Cryptology ePrint Archive: Report 2011/702

Comments of an efficient and secure multi-server authentication scheme with key agreement

Yitao Chen

Abstract: Recently, Tsaur et al. proposed an authentication scheme for multi-server environments and claimed their scheme could withstand various attacks. In this letter, we will point out that Tsaur et al. scheme is not suitable for multi-server environments since the user has to register for every server. Furthermore, we will show Tsaur et al. scheme is vulnerable to the password guessing attack and the privileged insider attack.

Category / Keywords: multi-server, password authentication protocol, smart card, password change, key agreement

Publication Info: The paper has not published.

Date: received 23 Dec 2011, last revised 1 Jan 2012

Contact author: chenyitao math at gmail com

Available formats: PDF | BibTeX Citation

Version: 20120102:022753 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]