A New Improved Secure Password Authentication Protocol to Resist Guessing Attack in Wireless Networks

Y.-C. Lee[1], Y.-C. Hsieh[2] and P.-S. You[3]
1: Department of Electrical Engineering, WuFeng Institute of Technology. Ming-Hsiung, Chia-Yi 621, Taiwan.
2: Department of Industrial Management, National Formosa University Huwei, Yunlin 632, Taiwan.
3: Graduate Institute of Transportation and Logistics, National ChiaYi University Chia-Yi 600, Taiwan.

Abstract: - Wireless communication is widely used today. It transmits information through an open network such that it always suffers by a variety of attacks. In 2006, Yoon et al. proposed a secure password authentication protocol for wireless networks to fix the drawback of Ma et al.'s protocol. In this article, we will show that the Yoon et al.'s protocol is vulnerable to both off-line password guessing attack and replay attack. We will present a new improved protocol to fix the flaw. As shown, the improved protocol is secure while the computation cost is quite low.

Key-Words: - Password authentication, Off-line guessing attack, Network security.

1 Introduction

With the rapid development of communication technologies and computer networks, wireless networks are widely used today. Wireless communications transmit information through air instead of wires, and it provides people convenient and easy ways to communicate each other. However, because it transmits information through open channels, the security issue becomes more significant than that of traditional wired networks. For the wireless communications, any potential attackers can easily eavesdrop transmitted information and attack the systems. Unfortunately, it is very difficult to detect or exclude attackers in wireless communications.

In order to effectively protect information from being attacked in wireless network, many security mechanisms have been developed. For example, the well-known Wired Equivalent Privacy (WEP) protocol was introduced in the ANSI/IEEE 802.11 standard [3]. However, it has been proved that security of the protocol cannot be guaranteed [7].

Password Authentication Protocol (PAP) is widely used in the Point-to-Point Protocol to authenticate users. The RADIUS protocol, which supports the PAP Protocol, is widely used in network environments [1]. In 2004, Kim and Choi [2] showed that the PAP-based RADIUS protocol, which is used in 802.11, cannot resist the man-in-the-middle attack [4, 6], and they presented an improved protocol to resist the attack. In 2006, Ma et al. [5] found the flaws in both the original version and improved version of the PAP protocol, and they presented an enhanced PAP protocol (M-PAP) to improve the security. In 2006, Yoon et al. have shown that the Ma et al.'s M-PAP protocol is still vulnerable to off-line password guessing attacks [8], and they presented an improved protocol to fix the flaw.

Authentication schemes which use weak keys such as passwords are vulnerable to guessing attacks. As known, password guessing attacks include both on-line attacks and off-line attacks. An on-line password guessing attack happens when an attacker attempts to guess the password in an on-line transaction, while an off-line password guessing attack happens when an attacker guesses the password and verifies his guess off-line. A replay attack is an attacker to impersonate a legal user by reusing the message obtained in previous authentication sessions. Efficient ways to resist replay attacks include using timestamp and nonce.

In this article, we will first show that the Yoon et al.'s protocol is not as secure as they declared. As shown, their protocol cannot stand off-line guessing attack. Moreover, their protocol cannot resist replay attack. We will present a new improved protocol to enhance the security.

The rest of the paper is organized as follows. In Section 2, we will briefly review Yoon et al.'s protocol. The drawbacks of the Yoon et al.'s protocol are discussed in Section 3. Next, the new improved protocol and its security analysis are presented in Sections 4. Finally, we will make brief conclusions.

2 Review of Yoon et al.'s protocol

Let *S* be an authentication server, *A* and *B* are names or identities of two users. Assume that *A* is the sender who wants to communicate with *B*.

Throughout this article, all notations are defined as follows.

KS : server's public key.

K_{AB}: a symmetric key shared by *A* and *B*. The server stores the symmetric key in a table secretely.

P : password shared by *A* and *B*.

$\{m\}_{KS}$: the message *m* is encrypted with server's public key *KS*.

$h(\cdot)$: a secure hash function such as SHA-1.

$\oplus$: a bit-wise exclusive OR operation.

X → *Y*: *m* : *X* sends a message *m* to *Y*.

Yoon et al.'s protocol [8] includes the following four steps.

(Y-1) *A* → *S*: $\{A, N_A, P\}_{KS}$

The user A generates a nonce N_A, and encrypts N_A with *A* and *P* by using server's public key *KS*. Next, A sends a message $\{A, N_A, P\}_{KS}$ to the server *S*.

(Y-2) *S* → *B*: $S, N_S, P \oplus h(N_S, K_{AB})$

On receiving $\{A, N_A, P\}_{KS}$, *S* decrypts it by using his private key and verifies whether *A* holds. If it holds, *S* generates a nonce N_S and computes $P \oplus h(N_S, K_{AB})$. Then, *S* sends $\{S, N_S, P \oplus h(N_S, K_{AB})\}$ to *B*.

