International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:3, No:11, 2009

Cryptanalysis of Two-Factor Authenticated Key Exchange Protocol in Public Wireless LANs

Hyunseung Lee, Donghyun Choi, Yunho Lee, Dongho Won, Seungjoo Kim

***Abstract*—**In Public Wireless LANs(PWLANs), user anonymity is an essential issue. Recently, Juang et al. proposed an anonymous authentication and key exchange protocol using smart cards in PWLANs. They claimed that their proposed scheme provided identity privacy, mutual authentication, and half-forward secrecy. In this paper, we point out that Juang et al.'s protocol is vulnerable to the stolen-verifier attack and does not satisfy user anonymity.

***Keywords*—**PWLANs, user privacy, smart card, authentication, key exchange

I. Introduction

IN a remote login system, the user authentication is a very important security mechanism. There are many ways to authenticate users and the password-based authentication scheme is one of the most used authentication mechanisms. In 1981, Lamport first proposed the user authentication protocol using password[1]. Although many protocols supplementing Lamport's scheme have been proposed[2-12] since then, all of those protocols were not suitable for the public wireless LAN services.

Unlike general services, the public wireless LAN services should satisfy its unique characteristics such as billing, roaming and security. Especially, security in public wireless LAN service is an essential issue. The security requirements of the public wireless LAN services are as follows. First, it should ensure the user anonymity. If the user anonymity is not ensured, the location information of the respective user is totally exposed to an attacker. Once a user's sensitive information such as location information is collected by an attacker, it leads to a violation of privacy. Here, the user anonymity means that not only a user's identity should be protected from being exposed to an attacker but also to the server. To protect a user's privacy, a user information must not be exposed even to servers. That is because there are chances that a server may abuse the user information. It is called anonymous communication to prevent exposing user's identity only during communication[13]. Second, a mutual authentication between a user and a server should be possible. If it is not guaranteed, an attacker may impersonate as an authenticated user or server. Third, a public wireless LAN service should satisfy the forward secrecy. If it does not satisfy the forward secrecy, an attacker is able to compute a session key based on the intercepted information.

In 2003, Park et al. proposed an authentication and key exchange protocol satisfying the above requirements[14]. However, in 2008, Juang et al. proved that the protocol proposed by Park et al. did not ensure the user anonymity and proposed a new protocol ensuring the user anonymity[15]. The protocol proposed by Juang et al. had a merit to require less computational overhead than the existing protocol while ensuring the anonymity, but we discover that their protocol does not satisfy the user anonymity and is vulnerable to the stolen-verifier attack. Moreover, it will be showed a shortcoming that the server has high computational overhead.

In this paper, we analyze the vulnerability of the protocol proposed by Juang et al. The structure of this paper is organized as follows. In Chapter II, we show previous studies to ensure anonymity. In Chapter III, we analyze the problems of Juang et al.'s scheme. Finally, we make conclusions in Chapter IV.

H. Lee, D. Choi, Y. Lee, D. Won and S. Kim are with Information Security Group, Sungkyunkwan University, 300 Cheoncheon-dong, Jangan-gu, Suwon-si, Gyeonggi-do, 440-746, Korea (e-mail : {hsrhee, dhchoi, leeyh, dhwon, skim} @security.re.kr)
Corresponding author: Seungjoo Kim

II. Introduction

A. Review of Park et al.'s protocol

In 2003, Park et al. proposed an authentication and key exchange protocol using password and smart card in a public wireless LAN environment. This protocol assumes that users and the server share parameters (p,q,g), where p is a large prime, q is a prime divisor of $(p-1)$, and g is an element of order q in Z^*_p. This protocol is composed of the following three stages. A denotes the user, and B denotes the server.

1) Registration stage

A and B share the password π and symmetric key t. A remembers π and stores t in the smart card. B stores π and t in a storage. Moreover, B chooses a random number b and sets it as a static private key, and after calculating $y_s = g^b \bmod p$, sets it as an public key.

2) Precomputation stage

A selects a random value x in Z_q and computes $y_u = g^x \bmod p$. After that, to reduce the computational overhead in the authentication and key exchange stage, A computes $c = g^{bx} \bmod p$ and stores it.

