Proceedings of the 4th WSEAS Int. Conf. on Information Security, Communications and Computers, Tenerife, Spain, December 16-18, 2005 (pp124-127)

A Password-Based Mutual Authentication Protocol for Wireless Network

JOONGMAN KIM DONGMYUNG SHIN YOOJAE WON BYONGJIN CHO
Information Security Technology Division
Korea Information Security Agency
78, Garak-Dong, Songpa-Gu, Seoul, Korea 138-803
KOREA

Abstract: - This paper proposes a password based authentication protocol which authenticates mutually and exchanges a session key between a user and an authentication server for multicast service through a public wireless network. The main idea is that after we create a user verifier and an authentication server verifier, we increase the randomness of those verifiers' information. Also we encrypt and transfer a session key for secret communication, and construct a method having strength to the off-line password dictionary attack. Therefore our contribution in this paper is that we propose a scheme which resists an exposure of a session key; furthermore, we are able to provide lightweight authentication procedure for a mobile user as well as a multicast user over wired and wireless network.

Key-Words: - Password, Mutual Authentication, Verifier, Session Key, Wireless Network, Multicast Service

1 Introduction

Security Protocols for wireless network focus on the authentication and key exchange, and in many cases they are designed to use certificates. As a typical example, WTLS (Wireless Transport Layer Security) protocol of WAP (Wireless Application Protocol) forum is used[1]. In addition to WTLS, many protocols used in wireless network are designed to be based on a public key cryptosystem using a certificate issued through wireless PKI (Public Key Cryptography). The management of a certificate makes a user inconvenient in a user's view. Also in case that the construction of a wireless PKI is incomplete, it is difficult to use these certificate based protocols.

Due to the convenience of human-memorable passwords as an alternation of a certificate, mainly passwords are used. When a user wants to connect a server, a user's password as a method of an authentication can be used. Because a password is maintained by human short memory, various password guessing attacks can be occurred.

Bellovin and Merritt proposed a password-based EKE protocol secure against the password guessing attacks in 1992. Our protocol uses a shared password to exchange secret information between a user and an authenticated server over an insecure network. There are several presented similar protocols. For example, PAK[2], SRP[3], SNAPI[4], AuthA[5], and AMP are verifier-based protocols that a server can authenticate a user with a verifier. Verifier-based protocols use a verifier which resists password guessing attacks and memorizes different information between a user and a server. At present, SRP, PAK, and AMP are being discussed by the IEEE P1363 Standard Working Group as practical protocols for standardization on password-based public key cryptographic techniques.

This paper is organized as follows. In the following section, the requirements for password-based authentication protocols are presented. In Section 3, our proposed protocol is described. In Section 4, security analysis for proposed protocol is explained in accordance with several requirements in Section 2. Finally this paper is concluded in Section 5.

2 Protocol Requirement

2.1 Prevention of off-line password dictionary attack [6]

One of vulnerabilities related to a password-based authentication protocol is off-line password dictionary attack which an attacker guesses a user's password. The method of this attack is that an attacker compares his/her guessed passwords with ones in a password dictionary list. Because this attack is executed by a number of devices with high computing ability, the success possibility of this attack is very high. Therefore, methods which can decrease the success possibility are required.

2.2 Forward secrecy

If a compromise of a long-term secret value (a user's password) does not mean a compromise of a session key in previous session, it is defined that a protocol satisfies a forward secrecy. That is, if an attacker can acquire a user's password by means of a sniffing tool, a backdoor program, or a physical method, it is possible that he/she can obtain a compromised session key in a previous session. Therefore, though a user's password is exposed, the method that an attacker can not acquire a compromised session key in a previous session is required.

2.3 Prevention of Denning-Sacco Attack [2]

A compromised session key is deleted in the session end. However, if an attacker can acquire a compromised session key by means of all other methods in addition to an exhaustive search, he/she can attempt execute an off-line password dictionary attack. Therefore, though an attacker can acquire a session key, he/she can not obtain any information related to a user's password.

2.4 Prevention of positive man in the middle attack and replay attack

The positive man in the middle attack is that an attacker impersonates both a user and an authenticated server. Also while an attacker exists in the middle of them, he/she intercepts exchanged messages. After that, he/she creates two session keys, which one of them is a key to communicate with a user, and the other is a key to communicate with an authenticated server independently.

The replay attack is that an attacker resends a user's messages to an authenticated server, and recreates a compromised session key created by a user

3 Proposed Protocol

3.1 Assumption

- Both a user shares his hashed password $H(pw)$ with an authentication server.

- A user negotiates a secret key algorithm (E), a hash algorithm (H), a key agreement algorithm, a big prime (p), and a generator (g) with an authentication server. Also the notation of $\bmod p$ will be omitted.

- When two input values' length for the Exclusive OR (XOR) operation are different with each other, the input value with bigger length will be padded at the front part of it with '0' value.

3.2 Protocol Description

1st Stage: User's client → Server:

$$(ID_C, r_C, E_{H(pw)}(g^A)) \quad (1)$$

2nd Stage: Server → User's client

$$(ID_S, r_S, E_{H(pw)}(g^B), V_S) \quad (2)$$

3rd Stage: User's client → Server:

$$V_C \quad (3)$$

3.2.1 1st Stage

A user creates his/her identification (ID_C), a random number (r_C), his/her public key (g^A) for a key agreement with the authentication server, and an encrypted value ($E_{H(pw)}(g^A)$) with a hashed password ($H(pw)$), and then sends them to an authenticated server.