(Y-3) *B* → *S*: $\{B, h(N_S, K_{AB})\}_{KS}$

After *B* receives $\{S, N_S, P \oplus h(N_S, K_{AB})\}$ from *S*, *B* computes $h(N_S, K_{AB})$ and obtains *P* by computing $P \oplus h(N_S, K_{AB}) \oplus h(N_S, K_{AB})$. Then, *B* verifies whether *P* holds. If it holds, *B* sends $\{B, h(N_S, K_{AB})\}_{KS}$ to *S*.

(Y-4) When *S* receives $\{B, h(N_S, K_{AB})\}_{KS}$ from *B*, *S* decrypts $\{B, h(N_S, K_{AB})\}_{KS}$ by using his private key and verifies whether *B* and $h(N_S, K_{AB})$ hold. If they hold, *S* believes the responding party is real *B*. Then *S* informs *A* with an acknowledgement.

3 Drawbacks of Yoon et al.'s protocol

The Yoon et al.'s protocol [8] was designed to fix M-PAP protocol which is vulnerable to off-line password guessing attacks. However, in this section, we will show that Yoon et al.'s protocol cannot withstand off-line password guessing attacks. As shown below, attackers can obtain exact password to impersonate legal mobile users since they can check the correctness of the guessed password. The off-line password guessing attacks on Yoon et al.'s protocol is as follows.

(D-1) Suppose that at previous sessions of communication, the attacker *C* intercepts $\{S, N_S, P \oplus h(N_S, K_{AB})\}$ and $\{B, h(N_S, K_{AB})\}_{KS}$ in step (Y-2) and (Y-3), respectively.

(D-2) *C* randomly chooses a candidate password *P'* from password dictionary *D*. Then attacker *C* computes $P \oplus h(N_S, K_{AB}) \oplus P'$.

(D-3) *C* encrypts $P \oplus h(N_S, K_{AB}) \oplus P'$ along with *B* by using server's public key K_S, and checks whether $\{B, P \oplus h(N_S, K_{AB}) \oplus P'\}_{KS}$ is equal to the received $\{B, h(N_S, K_{AB})\}_{KS}$ or not.

(D-4) If $\{B, P \oplus h(N_S, K_{AB}) \oplus P'\}_{KS}$ is equal to $\{B, h(N_S, K_{AB})\}_{KS}$, it means that *P'* is the real password *P*.

(D-5) If it is incorrect, *C* performs step 2 to step 4 until $\{B, P \oplus h(N_S, K_{AB}) \oplus P'\}_{KS}$ is equal to $\{B, h(N_S, K_{AB})\}_{KS}$.

Note that, for memory reasons, the bit-length of the password is usually quite short. Thus an attacker can easily obtain the exact password by repeating step (D-2) to step (D-4). By using the guessed password *P'*, an attacker *C* can successfully impersonate user *A* to communicate with user *B*. Therefore, the off-line password guessing attack is also effective to Yoon et al.'s protocol.

Moreover, the PAP protocol suffers from the replay attack since attackers can replay the message (Y-1) to the server, and the server and receiver *B* will respond as if it is really from *A*. Though attackers cannot communicate with the receiver successfully (since K_{AB} is unknown), attackers still can fool the server and users.

4 The new improved protocol

The off-line guessing attack on Yoon et al.'s protocol can work is due to the message on step (Y-2) and step (Y-3) which both contain information $h(N_S, K_{AB})$. The attackers can verify their guessing with these messages. A password authentication protocol can stand guessing attack only if attackers cannot verify their guessing. We propose a improvement protocol to fix the flaws. The new improved protocol is described as follows.

4.1 The new improved protocol

(I-1) $A \rightarrow S$: $T_A, \{A, N_A, T_A, P\}_{KS}$

The user A generates a nonce N_A, and encrypts N_A with T_A, A and P by using server's public key KS, where T_A is the timestamp. Next, A sends a message $T_A, \{A, N_A, T_A, P\}_{KS}$ to the server S.

(I-2) $S \rightarrow B$: $S, T_A, P \oplus h(T_A, K_{AB})$

On receiving $T_A, \{A, N_A, T_A, P\}_{KS}$, sender S decrypts it by using his private key. The server S checks whether T_A is in a valid time period or not, and verifies whether A holds. If both of them holds, S computes $P \oplus h(T_A, K_{AB})$. Then, S sends { $S, T_A, P \oplus h(T_A, K_{AB})$ } to B.

(I-3) $B \rightarrow S$: $T_B, \{B, h(T_B, K_{AB})\}_{KS}$

After B receives { $S, T_A, P \oplus h(T_A, K_{AB})$ } from S, B computes $h(T_A, K_{AB})$ and obtains P by computing $P \oplus h(T_A, K_{AB}) \oplus h(T_A, K_{AB})$. Then, B verifies whether P holds. If it holds, B sends $T_B, \{B, h(T_B, K_{AB})\}_{KS}$ to S. Where T_B is the timestamp of B.