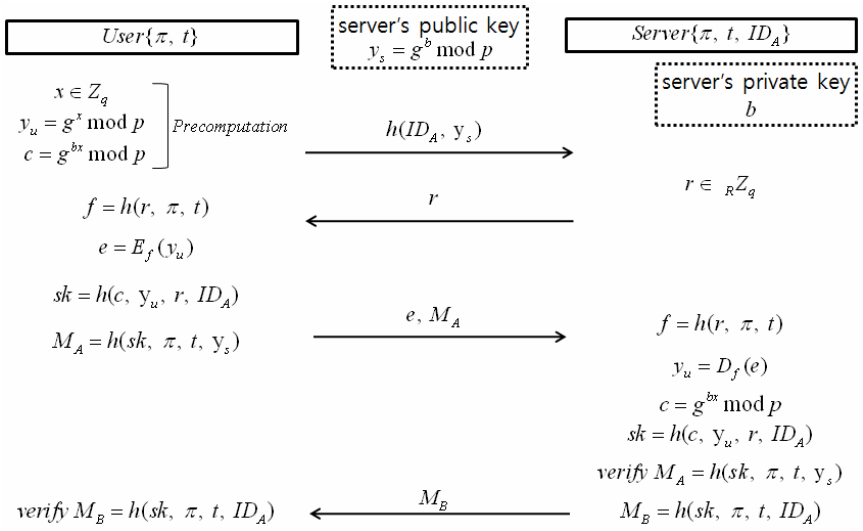

Fig. 1 A Protocol Proposed by Park et al.

3) Authentication and key exchange stage

In this stage, a mutual authentication between A and B is performed and the session key is established.

(1) A computes $h(ID_A, y_s)$ for the anonymous communication and sends it to B.

(2) B replaces all IDs stored in the database and finds ID_A, which satisfies $h(ID_A, y_s)$. After finding ID_A, B selects a random value r and sends it to A.

(3) A computes $f = h(r, \pi, t)$ and $e = E_f(y_u)$, where E_f denotes the symmetric encryption function with the symmetric key f. After that, A computes a session key $sk = h(c, y_u, r, ID_A)$ and $M_A = h(sk, \pi, t, y_s)$. A sends e and M_A to B.

(4) B computes $f = h(r, \pi, t)$ and $y_u = D_f(e)$, where D_f denotes the symmetric decryption function with the symmetric key f. Then, B computes $c = (g^x)^b \bmod p$ and $sk = h(c, y_u, r, ID_A)$. Now, A and B share the session key sk. After that, B computes $M_A = h(sk, \pi, t, y_s)$ and compares it with the M_A sent by A. If so, B authenticates A as a legitimate user. Finally, B computes $M_B = h(sk, \pi, t, ID_A)$ and sends it to A.

(5) A computes $M_B = h(sk, \pi, t, ID_A)$ and compares it with the M_B sent by B. If so, A authenticates B as a legitimate server. Now, a mutual authentication between A and B is completed.

B. Review of Juang et al.'s protocol

The authentication and key exchange protocol proposed by Park et al. has a vulnerability of exposing user's ID if an attacker intercepts $h(ID_A, y_s)$ and performs a guessing attack. Juang et al. indicated this problem and proposed a new protocol complementing this problem. This protocol is composed of the following three stages. A denotes the user, and B denotes the server.

1) Registration stage

A and B share the password π and symmetric key t. A remembers π and stores t in the smart card. B stores π and t in a storage. Moreover, B chooses a random number b and sets it as a static private key, and after calculating $y_s = g^b \bmod p$, sets it as an public key.

2) Precomputation stage

A selects a random value x in Z_q and computes $y_u = g^x \bmod p$. After that, to reduce the computational overhead in the authentication and key exchange stage, A computes $c = g^{bx} \bmod p$ and stores it.

3) Authentication and key exchange stage

In this stage, a mutual authentication between A and B is performed and the session key is established.

(1) A computes $SID_{A,i} = h(\pi, t, i)$, $f = h(\pi, t, ID_A)$, $e = E_f(y_u)$ and sends $(e, SID_{A,i}, i)$ to B.

(2) B replaces π and t stored in the database to $SID'_{A,i} = h(\pi', t', i)$ and finds a value matching $SID_{A,i}$ sent by A. After finding right π and t, B acquires ID_A. Then B computes $f = h(\pi, t, ID_A)$ and $y_u = D_f(e)$. After decryption, B computes $c = (g^x)^b \bmod p$, and selects a random value r. Next, B computes $sk = h(c, r, ID_A)$ and $M_B = h(sk, \pi, t, ID_A)$. B sends r and M_B to A.

