A SECURITY ENHANCED REMOTE USER AUTHENTICATION SCHEME USING SMART CARDS

EUN-JUN YOON¹, SUNG-HO KIM² AND KEE-YOUNG YOO²,*

¹Department of Cyber Security
Kyungil University
33 Buho-Ri, Hayang-Ub, Kyungsan-Si, Kyungsangpuk-Do 712-701, Republic of Korea
ejyoon@kiu.ac.kr

²School of Computer Science and Engineering
Kyungpook National University
1370 Sankyuk-dong, Buk-gu Daegu 702-701, Republic of Korea
shkim@knu.ac.kr; *Corresponding author: yook@knu.ac.kr

Received November 2010; revised March 2011

Abstract. A remote user authentication system has become an important part of security, along with confidentiality and integrity, for systems such as the Internet that offer remote access over untrustworthy networks. In 2006, Liaw et al. proposed an efficient and complete remote user authentication scheme using smart cards that includes a session key being agreed and an updated password phase. However, the current paper demonstrates that Liaw et al.’s scheme is vulnerable to some attacks and then presents an improved scheme in order to isolate such security problems.

Keywords: Security, Authentication, Smart card, Diffie-Hellman key agreement, Cryptography, Cryptanalysis

1. Introduction. Recently, a remote user authentication system has become an important part of security, along with confidentiality and integrity, for systems such as the Internet that offer remote access over untrustworthy networks [1-22]. In a remote password authentication scheme, based on knowledge of the password, a user can use it to create and send a valid login message to a remote system to gain the right to access. The remote system also uses the shared password to check the validity of the login message and authenticate the user. However, these remote password authentication schemes are vulnerable to password guessing attacks since most users usually choose easy-to-remember passwords. In 1981, a remote password authentication scheme was first proposed by Lamport [23] over an insecure channel. Since then, several schemes [24-43] have been proposed for improving security and achieving greater functionality.

In 2006, Liaw et al. [34] proposed an efficient and complete remote password authentication scheme using smart cards including an agreed session key and updated password phase. Their scheme had several merits: (1) the remote system does not need a dictionary of verification tables to authenticate users; (2) users can choose their passwords freely; (3) mutual authentication was achieved, between the user and the remote system; (4) the communication and computational costs are very low; (5) users can update their passwords after the registration phase; (6) a session key agreed by the user and the remote system can be generated in every session; and (7) the timestamp is discarded in order to avoid the serious time synchronization problem.