(I-4) When S receives $T_B, \{B, h(T_B, K_{AB})\}_{KS}$ from B, S checks whether T_B is valid. Then the server decrypts $\{B, h(T_B, K_{AB})\}_{KS}$ by using his private key and verifies whether B and $h(T_B, K_{AB})$ hold. If they hold, S believes the responding party is real B. Then S informs A with an acknowledgement.

To illustrate our point, the new improved protocol is shown in Figure 1. Both the new improved protocol and Yoon et al.'s protocol require two-time asymmetric encryption/ decryption operations. The computation cost of the new improved protocol is quite low.

Not that if the computers or digital devices such as PDAs of users are lack of time clock to generate timestamp, the nonce can be used to replace timpstamp. In this case, the nonce should be renewed and checked on each session to avoid replay attack.

4.2 Security Discussions

The new improved protocol can resist password guessing attacks and replay attacks. The main reasons are described as follows.

(1) *It can resist off-line password guessing attacks*. Because there is no common element for attackers to check the correctness of the guessing password, they cannot find the exact password with off-line password guessing attack. That is, if attackers intercept the messages from step (I-1) through step (I-4) and try to guess the exact password, they cannot find the real password because of no adequate information for verification. Therefore, the new improved protocol can resist off-line password guessing attacks.

(2) *It can resist replay attack*. The new improved protocol adopts the timestamp mechanism, and if attackers resend the message intercepted on step

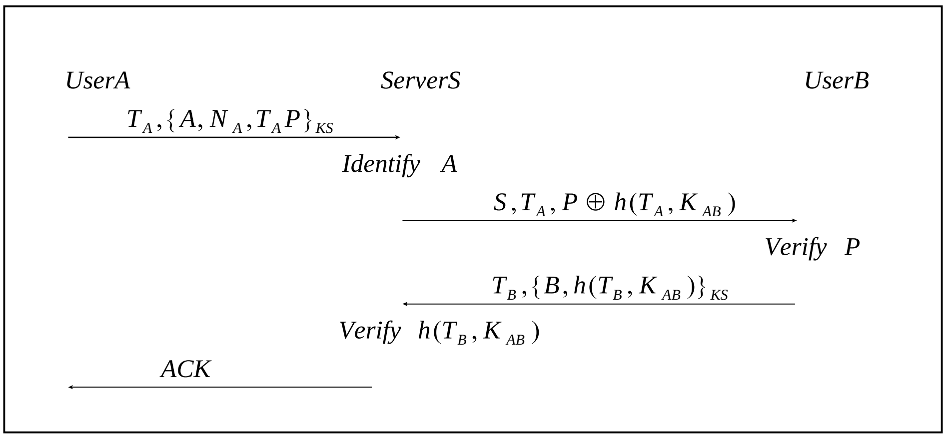

Figure 1. The improvement protocol

(I-1), both the server and the receiver will reject the request. Similarly, if attackers masquerade as a legal receiver and replay the message recorded on step (I-3) of previous session, the server will reject the communication by checking the timestamp. Thus the replay attack can be avoided in the new improved protocol.

5 Conclusions

Password authentication protocol is a simple mechanism to authenticate users for networks. This article has shown that Yoon et al.'s secure password authentication protocol cannot resist off-line password guessing attack and replay attack. In addition, we have presented a new improved protocol to fix the drawbacks. The new improved protocol is secure while the computation complexity is quite low.

References

[1] J. Hassell. *RADIUS*, O'Reilly, 2002.

[2] I. G. Kim and J. Y. Choi. "Formal verification of PAP and EAPMD5 protocols in wireless networks: FDR model checking", *Proceedings of the 18th International Conference on Advanced Information Networking and Applications* (AINA 2004), Fukuoka, Japan, pp.264-269, March 2004,

[3] LAN MAN Standards Committee of the IEEE Computer Society, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, ANSI/IEEE Standard 802.11, June 2003.

[4] G. Lowe. "Casper: a compiler for the analysis of security protocols", *The 10th IEEE Computer Security Foundations Workshop*, pp.18-30, 1997.

[5] X. Ma, R. McCrindle1 and X. Cheng, "Verifying and fixing password authentication protocol", *Proceedings of the Seventh ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing* (SNPD 2006), Las Vegas, Nevada, USA, pp.324-329, June 2006.

[6] P.Y. A. Ryan and S.A. Schneider, *Modeling and analysis of security protocols: the CSP approach*. Addison-Wesley, 2001.

[7] J. R. Walker, "Unsafe at any key size; An analysis of the WEP encapsulation", *Technical Report 03628E*, IEEE 802.11 Committee, 2000.

[8] E.J Yoon, K.Y Yoo, "Secure Password Authentication Protocol in Wireless Net-works", *The 2006 International Conference on Next Generation Web Services Practices* (NWeSP'06), pp.149-154, 2006.