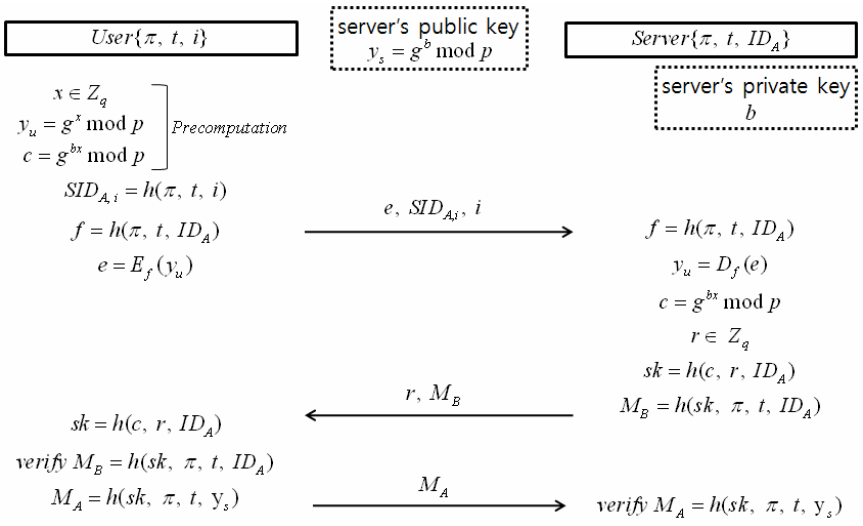

Fig. 2 A Protocol Proposed by Juang et al.

(3) A computes the session key $sk = h(c, r, ID_A)$. Now, A and B share the session key sk. Then it computes $M_B = h(sk, \pi, t, ID_A)$ and compares it with the M_B sent by B. If so, A authenticates B as a legitimate server. Finally, A computes $M_A = h(sk, \pi, t, y_s)$ and sends it to B.

(4) B computes $M_A = h(sk, \pi, t, y_s)$ and compares it with the M_A sent by A. If so, B authenticates A as a legitimate user. Now, a mutual authentication between A and B is completed.

III. Weaknesses of Juang et al.'s Protocol

The protocol proposed by Juang et al. has the following problems.

A. It does not satisfy the user anonymity.

The protocol proposed by Juang et al. does not expose users' ID during communication. Therefore, this protocol satisfies the anonymous communication. However, the server is able to know every user related information including the ID. In this environment, if there is no assumption that the server is honest, the user anonymity is not ensured[13].

B. It is vulnerable to the stolen-verifier attack

Stolen-verifier attack is a serious issue in the authentication schemes[16]. It denotes that the attacker can get the verifier, maintained by the server. In the protocol proposed by Juang et al., users' ID, π (password) and t (symmetric key) are stored in the server's database. If an attacker performs the stolen-verifier attack and steals the verification table stored in the server, every users' ID, π, t are exposed to an attacker. An attacker may impersonate as a legitimate user using the stolen information.

An attacker can impersonate as a legitimate user by performing the following steps. A denotes the attacker, and B denotes the server.

1. A selects a random value x in Z_q and computes $y_u = g^x \bmod p$ and $c = g^{bx} \bmod p$. Then, A computes $SID_{A,i} = h(\pi, t, i)$, $f = h(\pi, t, ID_A)$, $e = E_f(y_u)$ using stolen information. A sends $(e, SID_{A,i}, i)$ to B.
2. Server checks $SID'_{A,i} = h(\pi', t', i)$ by using π and t stored in the database to find a value matching $SID_{A,i}$. After finding right π and t, B acquires ID_A. Then B computes $f = h(\pi, t, ID_A)$ and $y_u = D_f(e)$. After decryption, B computes $c = (g^x)^b \bmod p$, and selects a random value r. Next, B computes $sk = h(c, r, ID_A)$ and $M_B = h(sk, \pi, t, ID_A)$. B sends r and M_B to A.
3. A can compute the session key $sk = h(c, r, ID_A)$ because he knows valid c, r, and ID_A. Then A computes $M_A = h(sk, \pi, t, y_s)$ and sends it to B.
4. B computes $M_A = h(sk, \pi, t, y_s)$ and compares it with the M_A sent by A. B authenticates A as a legitimate user and shares the session key sk.

