Security Analysis of Password-Authenticated Key Agreement Protocols*

Kyung-Ah Shim[1] and Seung-Hyun Seo[2]

[1] Department of Mathematics
[2] Department of Computer Science and Engineering,
Ewha Womans University, Seoul, Korea
kashim@ewha.ac.kr, seosh@ewhain.net

Abstract. Recently, there have been proposed a number of password-authenticated key agreement protocols for two-party setting or three-party setting. In this paper, we show that recently proposed three password-authenticated key agreement protocols in [11, 12, 10] are insecure against several active attacks including a stolen-verifier attack, an off-line password guessing attack and impersonation attacks.

1 Introduction

Two entities, who only share a password, and who are communicating over an insecure network, want to authenticate each other and agree on a session key to be used for protecting their subsequent communication. This is called the *password-authenticated key exchange* problem. The first password-authenticated key exchange (PAKE) protocol, known as Encrypted Key Exchange (EKE), was suggested by Bellovin and Merritt [1]. By using a combination of symmetric and public-key cryptography, EKE resists dictionary attacks by giving a passive attacker insufficient information to verify a guessed password. Since it was invented, many password-authenticated key agreement protocols that promised increased security have been developed [2-4, 8, 9, 14-16].

In 1995, Steiner, Tsudik, and Waidner [15] extended two-party EKE protocol to three-party one (STW-3P-EKE), in which all clients share a password with a trusted server S only and in which S mediates between two communication parties to allow their mutual authentication. The three-party EKE protocol is particularly well-suited for large communication environments because it is inconvenient in key management that every two communication parties mutually share a secret. Unfortunately, Ding and Horster [7] showed that the STW-3P-EKE is not resistant to undetectable on-line password guessing attacks. Lin, Sun and Hwang [13] also pointed out that the STW-3P-EKE is not only vulnerable to undetectable on-line password guessing attacks but also vulnerable to off-line password guessing attacks. They proposed a new three-party EKE, in which the server holds a long-term and publicly known public key to prevent both off-line

* This work was supported by the Korea Research Foundation Grant funded by the Korean Government(MOEHRD).(KRF-2005-217-C00002).

Y.G. Desmedt et al. (Eds.): CANS 2005, LNCS 3810, pp. 49–58, 2005.

and undetectable on-line password guessing attack. However, in their protocol, communication parties have to obtain and verify the public key of the server, a task which puts a high burden on the user. Later, there have been proposed several key agreement protocols for three-parties, in which two clients establish a common session key through a authentication server. Most of those protocols require to use server's public key to prevent password guessing attacks. However, the protocols may not be practical for some environments since clients need to verify and keep the server's public key. Recently, Lee *et al* [12] proposed a new efficient verifier-based key agreement protocol for three parties, which does not require server's public key. They argued that the protocol was secure against impersonation attacks and server compromise. In this paper, we show that the protocol is still insecure against a stolen-verifier attack and impersonation attacks. Also, Lee *et al* [11] proposed a two-party password-authenticated key agreement protocol PAKA and its verifier-based version PAKA-X. In the PAKA-X protocol, the client uses a plaintext of the password, while the server stores a verifier for the password. So the protocol does not allow an adversary who compromises the server to impersonate a client without actually running a dictionary attack on the password file. We will show that the PAKA-X protocol is insecure against a stolen-verifier attack and an off-line password-guessing attack.

At ICICS'02, Byun *et al* [5] proposed two password-authenticated key exchange protocol between clients with different passwords, so-called Client-to-Client Password-Authenticated Key Exchange (C2C-PAKE) protocol. One is for a cross-realm setting where two clients are in two different realms and hence there exist two servers involved, the other is for a single-server setting where two clients are in the same realm. The protocol being circulated for consideration at the 27th SC27/WG2. Subsequently, Chen [6] and Kim *et al* [10] showed that their protocol was insecure against a dictionary attack by a malicious server in a different realm and Denning-Sacco attacks mounted by insiders, respectively. And Kim *et al* [10] also proposed a modified protocol to resist these attacks. In this paper, we point out that the modified protocol is also insecure against impersonation attacks.

The rest of the paper is organized as follows. The next section presents the attacks on the PAKA-X protocol. In section 3, we point out the Lee *et al*'s PAKE for three-party is insecure against a stolen-verifier attack. In section 4, we show that the modified C2C-PAKE protocol is insecure against partition attacks and impersonation attacks. Concluding remarks are given in section 5.

2 Cryptanalysis of the PAKA-X Protocol

Lee *et al* [11] proposed a password-based authenticated key agreement protocol, PAKA and its verifier-based version, PAKA-X. In this section, we show that the PAKA-X protocol is insecure against a stolen-verifier attack and an off-line password guessing attack. First, we review the PAKA-X protocol.