Abstract

In 2004, Das et al. proposed a dynamic identity based remote user authentication scheme. This scheme allows the users to choose and change their passwords freely and the server does not maintain any verification table. Das et al. claimed that their scheme is secure against stolen verifier attack, replay attack, forgery attack, dictionary attack, insider attack and identity theft. Unfortunately, many researchers demonstrated that Das et al.’s scheme is susceptible to various attacks. Furthermore, this scheme does not achieve mutual authentication and thus can not resist malicious server attack. In 2006, Liou et al. improved Das et al.’s scheme and claimed that the improved scheme achieves mutual authentication and is secure against aforementioned attacks. However, we found that Liou et al.’s scheme is susceptible to impersonation attack, malicious user attack, offline password guessing attack and man-in-the-middle attack. This paper presents a secure dynamic identity based authentication scheme using smart cards to resolve the aforementioned problems, while keeping the merits of different dynamic identity based authentication schemes.
An Improvement of Liou et al.'s Authentication Scheme using Smart Cards


Index Terms

Computer Science

Security

Key words

Network Security

Cryptography

Password
Authentication Protocol

Smart Card

Hash Function