Efficient and Provably Secure Generic Construction of Three-Party Password-Based Authenticated Key Exchange Protocols*

Weijia Wang and Lei Hu

State Key Laboratory of Information Security,
Graduate School of Chinese Academy of Sciences, Beijing 100049, China
{wwj, hu}@is.ac.cn

Abstract. Three-party password-based authenticated key exchange (3-party PAKE) protocols make two communication parties establish a shared session key with the help of a trusted server, with which each of the two parties shares a predetermined password. Recently, with the first formal treatment for 3-party PAKE protocols addressed by Abdalla et al., the security of such protocols has received much attention from cryptographic protocol researchers. In this paper, we consider the security of 3-party PAKE protocols against undetectable on-line dictionary attacks which are serious and covert threats for the protocals. We examine two 3-party PAKE schemes proposed recently by Abdalla et al. and reveal their common weakness in resisting undetectable on-line dictionary attacks. With reviewing the formal model for 3-party PAKE protocols of Abdalla et al. and enhancing it by adding the authentication security notion for the treatment of undetectable attacks, we then present an efficient generic construction for 3-party PAKE protocols, and prove it enjoys both the semantic security and the authentication security.

Keywords: password, authenticated key exchange, key distribution, multi-party protocol.

1 Introduction

Three-party password-based authenticated key exchange protocols (3-party PAKE or 3PAKE) enable communicating parties within a large network, who only share a weak (low entropy) password with a trusted server respectively, to authenticate each other with the help of the trusted server and establish a strong session key for protecting their subsequent communications over the public channel. In this solution, a communicating party who wants to build secure communications with other parties does not need to remember so many passwords whose number would be large linearly in the number of all possible partners, instead it only holds a password shared with a trusted server. Due to this advantage, these protocols are particularly appealing for those real-world applications in which communication parties are human beings who are equipped

* This work was supported by NSFC(60373041,60573053).

R. Barua and T. Lange (Eds.): INDOCRYPT 2006, LNCS 4329, pp. 118–132, 2006.

with lightweight or mobile client machines that can not afford a heavyweight infrastructure such as public key infrastructure (PKI) and common secrets with every party.

Unlike public-key based key exchange protocols which rely on the existence of PKI, password-based authenticated key exchange protocols, in which secret keys shared among communication parties are not distributed over a large space, but are rather drawn from a small set of values, have a challenge from so-called exhaustive dictionary attacks. Generally, we can divide such attacks into the following three classes [13]:

1. Off-line dictionary attacks: Only by using the eavesdropped information, an attacker guesses a password and verifies its guess off-linely. No participation of the honest client or the server is required, so these attacks can not be noticed.
2. Undetectable on-line dictionary attacks: An attacker tries to verify a password guess in an on-line transaction. However, a failed guess can not be detected by the honest client or the server, since one of them is not able to distinguish a malicious request from an honest one.
3. Detectable on-line dictionary attacks: Similar to above, an attacker attempts to use a guessed password in an on-line transaction. Using the response from the honest client or the server, it verifies the correctness of its guess. But a failed guess can be detected by the honest client or the server.

Among these attacks, detectable on-line dictionary attacks are unavoidable and should be handled by taking additional precautions such as logging failed protocol attempts and invalidating the use of the password after a certain number of failures. However, both off-line and undetectable on-line dictionary attacks are serious attacks against password-based settings so that a secure password-based protocol should ideally resist the two types of attacks. Nevertheless, undetectable on-line dictionary attacks are always more difficult to be found than off-line ones in the design of password-based protocols, especially in that of 3-party PAKE cases so that some 3-party PAKE protocols are still susceptible to the undetectable attacks even if they are claimed to be provably secure [1, 2].

Our contribution. In this paper, we study the design of 3-party PAKE protocols resisting dictionary attacks, especially against both off-line and undetectable on-line dictionary attacks. Two formal treatments for 3-party PAKE protocols are proposed recently by Abdalla et al. [1, 2]. Unfortunately, these two schemes still suffer from undetectable on-line dictionary attacks due to the attacks being out of the scope of the security model [1] considered. In section 2, we will briefly describe such attacks against the above two schemes. Then, we review the formal model for 3-party PAKE protocols provided by Abdalla et al. [1] and enhance it by adding the authentication security notion for the treatment of undetectable attacks. Finally, we present a new generic construction scheme for the 3-party PAKE protocols. Compared with the resolution proposed by Abdalla et al. [1], our scheme is not only more efficient, but also resistant to both off-line and undetectable on-line dictionary attacks.