Trends in Applied Sciences Research

ISSN 1819-3579

Academic
Journals Inc.

www.academicjournals.com

Trends in Applied Sciences Research 2 (5): 456-459, 2007
ISSN 1819-3579

Password-Based Key Authentication Model-A New Approach

Yasir Khalil Ibrahim
Department of Computer, Jerash Private University, Jordan

Abstract: In network communication, security plays an important role. Recently Password-based authenticated key agreement plays an important role for providing secure transmission. In this study, securities vulnerabilities exist in the password-only authenticated key exchange are identified and a new approach is discussed to overcome those vulnerabilities. A combination of a picture function and a distortion function is adopted to authenticate the user and protect the password from malicious attack. A Nonce value is added in control frames to enhance the authentication process to identify the sender and receiver.

Key words: Password-based key, authentication, cryptography, nonce, communication, network security

INTRODUCTION

Password-based authenticated key agreement plays an important role in network communication. In the existing schemes, the secret password is shared between the sender and the receiver. In recently proposed password-based authenticated key establishment methods (Laih *et al*., 2005; Bellare and Rogaway, 2000) a user and a server can authenticate each other and negotiate a session key. In Jablon and LDH schemes (Laih *et al*., 2005; Tang and Mitchell, 2005), a special function is adopted to authenticate the user so as to protect the password from offline dictionary attacks (Bellare and Rogaway, 2000).

It has been shown that the above protocols suffer from some attacks such as offline dictionary attacks. It implies that the attacker can hack the messages sent during the protocol execution and use them as the basis for an exhaustive search for the password without initiating any new protocol instance. In this study, a new password-based authentication model is proposed based on the existing models. The proposed model is secure against the malicious attacks.

DESCRIPTION OF EXISTING KEY AUTHENTICATION SCHEMES

In recently proposed password-based key authentication schemes (Laih *et al*., 2005; Tang and Mitchell, 2005), a special function is defined as $\varphi(r, s) = g(p(r, s))$, where g is a distortion function and p is a picture function (Bellovin and Merritt, 1992). From the given inputs r and s, where r is a random string of characters and s is a random number, p generates a random picture. By giving an input, a picture, p(r, s) the distortion function g generates a distorted version $R' = g(p(r, s))$, so that we have the ability to recognize r from R'.

Suppose {Epw,Dpw} denotes a pair of symmetric encryption/decryption functions, where pw (a password) is the secret key. Here a h denotes a one-way hash function and n is a security parameter. All these system parameters except pw are made known to all relevant parties. The secret key pw (a password) is only known to the user and the server.

SECURITY VULNERABILITY IN EXISTING SCHEMES

In the existing method, some possible vulnerability is pointed out that leads to insecurity in the transmission for authentication. The following insecure situations are identified during transmission:

- When one entity shares the same password with at least two other entities, a malicious third party can mount the attack (Tang and Mitchell, 2005) For Example:
  Suppose that a client U whose identity ID_U, shares a password pw with two different servers, namely S_1 with identity ID-S_1 and S_2 with identity ID-S_2. Here a malicious third party can mount the attack. Suppose a client U initiate the protocol with an attacker that is impersonating server S_1. Meanwhile the attacker also initiates the protocol with server S_2, impersonating U. The attacker now forwards all messages sent by U (meant for S_1) to S_2. Also, all messages sent from S_2 to U are forwarded to U as if they come from S_1.
  This attack demonstrates that even if the server (S1) is absent, the attacker can make the client believe that the server is present.
- A human being must be able to easily recognize r from $D_{pw}(\varphi (r, s))$, which implies that $D_{pw}(\varphi (r, s))$ is very different from a completely random picture.
- If $pw' \neq pw$ then $D_{pw}'(\varphi (r, s))$ will resemble a random image. So it implies that it is possible to determine whether or not a guessed password pw' is correct merely by deciding whether $D_{pw}'(C_1)$ is a (distorted) image or not, where $C_1 = Epw(\varphi (r, s))$.
- It is very simple to develop software to distinguish between a distorted image and a random pattern. This is certainly a much simpler problem than automatic string.
  The following are some possible attacks that show the insecure on authentication.
  - In some cases it might be feasible for a machine to mount an offline password guessing attack. The machine works for all possible passwords and for each guessed password pw', the machine computes $A = D_{pw}'(C_1)$ where $C_1 = Epw(\varphi (r, s))$. Now the machine checks whether or not A resembles a distorted image rather than a random bit pattern. Here the correct password can be identified from the unique case where A is a distorted image rather than a random bit pattern. This attack only requires a machine-based search.
  - Checking the most likely passwords first can make the process significantly faster.
  - Even if the method of distinguishing random from genuine images is not perfect, then a human can be used to check the remaining candidate values A to eliminate all but the value corresponding to the correct password.
  - Distributed attacks are also possible. It may be possible to deploy a cooperative Internet-based attack.

Here it shows that the image recognition used to protect secrecy is seems to be risk.

PASSWORD-BASED KEY AUTHENTICATION MODEL

The existing schemes suffer from a number of vulnerabilities, which are mainly caused by the distortion function φ. The difficulty of these problems would appear to be much less well established than that of problems on which cryptographic protocols are typically based. The process is improved on password-based key scheme on which a user is involved in each communication.