3.2.2 2nd Stage

An authenticated server also creates its identification ID_S, a random number r_S, its public key g^B for a key agreement with the user, an encrypted value $E_{H(pw)}(g^B)$ with a hashed password $H(pw)$, and then use previous values as elements of the authenticated server's verifier V_S . Also the authenticated server computes a secret sharing value g^{AB} as a result of a key agreement protocol with g^B and g^A obtained from the user. This secret sharing value is used in the authenticated server's verifier V_S which is computed as follows.

$$V_S = H(g^{AB} \oplus H(pw) \oplus r_C \oplus r_S) \quad (4)$$

Finally, the authenticated server sends them $(ID_S, r_S, E_{H(pw)}(g^B), V_S)$ to the user.

3.2.3 3rd Stage

The user verifies the authenticated server's verifier V_S which is transferred from the authenticated server. The method which the user verifies the authenticated server's verifier is as follows. The user computes the authenticated server's verifier V_S' which the user computes, where $V_S' = ((g^{AB})' \oplus H(pw)' \oplus r_C' \oplus r_S')$. The user compares V_S' with V_S. If this verification is successful, he/she computes the user's verifier (V_C) as follows, and then sends it to the authenticated server.

$$V_C = H(V_S \oplus H(pw) \oplus r_C \oplus r_S) \quad (5)$$

Otherwise, the user should stop the communication with the authenticated server immediately.

Similarly, the authenticated server verifies the user's verifier V_C which is transferred from the user. The method which the authenticated server verifies the user's verifier is as follows. The authenticated server computes the user's verifier V_C' with V_S', $H(pw)'$, r_C', and r_S', which the authenticated server computes, where $V_C' = (V_S' \oplus H(pw)' \oplus r_C' \oplus r_S')$. The authenticated server also compares V_C' with V_C. If this verification is failed, the authenticated server should stop the communication with the user immediately. Otherwise, the mutual authentication is complete. After that, both the user and the authenticated server compute the session key K, which will be used in secret communication between them. The session key K is computed as follows using the key derivation function F_K.

$$\begin{aligned} & K \\ &= F_K(g^{AB}, g^A, g^B, ID_C, ID_S, H(pw)) \\ &= H(g^{AB} \oplus g^A \oplus g^B \oplus ID_C \oplus ID_S \oplus H(pw)) \end{aligned}$$

After that, both the user and the authenticated server exchange encrypted messages with the session key K which is shared by them. The user verifies the authenticated server's verifier V_S, and the authenticated server also verifies the user's verifier V_C. Consequently, both the user and the authenticated server complete the mutual authentication process.

4 Security Analysis

4.1 Prevention of off-line password dictionary attack

Prevention of off-line password dictionary attack, one of vulnerabilities related to the password-based authentication protocol means that though an attacker can obtain exchanged messages, he/she can not acquire any information related to a user password. Because elements of the proposed protocol include identification, random numbers, hashed values, and encrypted values, a user's password is secure against passive attacks.

4.2 Forward Secrecy

In the proposed protocol, though a password shared between a user and an authenticated server is exposed, a session key used in each session is created by Diffie-Hellman key agreement regardless of the user's password. Consequently, it is impossible for an attacker to obtain the session key used in a previous session. Even though a user's password is given, all an attacker can obtain are only a user's public key c and an authenticated server's public key g^B for Diffie-Hellman key agreement. Computing g^{AB} from those values is the same as solving the discrete logarithm problem. Therefore, proposed protocol has the same possibility that the discrete logarithm problem is solved.

4.3 Prevention of Denning-Sacco Attack

Denning-Sacco Attack is that though an attacker can obtain a session key in previous session, he/she can not compute the user's password. That is, when we assume that an attacker can acquire a session key K, since K is a value which hashes an XOR operation of $g^{AB}, g^A, g^B, ID_C, ID_S$, and $H(pw)$, he/she can not compute the user's password.

4.4 Prevention of Positive Man in the Middle Attack and Replay Attack

The positive man in the middle attack is the same as the impersonation attack. In the proposed protocol, when an attacker can obtain all exchanged messages, if he/she do not know a user's password, he/she can not execute Diffie-Hellman key agreement. Consequently, since an attacker can not compute a session key, the proposed protocol is secure against the positive man in the middle attack.

Also, since that all exchanged messages are created randomly is assumed, the success possibility of the replay attack may be ignored.

5 Conclusion

We propose a password-based mutual authentication protocol in this paper. The proposed protocol use two verifiers – the user's verifier and the authenticated server's verifier - , which make password guessing attacks difficult. Also we present protocol requirements for a password-based authentication protocol, and analyze the security of the proposed protocol. Our proposed mechanism is suitable and appropriated for wired multicast services together with mobile applications due to simple authentication procedure using hash value of a client and server

As future works, we will compare the proposed protocol with other password-based authentication protocols from the viewpoint of the performance and efficiency. Also we will present an advanced method which can increase the randomness of two verifiers and the session key.

References:

[1] Wireless Application Protocol Wireless Layer Security, *WAP Forum, 6th*, 2001.

[2] V. Boyko. A, Mackenzie. P. and Patel. S., Provably Secure Password Authenticated Key Exchange Using Diffie-Hellman, *Advances in Cryptology-EUROCRYPT 2000*, LNCS 1807, pp. 156-171, 2000.

[3] Wu. T, Secure remote password protocol, *Proceedings of the 1998 Internet Society Network and Distributed System Security Symposium*, pp. 97-111, 1998.

[4] Mackenzie. P and Swaminathan. R, Secure Network Authentication with Password Identification, *Presented to IEEE P1363.2*, 1999.

[5] Bellare. M and Rogaway. P, The AuthA protocol for password –based authenticated key exchange, *IEEE P1363.2*, 2000.

[6] Blake-Wilson. S and Menezes. A, Authenticated Diffie-Hellman Key Agreement Protocols, *Selected Areas in Cryptography '98-SAC '98*, LNCS 1556, pp. 339-361, 1998.