Cryptology ePrint Archive: Report 2011/365

Security flaws in a biometrics-based multi-server authentication with key agreement scheme

Debiao He

Abstract: Recently, Yoon et al. proposed an efficient biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem (ECC) for multi-server communication environments [E.-J. Yoon, K.-Y. Yoo (2011) Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem, Journal of Supercomputing, DOI: 10.1007/s11227-010-0512-1]. They claimed their scheme could withstand various attacks. In the letter, we will show Yoon et al.'s scheme is vulnerable to the privileged insider attack, the masquerade attack and the smart cart lost attack.

Category / Keywords: Authentication; Key agreement; Masquerade attack; Privileged insider attack; Elliptic curve cryptosystem; Smart card

Publication Info: The paper has not been published.

Date: received 5 Jul 2011, last revised 11 Jul 2011

Contact author: hedebiao at 163 com