Cryptanalysis of a New Efficient MAKEP for Wireless Communications

Jau-Ji Shen[1], Ching-Ying Lin[2], and Hung-Wen Yang[3]

(Corresponding author: Jau-Ji Shen)

Department of Information Management, National Formosa University[1]
64 Wunhua Rd., Huwei, Yunlin County, Taiwan 632, R.O.C. (Email: amitofo@sunws.nfu.edu.tw)
Graduate Institute of Networking and Communication Engineeing, Chaoyang University of Technology[2]
168 Gifeng E. Rd., Wufeng, Taichung County, Taiwan 413, R.O.C.
Department of Computer Science, National Chung Hsing University[3]
250,Kuo Kuang Road, Taichung County, Taiwan 402, R.O.C. (Email: hwyang@ms34.url.com.tw)

(Received June 20, 2005; revised and accepted July 5, 2005)

Abstract

In 2001, Wong and Chan proposed two mutual authentication and key exchange protocols (MAKEP) for low power wireless communications, which were suitable for establishing secure communications between a low-power wireless device and a powerful base station. Unfortunately, Shim pointed out Wong and Chan's schemes were incurred the unknown key-shared attack, then he proposed an improved scheme to overcome this weakness. Later, Jan and Chen found that the improved scheme was vulnerable to the man-in-the-middle attack. Then, they also proposed a new efficient MAKEP in spirit of Girault's method to withstand the above weakness. However, in this paper, we shall show that Jan and Chen's scheme suffered from the forgery attack and the man-in-the-middle attack.

Keywords: cryptanalysis, forgery attack, key exchange, man-in-the-middle attack, mutual authentication, wireless networks.

1 Introduction

With speedy growth of information science, the wireless networks have developed very well, the communication security between a client with its remote server is a very important issue. In 1976, Diffie and Hellman [2] proposed a well-known key exchange scheme based on the discrete logarithm problem. This scheme enables two parties to establish a common secret session key over an insecure channel. However, it is vulnerable to the man-in-the-middle attack since it does not execute mutual authentication between two participants. Later, many schemes [1, 5, 6, 8] have proposed to solve this weakness. Recently, Wong and Chan [9] proposed two efficient Mutually Authentication Key Exchange Protocols (MAKEP) : server-specific MAKEP and linear MAKEP. Their schemes allow two participants to establish a common session key and to identify each other. They claimed their schemes are suitable for establishing secure communication between a low power wireless device and a powerful base station under different system requirements. Unfortunately, Shim [7] found out that Wong and Chan's MAKEP are insecure against unknown key-shared attack, and he proposed an Improved Linear MAKEP (IL MAKEP) to overcome this weakness. Later, Jan and Chen's [4] also pointed out that the MAKEP and the IL MAKEP was vulnerable to the man-in-the-middle attack. In order to overcome this weakness, Jan and Chen proposed a new efficient MAKEP by using the Girault's method [3]. However, in this paper, we will show the Jan and Chen's scheme suffered from the forgery attack and the man-in-the-middle attack. In the forgery attack, a valid client can successful impersonate another valid client to login the remote server. In the man-in-the-middle attack, an adversary interposing in the line between two communicating parties could masquerade as one communicating party to cheat the other one. In the following section, the Jan and Chen's scheme will be briefly reviewed. In Section 3, we shall show that the scheme is vulnerable to the forgery attack and the man-in-the-middle attack. Finally, we shall state the conclusions of this paper in Section 4.

2 Brief Review of Jan and Chen's Scheme

The Jan and Chen's scheme [4] consists of registration and session key generation phases. Before explaining their scheme, we introduce the used notations.

2.1 Notations

The notations and abbreviations used in this paper are described as follows:

- C: the client.
- S: the server.
- $p \cdot q$: two large distinct random odd primes that the server selected.
- N: a public value which is equal to $p \cdot q$.
- g: a maximum order in the multiplication groupZ_N^*.
- h($\cdot$):an one-way hash function.
- (e, d):a pair of public and secret key of the server.

2.2 Registration Phase

The client chooses a prime number x and computes $v = g^{-x}$ mod N . Then, the client sends the computed result with his identity to the server. Upon receiving the message, the server computes the client's public key as $y = (v - ID)^d \bmod N$ and forwards y to the client.

2.3 Session Key Generation Phase

The client must negotiate with the server to generate a session key before the client logins to the server.

