Security Enhancements of Smart Card-Based Remote User Password Authentication Scheme with Session Key Agreement

Younghwa An

Division of Computer & Media Information Engineering, Kangnam University, Korea
yhan@kangnam.ac.kr

***Abstract*-**Smart card-based user authentication schemes have been proposed recently to improve the security drawbacks in user authentication scheme. Li et al., in 2013, proposed an enhanced smart card-based remote user password authentication scheme which can withstand the security drawbacks of Chen et al.'s scheme. In this paper, we show that Li et al.'s scheme is vulnerable to user impersonation attack, server masquerading attack, password guessing attack and does not provide mutual authentication between the user and the server. Also, we propose the enhanced scheme with session key agreement to overcome the security drawbacks of Li et al.'s scheme, even if the secret values stored in the smart card is revealed. As a result, the enhanced scheme is relatively more secure than the related scheme in terms of security.

***Keywords*-**Authentication, User Impersonation Attack, Server Masquerading Attack, Password Guessing Attack, Session Key Agreement

Younghwa An received his B.S. and M.S. degrees in electronic engineering from Sungkyunkwan University, Korea in 1975 and 1977, respectively. He obtained his Ph. D. in information security from same university, 1990. From 1983 to 1990, he served as an assistant professor with the department of electronic engineering at Republic of Korea Naval Academy. Since 1991, he has been a professor with department of computer and media information engineering at Kangnam University. During his tenure at Kangnam University, he served as the director of computer & information center and the director of central library. His major research interests include information security and network security.