The password-based key exchange protocol using a password-hardening protocol

SANG-MAN AHN*, SOO-HYUN OH*, DONG-HO WON*
Information and Communications Security Laboratory
* School of Information & communication Engineering, SungKyunKwan University,
300 Chunchun-dong, Jangan-gu, Suwon, Kyunggi-do
KOREA
{smahn, shoh, dhwon}@dosan.skku.ac.kr

Abstract: We describe the password-hardening protocol proposed by Ford and Kaliski[12] and propose a new 1-pass password-based key exchange protocol using the password-hardening protocol and Nyberg-Rueppel's scheme[9]. The verifier stored in the server's database is blinded by the blinding factor of client and server, respectively. Therefore, our protocol will reduce the server compromise attack and remove a credentials server. The security of proposed protocol is depended on the DLP(Discrete Logarithm Problem) and DHP(Diffie-Hellman Problem)[10]. We prove that the proposed protocol has the characteristics of forward secrecy and is secure against the server spoofing, Server data eavesdropping, known-key attack such as Denning-Sacco Attack[1].

Key-Words: Password authentication, Key agreement, Security

1 Introduction

The password-authenticated key exchange problem can be informally stared as follows. Two entities who only share a password wish to set up a secure session over an insecure network[13]. However, a complex problem with password only authentication is a password has low entropy(uncertainty) so that it is vulnerable to guessing attack.

Lomos et.al.[2] presented the first protocols which were resistant to off-line dictionary attacks. The protocols assumed that the client had the server's public key of this protocols thus were not strictly password-only protocols. Also, the protocols must use the server's public key, there is additional requirement that must use complicated and inefficient *PKI(Public Key infrastructure)*.

Bellovin and Merritt [3] proposed EKE(Encrypted Key Exchange) that is first password-authenticated key exchange protocol that did not require the server's public key. The EKE was to user the password to symmetrically encrypt the protocol message of DH(Diffie-Hellman) key exchange[10]. Therefore, an attacker can decrypt the symmetric encryption by guessing attack about password, but cannot break the asymmetric encryption in the message, and thus cannot verify the guessed-value.

Since Bellovin and Merrit introduced the EKE, many protocols for password-authenticated key exchange were proposed which did not require the user to know the server's public key and satisfied the new special quality(e.g., forward secrecy, known key attack, server compromise). But, most of protocols for password-authenticated key exchange always secretly stored the verifier derived from the client's password, even if the protocols are verifier-base mechanism.
The server master, or attacker who compromises the server, can always mount an exhaustive attack on the client's password. That is, if the attacker gains access to the server's database, he can exhaustively guess password, apply the derivation function, and compare the results with the stored value.

To solve this problem, Ford and Kaliski's methods [12] use multiple servers to further prevent guessing attacks by an enemy that compromises all but one server.

In this paper, we will propose the efficient 1-pass password-based key exchange protocol. The password-authenticated key exchanges are preformed by verifier-based mechanism using the password-hardening protocol proposed by Ford and Kaliski[12] and Nyberg-Rueppel one-pass scheme[9]. The verifier stored in the server's database is blinded by the blinding factor of client and server, respectively. Therefore, our protocol will reduce the server compromise attack and remove a credentials server.

In section 2, we describe the password-hardening protocol proposed by Ford and Kaliski[12]. Section 3 proposes the new password-authenticated key exchange protocol using the verifier. In section 4,

discuss its security. Finally, section 5 concludes this paper.

2 The password-hardening protocol

Ford and Kaliski[12] described about the password-hardening protocol using the multiple server to prevent the password verifier that is stored to the server from cheating of adversary. Before protocol explanation, we summarize the notation about the symbols that is used in this paper. Table 1 shows the notation.

The goals of this section obtain a value R from the client's password p. It should not be possible for an outside attacker to determine R by exhaustive search, the server should not learn R or p, and the same value R should be obtained each time the user runs the protocol with a given password. Achievement process of this protocol is as following.

In setup step for process the password-hardening protocol, the server selects a prime p such that $p = 2q - 1$ where q is a large prime factor of $p - 1$, and for each client selects the secret exponent d_C between 1 and $q - 1$, and publish a prime p. The server also publishes a function f that maps password to elements of multiplicative order q in Z_p^*.

