Abstract: An Adaptive Timestamp-Nonce Based Authentication Scheme Using Portable Storage Devices

Wei-Chen Wu[1,3], Horng-Twu Liaw[2], and Yi-Ming Chen[3]
[1]*Computer Center, Hsin Sheng College of Medical Care and Management, Taoyuan County, Taiwan, R.O.C.*
wwu@hsc.edu.tw
[2]*Department of Information Management, Shih Hsin University, Taipei, Taiwan, R.O.C.*
htliaw@cc.shu.edu.tw
[3]*Department of Information Management, National Central University, Jhongli City, Taoyuan County, Taiwan, R.O.C.*
cym@cc.ncu.edu.tw

Abstract

In this paper, we improve an efficient and complete remote user authentication scheme and propose an adaptive timestamp-nonce based authentication scheme using portable storage devices. Compared with other smart card-based, timestamp-based and nonce-based schemes, our scheme achieves more functionality. The new importance merits are: An adaptive timestamp-nonce structure is proposed; portable device stores authentication data not only smart card; all transactions through non-secure channel, especially in the registration phase, and batch of portable storage devices is issued. Besides, the basic merits include a dictionary of verification tables is not required to authenticate users, users can choose their password freely, mutual authentication is provided between a user and the remote system, the communication cost and the computational cost are very low, a user can update their password after the registration phase, a session key agreed by a user and the remote system is generated in every session and the serious time synchronization problem are solved.