Step 1. $C \longrightarrow S : ID, y$
The client C submits his identity ID and his public key y to the server.

Step 2. $S \longrightarrow C : r_s$
The server computes $v = y^e + ID = g^{-x} \bmod N$ and chooses a random number r_s in Z_N. The server forwards r_s to the client.

Step 3. $C \longrightarrow S : (u, t, s)$
After receiving r_s, the client chooses two random numbers (w, k) and computes $u = g^w \bmod N$, $t = E_e(k)$ and $s = w + x \cdot H(r_S||t||u)$. Note that, $E_e(k)$ denotes the random value k is encrypted by using the server's public key. The client sends (u, t, s) to the server and computes the new session key $\sigma = k \bigoplus s$.

Step 4. $S \longrightarrow C : H(k)$
After receiving (u, t, s), the server verifies whether $g^S \cdot v^{H(r_s||t||u)} \equiv u \bmod N$ holds or not. If it holds, the server decrypts t to get k and computes the new session key $\sigma = k \bigoplus s$. Otherwise, the server will reject this request. Finally, the server sends $H(k)$ to the client, the client checks whether the received message is correct or not. If it is correct, the client authenticates the server.

3 Cryptanalysis of Jan and Chen's Scheme

In this section, we will show that Jan and Chen's scheme are vulnerable to the forgery attack and the man-in-the-middle attack. We denote A is the client A, T is the client T, ID_A is client A's identity, and ID_T is client T's identity.

3.1 Attack 1

In Jan and Chen's scheme, the server does not record any information of the clients, such as the client's pubic key. On the other hand, the server employs the received y to compute the new session key. Hence, a valid client T can forge another valid client A to communicate with the server easily.

3.1.1 Registration Phase

T chooses a prime number X_T as his secret key, and computes $v_T = g^{-x_T} + ID_T - ID_A$ mod N. Then, T submits (ID_T, v_T) to the server. Upon receiving the message, the server computes the public key of T as $y_T = (v_T - ID_T)^d = (g^{-x} - ID_A)^d$ mod N and sends it to T.

3.1.2 Session Key Generation Phase

Step 1. $T \longrightarrow S$: ID_A, y_T
T submits (ID_A, y_T) to the server.

Step 2. $S \longrightarrow T$: r'_s
Upon receiving the message, the server computes $v_T = y_T^e = g^{-x_T}$ mod N and chooses a random number r'_s. The server sends r'_s to T.

Step 3. $T \longrightarrow S$: (u_T, t', s_T)
After receiving r'_s, T chooses two random numbers w_T and k_T and computes $u_T = g^{w_T}$ mod N, $t' = E_e(k_T)$ and $s_T = w_T + x_T \cdot H(r'_s||t'||u_T)$. T sends (u_T, t', s_T) to the server and computes the new session key $\sigma' = k_T \bigoplus s_T$.

Step 4. $S \longrightarrow T$: $H(k_T)$
The server verifies whether $g^{s_T} \cdot v_T^{H(r'_s||t'||u_T)} \equiv u_T$ mod N holds or not. We can find it holds, the server decrypts t' to get k_T and to computes the session key $\sigma' = k_T \bigoplus s_T$. Finally, The server sends $H(k_T)$ back to T.

Step 5. Upon receiving $H(k_T)$, T check it is true or not. If it is true, it is indicated that the server is authenticated.

From the above cryptanalysis, the Jan and Chen's scheme is vulnerable to the forgery attack.

3.2 Attack 2

When A wants to communicate with the server, T interposing in the line between A and the server. T intercepts the communication messages and uses A's login request to cheat the server. Because A's login request can pass the server's authentication, but the server believes the party of shared session key is T.

3.2.1 Registration Phase

A chooses a prime number x_A as his private key, and computes $v_A = g^{-x_A} \; mod \; N$. Then, A submits (ID_A, v_A) to the server, the server sends the public key y_A to A. Now, T monitors the communication channel between A and the server to obtain $A's$ public key (y_A). Then, T can perform the registration phase. First, T computes $v_A = y_A^e + ID_A = g^{-x_A} \; mod \; N$ and sets $v_T = v_A$. Then, T sends (ID_T, v_T) to the server. Upon receiving the message, the server computes $y_T = (v_T - ID_T)^d \; mod \; N$ and sends y_T to T.

3.2.2 Session Key Generation Phase

Step 1. $T \longrightarrow S$: ID_T, y_T

When A wants to access resource, he would sends (ID_A, y_A) to the server. Now, T intercept A's messages and submits (ID_T, y_T) to the server.

