Cryptanalysis of Some Authenticated Key Agreement Protocols

Eric Jui-Lin Lu Cheng-Chi Lee Min-Shiang Hwang

Department of Information Management
Chaoyang University of Technology
168, Gifeng E. Rd., Wufeng,
Taichung County, Taiwan 413, R.O.C.
Email: mshwang@cyut.edu.tw

August 6, 2002

Abstract: In this article, we show that both Seo-Sweeney's and Hwang's authenticated key agreement protocols are insecure against several attacks, such as masquerade, dictionary, replay, and modifying attacks.
Key Words: Cryptography, key agreement, man-in-middle attack.

1 Introduction

In 1976, Diffie and Hellman proposed a key agreement protocol [3] so that two parties can agree on a session key in an insecure channel. However, Diffie-Hellman's protocol is vulnerable to the man-in-middle attack [1, 2]. Also, the communication parties using Diffie-Hellman's protocol cannot authenticate each other. To overcome these problems, two approaches have been proposed. One is of signature based. The other is of password based.

In signature-based approach, Alexandris et al. [1] and Arazi [2] independently proposed protocols to withstand the man-in-middle attack. However, their protocols are insecure [12]. When a session key is disclosed to an attacker, the attacker can derive all of the other session keys in their protocols. In 1997, Harn [4] proposed a digital signature without using a one-way function for Diffie-Hellman public keys. However, it is also insecure [5]. He and Wu proposed an improved Harn's protocol [5]. Later, Hwang further improved Harn's protocol [10]. Hwang claimed that his protocol is more efficient than that of He-Wu's protocol. The reduction ratio of the total cost for each user is at least 28.57% [10].

In password-based approach, many authenticated key agreement protocols have been proposed. These protocols have the following advantages: (1) They can prevent the masquerade and dictionary attacks; (2) They can achieve perfect forward secrecy. However, these protocols are complicated. Later, although Seo and Sweeney [13] proposed a simple authenticated key agreement protocol, there are some weaknesses in Seo-Sweeney's protocol. For example, Seo-Sweeney's protocol cannot withstand the masquerade attack. We will show that in next section.

2 Literature Reviews

In this section, we review Seo-Sweeney's protocol [13] and Hwang's protocol [10]. We also illustrate the weaknesses in their protocols. The security of both Seo-Sweeney's protocol and Hwang's protocol is summarized in Table 1.

Table 1: Summary of Seo-Sweeney's protocol and Hwang's protocol in security

	Seo-Sweeney's Protocol	Hwang's Protocol
Withstand Man-in-Middle Attack	Yes	Yes
Withstand Masquerade Attack	No	No
Withstand Dictionary Attack	No	Yes
Withstand Replay Attack	No	No
Withstand Modifying Attack	No	No
Perfect Forward Secrecy	No	Yes

2.1 The Weaknesses of Seo-Sweeney's Protocol

Seo and Sweeney proposed a password-based key agreement algorithm [13] which is simpler than other password-based protocols. Seo-Sweeney's protocol assumed that Alice and Bob agree on a common password W and a predetermined way to generate two integers ($Q \bmod p-1$, and $Q^{-1} \bmod p-1$) from W in advance, where p is a large prime. If Alice and Bob want to communicate securely by using a common session key, Alice chooses a random number a and computes $X_a = g^{aQ} \bmod p$, where g is a primitive element in $GF(p)$. Next, Alice sends X_a to Bob. In the meanwhile, Bob also chooses a random number b, calculates $X_b = g^{bQ} \bmod p$, and sends X_b to Alice. When Alice receives X_b from Bob, she calculates $Y_b = X_b^{Q^{-1}} \bmod p$ and a common session key ($K_a = Y_b^a \bmod p$), and then sends ($K_a^Q \bmod p$) to Bob. Similarly, after receiving X_a from Alice, Bob sends ($K_b^Q \bmod p$) to Alice, where ($K_b = Y_a^b \bmod p$) and ($Y_a = X_a^{Q^{-1}} \bmod p$). Once Alice and Bob receives ($K_b^Q \bmod p$) and ($K_a^Q \bmod p$) respectively, Alice and Bob can verify K_b and K_a easily by computing ($K_a = (K_b^Q)^{Q^{-1}} \bmod p$) and ($K_b = (K_a^Q)^{Q^{-1}} \bmod p$). As a result, they can agree on a common session key $g^{ab} \bmod p$ ($= K_a = K_b$).

Seo-Sweeney's protocol is simple and easy to implement. However, there are some weaknesses in their protocol which are described as follows.

1. An illegal user can pretend to be a legal user (i.e., Alice) to communicate with another party (i.e., Bob). Although the pretender does not know the secret number Q that is shared by Alice and Bob, he/she can choose a random number a' and calculates $X'_a = g^{a'} \bmod p$. Next, the pretender sends X'_a to Bob. After receiving $K_b^Q \bmod p$ from Bob, the pretender sends the same value $K_b^Q \bmod p$ to Bob. Since $(K_b^Q)^{Q^{-1}} \bmod p = K_b = K_a$, Bob convinces Alice's identity and the common session key.

2. The protocol does not provide perfect forward secrecy. When a password is compromised, all common session keys K_a or K_b can be derived by computing $K_a = (K_a^Q)^{Q^{-1}}$ or $K_b = (K_b^Q)^{Q^{-1}}$.