In the proposed scheme, the following evaluations are made:

Consider a user U with identity ID_U and a server S with identity ID_S share a secret password pw. Consider two large prime numbers, say p and q and perform any permutation relating these numbers such that result of computation on q should match with p and execute a secure one-way hash function h on it.

- In one case, by including the identities of the participants, the attack can be controlled.
- In another case, When U and S want to negotiate a session key, then

Compute $g = h (pw \| ID_U \| ID_S \| i) \bmod p$, where i is the smallest integer.
Now U and S perform the following steps:

- U generates a random number t_1 and sends $m_1 = g^{t1} \bmod p$ to S.
- After receiving m1, S generates a random number t_2 and sends $m_2 = g^{t2} \bmod p$ to U. S uses a scheme to construct a distorted picture $\varphi (r)$, where r is a random string and also sends $\varphi (r)$ to U.

Now S computes $z = g^{t2.t1} \bmod p$ as the shared key material and computes $K = h (z\|1)$ as the shared key.

- U receives m_2. Now U can recognize r from the distorted picture $\varphi (r)$ and computes $z = g^{t2.t1} \bmod p$ as the shared key material and computes $K = h (z\|1)$ as the shared key.

Now U constructs and sends the confirmation message to S:

$$C_1 = h(\varphi(r)\|r\|3\|m_1\|m_2\|g^{t2.t1}\|g\|ID_U\|ID_S)$$

- S receives C_1. S checks that received message equals

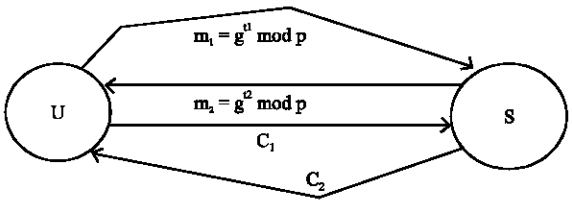
$$h(\varphi(r)\|r\|3\|m_1\|m_2\|g^{t2.t1}\|g\|ID_U\|ID_S)$$

If it fails then S terminates the execution.
If it succeeds, then S computes and sends the message (C_2) to U:

$$C_2 = h(4\|m_1\|m_2\|g^{t2.t1}\|g\|ID_U\|ID_S)$$

- After receiving C_2, U checks that the received message equals

$$h(4\|m_1\|m_2\|g^{t2.t1}\|g\|ID_U\|ID_S)$$



Where

$$C_1 = h(j(r)\|r\|3\|m_1\|m_2\|g^{t2.t1}\|g\|ID_U\|ID_S)$$

$$C_2 = h(4\|m_1\|m_2\|g^{t2.t1}\|g\|ID_U\|ID_S)$$

If the check fails, U terminates the execution. Otherwise, U confirms that the execution is successfully tested.

A Nonce (Stallings, 2003) value is a locally generated pseudorandom number and appears in responses. Once used Nonce value cannot be reused. Also it can be encrypted during certain portions of exchange for security purpose.

The concept of Nonce is incorporated in the proposed scheme, which provides additional security. It is added in each transaction to improve the authentication process and C_1 is replaced with the following function either as a Nonce value or an Encrypted version of Nonce value.

$$C_1 = h(\varphi(r)||r||3||m_1||m_2||g^{t2.t1}||g||ID_U||ID_S||N)$$

or

$$C_1 = h(\varphi(r)||r||3||m_1||m_2||g^{t2.t1}||g||ID_U||ID_S||E_k[N])$$

Where E_k is Encryption using key k.

Every transaction has new Nonce value, so that a new transmission can be identified with its originator. i.e., it authenticates the sender.

FEATURES

The proposed model has the following key features

- The identities of the participants are included in the authentication message.
- The special function scheme, which is a combination of a picture function and a distortion function adopted to authenticate the user, guarantees that a human is involved in an ongoing protocol execution.
- Even if the special function scheme is attacked, the security of improved password-key doesn't compromise.
- The usage of Nonce values uniquely identify that the reply is from correct user so that unauthorized access is denied.

CONCLUSIONS

In this study, the potential security vulnerabilities exist in the strong password-only authenticated key exchange and the solutions to over come those vulnerabilities are discussed. A combination of a picture function and a distortion function is adopted to authenticate the user and to protect the password from certain malicious attacks is given. By providing Nonce values to each communication, the identification of the originator can be uniquely identified. Finally, the proposed scheme removes the security vulnerabilities and provides a better security for communication using password-based authentication scheme.

REFERENCES

Bellare, M. and P. Rogaway, 2000. Authenticated key exchange secure against dictionary attacks. IEEE., pp: 1363.

Bellovin, S.M. and M. Merritt, 1992. Proceedings of the 1992. IEEE Symposium on Security and Privacy, Washington, DC, USA., pp: 72-84.

Laih, C.S., L. Ding and Y.M. Huang, 2000. Password-only authenticated key establishment protocol without public key cryptography. Electron. Lett., pp: 185-186.

Stallings, W., 2003. Cryptography and Network security. Principles and Practices. 3rd Edn.,

Tang, Q. and C. Mitchell, 2005. On the security of some password-based key agreement schemes. Information Security Group.