Efficient Password Scheme Without Trusted Server

Sattar J. Aboud, Iraqi Council of Representatives, Iraq
Mohamed Alnuaimi, Middle East University for Graduate Studies, Jordan
Haidar S. Jabbar, Mansour University College, Iraq

ABSTRACT

In 2005, Lee suggested a password scheme for three participants without trusted server. Lee claimed that the scheme can withstand different attacks and give the perfect secrecy. In this paper, the authors demonstrate what the Lee scheme undergoes from the imitation attack. Simultaneously, the authors suggest an enhanced algorithm to resist the mentioned attacks.

Keywords: Cryptanalysis, Information Security, Key Agreement, Password Scheme, Trusted Server

INTRODUCTION

If two participants need to communicate between each of them, the identity authentication of the other participant is a vital need. For improving the functioning of the scheme (Bellovin & Merrit, 1992) suggested an encrypted exchange protocol relied on password for authentication and key agreement. Subsequent the idea of Bellovin and Merrit’s (1992) scheme, several three-party schemes is suggested (e.g., Chang & Cheng, 2004; Lee, Hwang, & Lin, 2004; Lu & Cao, 2007). But, many of these schemes still have certain security difficulties; for instance, an off-line password guessing attack (Nam, Lee, Kim, & Won, 2007) and an on-line password guessing attack (Shim & Woo, 2007). Not just that, several schemes also needed trusted server to protect the common password (Sun, Chen, & Hwang 2005).

To improving the efficiency and avoiding some attacks (Lee, Kim, & Yoo, 2005) suggested an effective verifier typed key agreement scheme for three participants without trusted server. Lee scheme gives the perfect secrecy by using the idea of the (Diffie & Hellman, 1976) protocol and every user expect only requests to memorize an unforgettable password. The scheme is appropriate for some uses of low calculations. However, we will illustrate that Lee scheme is weak under the imitation attack without construction an off-line password guessing attack. Simultaneously, in this paper we will suggest an enhanced algorithm to resist the mentioned attack.
RELATED WORK

Since the innovative method that withstands the password guessing attacks was presented by Lomas, Gong, Saltzer, and Needham (1989), there have been several password-typed authenticated key agreement schemes introduced. For example Jablon (1996) proposed a scheme were security relied on heuristic arguments. Also Halevi and Krawczyk (1999) introduced another scheme, the scheme considered as inflexible for security of password-typed authenticated scheme.

However, Boyarsky (1999) improved this scheme by making it secure in multi-user environment, but, this scheme is inappropriate for situation where communication has to be established between entities those sharing a common limited-entropy password. Another password-typed key exchange scheme has been suggested by Boyko, MacKenzie, and Patel (2000). This scheme is relied on two-party password-typed scheme. An enhancement for this scheme was made to multi-party setting by Bresson, Chevassut, and Pointcheval (2004). The security of Bresson, Chevassut, and Pointcheval scheme is based on the arbitrary oracle approach and in the ideal cipher approach.

Another scheme by Lee, Kim, Kim, and Yoo (2004) suggested a verifiable-typed key agreement scheme. In this scheme, the entity employs a document of the password, while the server keeps as a verifier for the password. Thus the scheme cannot let an opponent who able to exchange information with the server to impersonate any entity without running the dictionary attack in the password file. But, the scheme is not protected against stolen-verifier attack as Kwon (2004) has claimed. Also, Yoon and Yoo (2005) proposed a two-party key agreement scheme relied on Diffie and Hellman scheme.

Also Strangio (2006) presented another two-party key agreement protocol relied also on Diffie and Hellman scheme. Both schemes are not appropriate for large networks since they cannot assume each party shares a secret password with other entity. However, the first work that copes with off-line dictionary attacks is introduced by Bellovin and Merritt (2007). They presented a family of encrypted key exchange to resist dictionary attack. This protocol is very important and become the foundation for future work in this area.

Also Hussain and Al-Bahadili (2008) proposed simple authenticated key agreement protocol which is relied on Diffie and Hellman key agreement protocol. Unfortunately, this protocol is inefficient for practical use and does not allow concurrent executions. Also, this scheme is simple and cost effective. Another scheme by Shin, Kobara, and Imai (2009) introduced a scheme relied on threshold anonymous scheme. However, the scheme is complicated and costly.

REVIEW OF LEE SCHEME

In this section, we will review Lee scheme illustrate that the scheme is vulnerable. Prior to describing the scheme, we will determine the notations used which are as follows.

\[ \text{id}_A : \text{Indicates the identity of entity A} \]
\[ \text{id}_B : \text{Indicates the identity of entity B} \]
\[ \text{id}_T : \text{Indicates the Trusted server T} \]
\[ p : \text{Represents a prime number and } g \text{ is a primitive in the cyclic group } Z_p^* \]
\[ h(.) : \text{Represents a secure one-way hash function} \]
\[ w_A : \text{Represents a password for entity A} \]
\[ w_B : \text{Represents a password for entity B} \]
\[ H : \text{Represents the hacker} \]

LESS SCHEME DESCRIPTION

Prior to execution the scheme, suppose there are two entities, entity \( A \) and entity \( B \), decide to agree a shared session key over a trusted server, named \( T \). For enrolling \( T \), \( A \) and \( B \) respectively, select passwords \( w_A \) for entity \( A \) and for entity \( B \). Calculate verifiers

\[ v_A = g^{(\text{id}_A, \text{id}_T, w_A)} \mod p \]
\[ v_B = g^{(\text{id}_B, \text{id}_T, w_B)} \mod p \]
A Distributed Systems Approach to Airborne Self-Separation
Henrique Moniz, Alessandra Tedeschi, Nuno Ferreira Neves and Miguel Correia
www.igi-global.com/chapter/distributed-systems-approach-airborne-self/38109?camid=4v1a