Buletinul Ştiinţific al Universităţii "Politehnica" din Timişoara

Seria ELECTRONICĂ şi TELECOMUNICAŢII
TRANSACTIONS on ELECTRONICS and COMMUNICATIONS

Tom 53(67), Fascicola 2, 2008

On The Improvement of Password Authentication Protocol in Wireless Network

Seifedine Kadry[1], Khaled Smaili[2]

Abstract – In 2006, Ma et al. found flaws in the original and fixed versions of the PAP protocol by using a new knowledge based framework, and presented an enhanced PAP (M-PAP) protocol. In 2006 also, 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 still 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.

Keywords: Cryptography, Wireless network, PAP protocol, Off-line password guessing attack.

I. INTRODUCTION

With the rapid development of network communications, an increasing range of computing devices are being used. Mobile computing devices, such as laptop computers and PDAs, are widely used in different network environments, where cable connection to the Internet is not always convenient or even possible. As a result, wireless connection and communication have become necessary to liberate people from the restrictions of network cables and sockets and to realize mobile computing [10]. Since information in wireless computing environments is transmitted through air instead of wires, the issue of security becomes more significant than when transmission occurs across traditional wired networks [9]. Any potential attackers, with an appropriate radio receiver, can eavesdrop transmitted information without much effort [11]. It is difficult to detect such attackers in wireless communications.

Password Authentication Protocol (PAP) is widely used in the Wireless Fidelity Point-to-Point Protocol to authenticate an identity and password for a peer.

In 2004, Kim and Choi [2] showed that PAP-based RADIUS protocol [1], which is frequently used in 802.11, is vulnerable to a man-in-the-middle attack by using Casper and CSP/FDR model checking tool [4], and presented an improved protocol that can withstand the attack. In 2006, Ma et al. [5], however, found flaws in both the original and improved versions of the PAP protocol by using a new knowledge-based framework, and presented an enhanced PAP (M-PAP) protocol.

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.

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.

II. Off-line versus On-line attack

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.

III. Drawbacks of Yoon et al.'s protocol

First, we shall the Yoon et al.'s protocol then we shall discuss its drawbacks.

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

A, i.e. Alice, generates a random nonce N_A, and encrypts it with A and P (password) by using K_S. Then, A sends an Authenticate-Request packet $\{A, N_A, P\}_{KS}$ to S.

(A-2) $S \rightarrow B: S, N_S, P \oplus f(N_S, K_{AB})$

[1] Lebanese University, Faculty of Sciences e-mail skadry@gmail.com
[2] Lebanese University, Faculty of Sciences e-mail ksmeily@hotmail.com

After S receives $\{A,N_A, P\}_{KS}$ from A, S decrypts it by using a private key and verifies whether A holds. If it holds, S generates a random nonce N_S and computes $f(N_S,K_{AB})$. Finally, S sends S, N_S, $P \oplus f(N_S,K_{AB})$ to B.

(A-3) B → S: $\{B, f(N_S,K_{AB})\}_{KS}$

After B, i.e. Bob, receives S,N_S, $P \oplus f(N_S,K_{AB})$ from S, B computes $f(N_S,K_{AB})$ and extracts P by computing $P \oplus f(N_S,K_{AB}) \oplus f(N_S,K_{AB})$. Then, B verifies whether P holds. If it holds, B accepts A's authentication request and sends $\{B, f(N_S,K_{AB})\}K_S$ back to S.

(A-4) After S receives $\{B, f(N_S,K_{AB})\}_{KS}$ from B, S decrypts $\{B, f(N_S,K_{AB})\}_{KS}$ by using private key and verifies whether B and $f(N_S,K_{AB})$ hold. If they hold, S believes the responding party is real B.

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.

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

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

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

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

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

Thus an attacker can easily obtain the exact password by repeating step (B-2) to step (B-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 (A-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.

IV. The New Improvement Protocol

The off-line guessing attack on Yoon et al.'s protocol can work is due to the message on step (A-2) and step (A-3) which both contain information $f(N_S, K_{AB})$. 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.

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

A, i.e. Alice, generates a random nonce N_A, and encrypts it with A and P (password) by using K_S. where T_A is the time stamp of A. Then, A sends an Authenticate-Request packet $\{A,N_A, T_A, P\}_{KS}$ to S.

(C-2) S → B: S, T_A, N_S, $P \oplus f(T_A, N_S,K_{AB})$

After S receives T_A, $\{A,N_A, T_A, P\}_{KS}$ from A, S check whether T_A is in a valid time period or not and verifies whether A holds. If it holds, S generates a random nonce N_S and computes $f(N_S, T_A, K_{AB})$. Finally, S sends S, T_A, N_S, $P \oplus f(N_S, T_A, K_{AB})$ to B.

(C-3) B → S: T_B,$\{B, f(N_S, T_B, K_{AB})\}_{KS}$

After B, i.e. Bob, receives S, T_A, N_S, $P \oplus f(N_S, T_A, K_{AB})$ from S, B computes $f(N_S, T_A, K_{AB})$ and extracts P by computing $P \oplus f(N_S, T_A, K_{AB}) \oplus f(N_S, T_A, K_{AB})$. Then, B verifies whether P holds. If it holds, B accepts A's authentication request and sends T_B,$\{B, f(N_S, T_B,K_{AB})\}K_S$ back to S. where T_B is the time stamp of B.

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

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.

V. Security Discussions

Unlike the papers [12, 13] which do not take into account the guessing and replay attacks nor the independent of platform[14], our 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 (C-1) through step (C-4) and try to guess the exact password, they cannot find the real password because of no adequate information for Verification n. 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 (C-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 (C-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.

VI. CONCLUSION

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 Networks", *The 2006 International Conference on Next Generation Web Services Practices* (NWeSP'06), pp.149-154, 2006.

[9] M. T. Thai, Y. Li, C. Ai, and D.-Z. Du, "On the construction of energy-efficient broadcast tree with hitchhiking in wireless networks", Proceedings of the 24th IEEE International Performance Computing and Communications Conference (IPCCC 2005), Phoenix, Arizona, USA, April 2005, pp 135-139.

[10] F. Wang, M. Min, Y. Li, and D.-Z. Du, "On the construction of stable virtual backbones in mobile ad-hoc networks", Proceedings of the 24th IEEE International Performance Computing and Communications Conference (IPCCC 2005), Phoenix, Arizona, USA, April 2005, pp. 355-362.

[11] W. A. Arbaugh, N. Shankar, Y.C. J. Wan, and K. Zhang, "Your 802.11 wireless network has no clothes", IEEE Wireless Communications, IEEE Communications Society, Dec 2002, 9(6):44–51.

[12] H. Luo, P. Henry, "A secure public wireless LAN access technique that supports walk-up users," In the Proceedings of the IEEE Global Telecommunications Conference, Volume 3, pp. 1415-1419, 2003.

[13] P. Prasithsangaree, P. Krishnamurthy, "New authentication mechanism for loosely coupled 3G-WLAN integrated networks," In the Proceedings of the IEEE Vehicular Technology Conference, Volume 5, 17-19, pp.2998-3003, May 2004.

[14]www.microsoft.com/technet/security/guidance/cryptographyetc/peap_0.mspx