Security Weaknesses of an Improved Biometrics-based User Authentication Scheme without Concurrency System

Young-Hwa An*

*Computer Media Information Engineering, Kangnam University, 111, Gugal-dong, Giheung-gu, Yongin-si, Gyounggi-do, 446-702, Korea
yhan@kangnam.ac.kr

Abstract—Recently, many biometrics-based user authentication schemes using smart cards have been proposed to improve the security weaknesses in user authentication system. In 2010, Chang et al. proposed an improved biometrics-based user authentication scheme without concurrency system which can withstand the forgery attack, the off-line password guessing attack, the replay attack, etc. In this paper, we analyze the security weaknesses of Chang et al.’s scheme, and we will show that Chang et al.’s scheme is still vulnerable to the user impersonation attack, the server masquerading attack and the biometric guessing attack, and does not provide the mutual authentication between the user and the remote server.

Keywords—Authentication, Biometrics, User Impersonation Attack, Server Masquerading Attack, Mutual Authentication