Each time the client wants to blind the password and she engages in the following interactions with the server:

1. The client computes $r \equiv f(p)^k \bmod p$, where $k \in Z_q$ is a secret random exponent, and sends ID_C and r to the server.

$$\text{Client} \rightarrow \text{Server}: \ ID_C, r \tag{1}$$

2. The server computes $V \equiv r^{d_C} \bmod p$ and sends ID_S and V to the client.

$$\text{Server} \rightarrow \text{Client}: \ ID_S, V \tag{2}$$

3. The client computes $R \equiv V^{k^{-1}} \bmod p$, where k^{-1} is the inverse of $k \bmod p$.

$$\text{Client}: \ R \tag{3}$$

As a result of this protocol, the client obtain $R \equiv f(p)^{d_C} \bmod p$ and the server reserved the value V as the client's verifier. Also, the exponent k serves as a blinding factor, so the server does not learn any information about the client's password p from r, and consequently does not learn the hardened password R. The value R is a strong secret since it depends on the secret exponent d_C. The server can't calculate the client's verifier, as verifier is blinded by private key k of the client's blinding factor, vise-versa. Therefore, when the verifier is exposed to attacker, if he can exhaustively guess passwords, he cannot compare the results with the exposed verifier. We will omit to describe the basic constraint, because above the password-hardening protocol is resembled with Ford and Kaliski's protocol. This progress is used by set-up step of our protocol

Table 1. The details of a notation in proposed scheme

p	Large prime modular $(p = 2q - 1)$
q	Large prime factor of $p - 1$
ID_C	Client' s name or address bit string
ID_S	Server's name or address bit string
V	Verifier stored in server's password file
p	Client's password
k	Client's secret random number
$f(p)$	A function that converts p in to a suitable DH base
x, r	Randomly chosen integers
d_C	Secret key about each Client that is created by server
K	Session key

3 The proposed protocol

We propose the efficient 1-pass password-based key exchange protocol. The password-authenticated key exchange is preformed by verifier-based mechanism using the password-hardening protocol proposed by Ford and Kaliski[12] and Nyberg-Rueppel one-pass scheme[10]. To authenticate the client and exchange the session key, the client engage in the following interactions with the server:

1. The client computes $e \equiv f(p)^{x-r} \bmod p$ and $s \equiv k^{-1} \cdot r + e \bmod q$, where $x, r \in Z_q$ is a random exponents and sent (e, s) to the server.

$$\text{Client} \rightarrow \text{Server}: \ ID_C, e, s \tag{4}$$

To compute the session key, the client computes as follows:

$$K \equiv R^x \bmod p \tag{5}$$

2. The server verifies the value $e \neq 0 \bmod p$, $s \neq 0 \bmod p$ and compute the session key K as follows:

$$K \equiv V^s \cdot V^{-e} \cdot e^{d_C} \bmod p \tag{6}$$

After the protocol is processed, both sides will agree on the session key $K \equiv f(p)^{x \cdot d_C} \bmod p$, if all steps are executed correctly.

4 Security analysis

The protocol proposed in this paper reduced sharply danger about the exposure of verifier stored in the server's database. The verifier about the client's password is blinded by the client's blinding factor and the server's blinding factor, respectively. Thus, even if the attacker can obtain the verifier, our protocol prevent exhaustive password guessing attack, because even client and server can not compute the verifier without both side's cooperation.

By assumption of DLP(Discrete Logarithm Problem) and DHP(Diffie-Hellman Problem), our protocol has the security against password guessing attack, Server spoofing, Server data eavesdropping, Forward Secrecy, Denning-Sacco attack[1] etc.

Detailed proof about each special quality is as follows.

4.1 Resistance to Guessing attack

If Eve is a passive attacker, information that is given to an attacker is as follows;

$$p,\ q,\ f(p)^{x-r} \bmod p, k^{-1} \cdot r + e \bmod q.$$

If Eve guesses the password p', then she finds $e' \equiv f(p')^{x-r} \bmod p$, $e \equiv k^{-1} \cdot r + e \bmod q$.

Also, she guesses the session key $K \equiv f(p')^{x \cdot d_C} \bmod p$.

To verify the password, she must solve the DLP and DHP. But, by assumption of the DLP and DHP, any information that can verify the password is not offered to passive attacker.

4.2 Resistance to Server spoofing

At process that calculate the key token $f(p)^x \bmod p$ to compute the session key using public information that the client transmits, only real server that know a secret key d_C of the client can compute the key token $f(p)^x \bmod p$.

Thus server spoofing can be prevented.

4.3 Resistance to Server date eavesdropping

Even in case that the password verifier that is stored to the server is exposed to the intruder, he can't impersonate the client. To exchange the session key, he has to use the password as a base $f(p)$ to compute the session key, but he can not derived password from the verifier. In case of password guessing attack, as the verifier, V is blinded by a secret random value of client and server, respectively, as long as DLP and DHP isn't broken, password guessing attack using the exposed verifier also impossible.

