IMPROVING THE LEE-LEE’S PASSWORD BASED AUTHENTICATED KEY AGREEMENT PROTOCOL

EUN-JUN YOON¹ AND KEE-YOUNG YOO²*

¹Department of Cyber Security
Kyungil University
33 Buho-Ri, Hayang-Ub, Kyungsan-Si, Kyungsangpuk-Do 712-701, Republic of Korea
ejyoon@kiu.ac.kr

²Department of Computer Engineering
Kyungpook National University
1370 Sankyuk-dong, Buk-gu Daegu 702-701, Republic of Korea
*Corresponding author: yook@knu.ac.kr

Received December 2010; revised April 2011

ABSTRACT. Password based authenticated key agreement protocols have been the most widely used methods for user authentication, since it allows people to choose and remember their own passwords without any assistant device. Password based authenticated key agreement protocols, however, are vulnerable to password guessing attacks since users usually choose easy-to-remember passwords. Recently, Lee and Lee pointed out that N. Y. Lee et al.’s password based authenticated key agreement protocol is vulnerable to a man-in-the-middle attack, and then proposed an improvement to overcome the attack. The current paper, however, demonstrates that Lee-Lee’s password based authenticated key agreement protocol is still vulnerable to off-line password guessing attacks, and then proposes an improvement of the protocol in order to overcome such security attacks. Compared with Lee-Lee’s protocol, the proposed protocol is very useful in password-based Internet and wire/wireless communication environments to access remote information systems since it provides security, reliability and efficiency.

Keywords: Cryptography, Authenticated key agreement, Cryptanalysis, Password guessing attacks

1. Introduction. Password based authenticated key agreement protocols [1] have been the most widely used method for user authentication, since it allows people to choose and remember their own passwords without any assistant device. The objective of a password based authenticated key agreement protocol is the same as a conventional authenticated key agreement protocol: after two communicating parties successfully execute the protocol, each of them should have certain assurances of the other’s true identity (authentication), and it shares a new and random session key only with each other and the key is derived from contributions of both parties (key agreement) [2-23].

Password based authenticated key agreement protocols, however, are vulnerable to password guessing attacks [24] since users usually choose easy-to-remember passwords. Unlike typical private keys, the password has limited entropy, and is constrained by the memory of the user. For example, one alphanumerical character has 6 bits of entropy. Therefore, the goal of the attacker, which is to obtain a legitimate communication parties’ password, can be achieved within a reasonable time. Thus, the password guessing attacks on password based authenticated key agreement protocols should be considered realistic [25-30].