Security Improvements of Dynamic ID-based Remote User Authentication Scheme with Session Key Agreement

Young-Hwa An*

** Division of Computer and Media Information Engineering, Kangnam University 111, Gugal-dong, Giheung-gu,Yongin-si, Gyounggi-do, 446-702, Korea*

yhan@kangnam.ac.kr *ffmail.com*

***Abstract*—Password-based authentication schemes have been widely adopted to protect resources from unauthorized access. In 2010, Khan et al. proposed an efficient and secure dynamic ID-based authentication scheme to overcome the weaknesses of Wang et al.'s scheme. In this paper, we show that Khan et al.'s scheme is vulnerable to password guessing attack, forgery attack, and does not provide user anonymity. Also, we propose the improved scheme to overcome the security drawbacks of Khan et al.'s scheme and to provide user anonymity and session key agreement, even if the secret values stored in the smart card is revealed. As a result, the improved scheme is relatively more secure than the related scheme in terms of security.**

***Keywords*—Authentication, Forgery Attack, Password Guessing Attack, Session Key Agreement, User Anonymity**

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.