Thus, server data eavesdropping can be prevented.

4.4 Forward secrecy

The preceding proof establishes that it is computationally infeasible to construct a session key even with the client's password and all publicly- visible information. In our protocol, even if the client's password is revealed to the active attacker, he can't construct the session key of past sessions. It is equal to DLP and DHP that construct the session key using publicly-visible information and password. Thus, our protocol satisfies the security against forward secrecy.

4.5 Resistance to the Denning-Sacco Attack

The Denning-Sacco Attack[1] occurs when an intruder Eve captures the session key K from an eaves-dropped session and uses it either to gain the ability to impersonate the user directly or to conduct a brute-force search against the client's password.

If K is revealed to a passive intruder Eve, she does not learn any new useful information from combining and values . Also, to verify a password, she must solve the DLP and DHP.

This problem is proved already in chapter 4.1.

4.5 Implicit Key Authentication

Our Protocol exchange the session key by communication of once, unlike many password-authenticated key exchange schemes that proposed before. Therefore, unlike other protocols, the characteristics of mutual authentication is not satisfied. But, at process that generate the session key, the client compute the session key using value R signed by the server and the server creates the session key using own secret key d_C and verifier V and public information.

So, our protocol satisfies the characteristics of implicit key authentication.

5 Conclusion

In this paper, we describe the password-hardening protocol proposed by Ford and Kaliski [12] and propose a new efficient 1-pass password-based key exchange protocol which both entities agree on the correct Diffie-Hellman exponent $f(p)^{x \cdot d_C} \bmod p$, using the password-hardening protocol and Nyberg-Rueppel's scheme. Also, the security of proposed protocol is depended on the DLP and DHP[10].

As we mentioned earlier, we prove that the proposed protocol has the characteristics of forward secrecy and is secure against dictionary attack, server spoofing, server data eavesdropping, known-key attack such as Denning-Sacco Attack[1].

References:

[1] D. Denning and G. Sacco, Timestamps in key distribution. *Communications of the ACM*, August 1981.

[2] T. M. Lomos, L. Gong, J. H. Saltzer, and R. M. Needham, Reducting risks from poorly chosen keys, *ACM Operating systems Review, Proceeding of the 12th ACM Symposium on Operating systems Principles*, 23(5): Dec. 1989, pp 14-18.

[3] S.M. Bellovin, M. Merritt, Eencrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks, *Proceedings of the IEEE Symposium on Research in security and Privacy*, 1992.

[4] S.M. Bellovin, M. Merritt, Augmented Encrypted Key Exchange : a Password-Based Protocol Secure Against Dictionary Attacks and Password File Compromise, *Proceedings of the First ACM Conference on Computer and Communications Security*, 1993.

[5] S.M. Bellovin, M. Merritt, Attack on the Interlock Protocol When Used for Authentication, *IEEE Transactions on Information Theory* 40:1, January 1994, pp. 273-275.

[6] D.P. Jablon, Strong Password-Only Authenticated Key Exchange, *Computer Communication Review, ACM SIGCOMM*, vol.26, no.5, October 1996, pp5-26.

[7] D.P. Jablon, Extended Password Key exchange Protocols Immune to Dictionary Attack, *In WETICE '97 Enterprise Security Workshop*, Cambridge, MA, June 1997.

[8] T. Wu, The Secure Remote Password Protocol, *Internet Society Symposium on Network and Distributed System Security*, 1998.

[9] K. Nyberg and R. Ruppel, A new signature scheme based on DSA giving message recovery, *Proc, 1st ACM Conf, on Comput. Commun. Security*, 1986, pp. 58-61.

[10] W. Diffie and M. Hellman, New directions in cryptography, *IEEE Trans. Inf. Theory*, vol.IT-22, no.6, , 1976, pp. 644-654.

[11] S. Patel, Number theoretic attacks on secure password schemes. *In Proceeding of the IEEE Symposium on Research in Security and Privacy*, 1997, pp. 236-247.

[12] W. Ford & B. Kaliski, Server-Assisted Generation of a Strong Secret from a Password, *Proceedings of the IEEE 9th International Workshops on Enabling Technologies: NIST*, Gaithersburg MD, June 14-16, 2000.

[13] P. MacKenzie, On the Security of the SPEKE Password-Authenticated Key Exchange Protocol, *Cryptology Print Archive: Report* , 2001.