as without synchronized clock, freely changes password, mutual authentication, as well as low computation costs. However, these two schemes still have much space for security enhancement. In this paper, we first demonstrate a series of vulnerabilities on these two schemes. Then, an enhanced scheme with corresponding remedies is proposed to eliminate all identified security flaws in both schemes.

Category / Keywords: Biometrics, user authentication, smart cards, security

Date: received 13 Dec 2011

Contact author: tljz at jnu edu cn