Step 2. $S \longrightarrow T$: r'_s

Upon receiving the message, the server computes $v_T = y_T^e + ID_T = g^{-x_A} \; mod \; N$ and chooses a random number r'_s, the server sends r'_s to T. Then, T forwards it to A.

Step 3. $T \longrightarrow S$: (u_T, t', s_T)

After receiving r'_s, A chooses two random numbers (w_A, k_A) and computes $u_A = g^{w_A} \; mod \; N$, $t' = E_e(k_A)$, $s_A = w_A + x_A \cdot H(r'_s||t'||u_A)$. A sends (u_A, t', s_A) to the server and computes the new session key $\sigma' = k_A \bigoplus s_A$. Then, T intercepts this message (u_A, t', s_A) and forwards it to the server.

Step 4. $S \longrightarrow T$: $H(k_T)$

The server verifies whether $g^{s_A} \cdot v_T^{H(r'_s||t'||u_A)} \equiv u_A \; mod \; N$ holds or not. We can find it holds, because $v_T = v_A = g^{-x_A} \; mod \; N$. However, the server believes the party of share session key is T. Thus, the Jan and Chen's scheme is vulnerable to the man-in-the-middle attack.

4 Conclusions

In this paper, we have showed that the Jan and Chen's scheme is vulnerable to the forgery attack and the man-in-the-middle attack. We proposed forgery attacks that enabling a valid client can forge another valid client to login the server for requesting the source by passing the server's authentication. We proposed man-in-the-middle attack that enabling an adversary can cheat the server to generate session key without detecting the valid user.

Acknowledgements

This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC93-2213-E-005-033.

References

[1] T. C. Wu, C. L. Hsu, T. S. Wu, and C. Mitchell, "Improvement of modified authenticated key agreement protocol," *Applied Mathematics and Computation*, vol. 142, pp. 305–308, 2003.

[2] W. Diffie and M. Hellman, "New directions in cryptology," *IEEE Transations on Information Theory*, vol. IT-22, no. 6, pp. 644–654, 1976.

[3] M. Girault, "Self-certified public key," *Advances in Cryptology-EUROCRYPT'91*, pp. 491–497, 1991.

[4] J. K. Jan and Y. H. Chen, "A new efficient makep for wireless communications," in *Proceedings of the 18th International Conference on Advanced Information Networking and Application*, vol. 2, pp. 347–350, 2004.

[5] W. C. Ku and S. D. Wang, "Cryptanalysis of modified authenticated key agreement protocol," *Electronics Letters*, vol. 36, no. 21, pp. 1770–1771, 2000.

[6] D. H. Seo and P. Sweeney, "Simple authenticated key agreement algorithm," *Electronics Letters*, vol. 35, no. 13, pp. 1073–1074, 1999.

[7] K. Shim, "Cryptanalysis of mutual authentication and key exchange for low power wireless communications," *IEEE Communications Letters*, vol. 7, no. 5, pp. 248–250, 2003.

[8] Y. M. Tseng, "Weakness in simple authenticated key agreement protocol," *Electronics Letters*, vol. 36, no. 1, pp. 48–49, 2000.

[9] D. S. Wong and A. H. Chan, "Mutual authentication and key exchange for low power wireless communications," in *Military Communications Conference for Network-Centric Operations: Creating the Information Force*, vol. 1, pp. 39–43, 2001.

Jau-Ji Shen received Ph.D. degree in Information Engineering and Computer Science from National Taiwan University at Taipei in 1988. From 1988 to 1994, he was the leader of the software group in Institute of Aeronautic, Chung-Sung Institute of Science and Technology. The following nine years after 1994, he was an associate professor of Information Management Department in the Chaoyang University of Technology at Taichung. He is currently an Associate Professor of Information Management Department in the National Formosa University at Yunlin. His current research areas focus on the data engineering, database techniques, and information security.

Ching-Ying Lin received her B.S. in Information Management from Chaoyang University of Technology in 2004. She is pursuing her M.S. in Networking and Communication Engineering from Chaoyang University of Technology. Her current research interests include information security, and mobile communications.

Hung-Wen Yang received his M.S. in Information Management from Chaoyang University of Technology in 2005. He is pursuing his Ph. D. in Computer Science from National Chung Hsing University. His current research interests include information security, and mobile communications.