As above, to impersonate as a legitimate user for an attacker, he should compute e, SID_A, M_A. Since the attacker knows ID, π, t through the stolen-verifier attack, he can computes valid e, SID_A, M_A. Therefore, the Juang's protocol is vulnerable to the stolen-verifier attack.

C. The server has high computational overhead

To verify the real ID from the *SID* sent by the user, the server should try until the right *SID* comes out by checking every π and t that the server stores to $h(\pi, t, i)$. In the worst case, it should perform as many hash functions as the number of registered users in the server. It needs high computational overhead and also results in consuming too much time.

IV. Conclusion

In 2003, Park et al. proposed an authentication and key exchange protocol in Public Wireless LANs. After that, Juang et al. proved that the protocol proposed by Park et al. did not ensure the user anonymity and proposed a new protocol ensuring the user anonymity. In this paper, we have pointed out that the Juang's protocol was vulnerable to the stolen-verifier attack and did not satisfy the user anonymity. In the future, the research about improved protocol solving above problems will have to be accomplished

Acknowledgment

* This work was supported by Defense Acquisition Program Administration and Agency for Defense Development under the contract UD070054AD.
* This research was supported by the MKE(Ministry of Knowledge Economy), Korea, under the ITRC(Information Technology Research Center) support program supervised by the NIPA(National IT Industry Promotion Agency) (NIPA-2009-(C1090-0902-0016))

References

[1] Lamport L. “Password authentication with insecure communication,” Communications of the ACM, 1981;24(11):770-.2.
[2] Awasthi A, Lal S. “A remote user authentication scheme using smart cards with forward secrecy,” IEEE Trans. Consumer Electronic, 2003;49(4):1246-.8.
[3] Awasthi A, Lal S. “An enhanced remote user authentication scheme using smart cards,” IEEE Trans. Consumer Electronic, 2004;50(2):583-.6.
[4] Juang W. “Efficient password authenticated key agreement using smart card,” Computers & Security, 2004;23:167-.73.
[5] Ku W, Chen S. “Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards,” IEEE Trans. Consumer Electronic, 2004;50(1):204-.7.
[6] Kumar M. “New remote user authentication scheme using smart cards,” IEEE Trans. Consumer Electronic, 2004;50(2):597-.600.
[7] Kwon T, Park Y, Lee H. “Security analysis and improvement of the efficient password-based authentication protocol,” IEEE Communications Letters, 2005;9(1):93-.5.
[8] Park Y, Park S. “Two factor authenticated key exchange (TAKE) protocol in public wireless LANs,” IEICE Trans. Communications 2004;E87-B(5):1382-.5.
[9] Sun H. “An efficient use authentication scheme using smart cards,” IEEE Trans. Consumer Electronic, 2000;46(4):958-.61.
[10] Wang X, Zhang W, Zhang J, Khan M. “Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards,” Computer Standards & Interfaces, 2007;29(5):507-.12.
[11] Yang C, Hwang M. “Cryptanalysis of simple authenticated key agreement protocols,” IEICE Trans. Communications, 2004;E87-A(8):2174-.6.
[12] Yang C, Wang R. “Cryptanalysis of a user friendly remote authentication scheme with smart cards,” Computer Security, 2004;23:425-.7.
[13] Zhenchuan Chai, Zhenfu Cao, Rongxing Lu, "Efficient Password-Based Authentication and Key Exchange Scheme Preserving User Privacy," Wireless Algorithms, Systems, and Applications 2006, Vol. 4138, pp. 467-477.
[14] Young Man PARK, Sang Kyu PARK, "Two factor authenticated key exchange(TAKE) protocol in public wireless LANs," IEICE Trans. Communications, 2004, E87-B(5), pp. 1382-1385.
[15] Wen-Shenq Juang, Jing-Lin Wu, "Two efficient two-factor authenticated key exchange protocols in public wireless LANs," Computers and Electrical Engineering, 2008, Vol. 10, pp. 1-8.
[16] Tzu-Chang YEH , Hsiao-Yun SHEN, Jing-Jang HWANG, “A Secure One-Time Password Authentication Scheme Using Smart Cards,” 2002, Vol.E85-B No.11, pp.2515-2518.