Malaysian Journal of Mathematical Sciences

Journal homepage: https://einspem.upm.edu.my/journal

On the Security of a Non-Interactive Authenticated Key Agreement over Mobile Communication Networks

Yau, W. C. [1], Yap, W. S. [2], and Chin, J. J. *[3]

[1]*School of Electrical and Computer Engineering, Xiamen University Malaysia, Malaysia*
[2]*Lee Kong Chian Faculty of Engineering and Science, Universiti Tunku Abdul Rahman, Malaysia*
[3]*Faculty of Computing and Informatics, Multimedia University, Malaysia*

E-mail: jjchin@mmu.edu.my
**Corresponding author*

Received: 16 Jun 2021
Accepted: 7 October 2021

Abstract

Setting up a common secret key for communications between two parties over insecure mobile communication networks is important for many network applications. Previously, Wu and Lin proposed a non-interactive authenticated key agreement over mobile communication networks with security proofs assuming the Bilinear Diffie-Hellman problem is hard. Wu and Lin scheme is unique as the users do not need to interact at all in sharing a secret key. Besides, their scheme will at least achieve trust level of 2, where the system authority will not know the user secret keys since self-certified cryptography is used. In this paper, we demonstrate that any malicious outsider can break the security of Wu and Lin's scheme by impersonating any one of the party using public key replacement attack. Besides, we show that the system authority can easily recover all the user secret keys which contradicts with the concept of self-certified cryptography. Lastly, if the secret key shared between two parties or one of the party's private key had been compromised, the same two users can no longer communicate in the future since the same secret key will be derived and shared forever. This violates the property of forward secrecy, a property that must be provided for a key agreement scheme.

Keywords: key agreement; security analysis; attacks; communication networks and applications.