3. The protocol cannot withstand the dictionary attack. A pretender sends X'_a ($= g^{a'} \bmod p$) to Bob. Bob computes ($Y_a = X_a'^{Q^{-1}} \bmod p$) and sends K_b^Q ($= Y_a^{bQ} \bmod p$) to the pretender. The pretender also returns the same value of K_b^Q to Bob. Bob is convinced that he is communicating with Alice. However, if the password W is poorly chosen [10, 7, 9, 8, 11], the pretender can determine Q using the equation $(K_b^Q)^Q = (X_b)^{a'} \bmod p$.

4. The protocol has more traffic signals. Although the protocol defeats the man-in-middle attack in Diffie-Hellman protocol, the protocol requires two more communications than the original Diffie-Hellman protocol [3].

2.2 The Weaknesses of Hwang's Protocol

Hwang proposed an efficient signature-based key agreement protocol [10]. There are four types in Hwang's protocol. Here, we only review the most efficient one in his protocol. In Hwang's protocol, there are three public values p, q, and g, where p and q are two large prime and g is a primitive element in $GF(p)$. Each user i randomly selects his/her secret key x_i and computes his/her public key $y_i = g^{x_i} \bmod p$.

Before Alice and Bob communicate, Alice chooses two random numbers w and k_a, and calculates $r_a = (w \parallel ID_a) y_b^{-k_a} \bmod p$, where ID_a is her identity and $\parallel$ is a concatenation operation. Next, Alice calculates s_a such that it satisfies $k_a = s_a x_a + r_a \bmod q$. Lastly, she sends (ID_a, r_a, s_a) to Bob.

When Bob receives (ID_a, r_a, s_a), he calculates $r'_a = y_a^{s_a} g^{r_a} \bmod p = g^{k_a} \bmod p$ and obtains $(w \parallel ID_a)'$ by computing $r_a (r'_a)^{x_b} \bmod p$. If $(w \parallel ID_a)'$ contains the correct ID_a, he is convinced that Alice is a legal user and the signature is really signed by Alice. Next, he chooses a random number k_b and computes $r_b = g^{k_b} \bmod p$. He calculates s_b such that it satisfies $k_b = s_b x_b + r_b \bmod q$. Finally, Bob sends (r_b, s_b) to Alice.

After receiving (r_b, s_b), Alice verifies the signature by checking whether or not r_b is equal to $y_b^{s_b} g^{r_b} \bmod p$.

Finally, after Alice and Bob authenticate each other, they can generate a common session key $K_{ab} = (r_b)^{wk_a} \bmod p = (r_a)^{wk_b} \bmod p$.

Hwang's protocol is simple and easy to implement. However, the weaknesses of Hwang's protocol are:

1. The protocol did not remedy the replay attack. Assume a pretender wants to forge Alice communicating with Bob. Although the pretender does not know the secret key x_a, he/she can intercept a triple value (ID_a, r_a, s_a) from the communication between Alice and Bob. After a period of time, the pretender can replay the messages to Bob. Bob can be fooled to execute the verification procedures and is convinced that he is communicating with Alice.

2. The protocol did not prevent the modifying attack. When Alice and Bob want to generate a common session key, an attacker can modify their transmitted messages such that their session key is different. For example, when Bob sends (r_b, s_b) to Alice, an attacker can intercept and modify it to (r_b', s_b'), where r_b' and s_b' are the former transmitted messages from Bob to Alice. When Alice receives these messages, she validates that these messages are sent from Bob. However, their session keys are different because $K_{ab} = (r_b')^{wk_a} \bmod p \neq (r_a')^{wk_b} \bmod p$.

3 Conclusions

We have shown that both Seo-Sweeney's and Hwang's protocols are insecure against several attacks such as masquerade, dictionary, replay, and modifying attacks.

Acknowledgements

The authors wish to thank many anonymous referees for their suggestions to improve this paper. Part of this research was supported by the National Science Council, Taiwan, R.O.C., under contract no. NSC89-2213-E-324-053.

References

[1] N. Alexandris, M. Burmester, V. Chrissikopoulos, and Y.Desmedt. A proven secure public key distribution system. In *Proceedings of 3rd Symp. State and Progress of Research in Cryptograph*, Rome, Italy, 1993.

[2] A. Arazi. Integrating a key cryptosystem into the digital signature standard. *Electronics Letters*, 29(11):966–967, 1993.

[3] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22:644–654, 1976.

[4] L. Harn. Digital signature for Diffie-Hellman public keys without using a one-way function. *Electronics Letters*, 30(2):125–126, 2001.

[5] W. H. He and T. C. Wu. Improvement of Harn's digital signature for Diffie-Hellman public keys. *Electronics Letters*, 33:1304–1305, 1997.

[6] M. S. Hwang. Cryptanalysis of remote login authentication scheme. *Computer Communications*, 22(8):742–744, 1999.

[7] M. S. Hwang. A remote password authentication scheme based on the digital signature method. *International Journal of Computer Mathematics*, 70(4):657–666, 1999.

[8] M. S. Hwang, C. C. Lee, and Y. L. Tang. An improvement of SPLICE/AS in wide against guessing attack. *International Journal of Informatica*, 12(2):297–302, 2001.

[9] M. S. Hwang and L. H. Li. A new remote user authentication scheme using smart cards. *IEEE Transactions on Consumer Electronics*, 46(1):28–30, 2000. ", , vol. 46, no. 1, pp.28-30, Feb. 2000.

[10] S. J. Hwang. Simple improvements to Harn's digital signature for Diffie-Hellman public keys. *Electronics Letters*, 35:1942–1943, 1999.

[11] L. H. Li, I. C. Lin, and M. S. Hwang. A remote password authentication scheme for multi-server architecture using neural networks. *IEEE Transactions on Neural Networks*, 12(6):1498–1504, 2002.

[12] K. Nyberg and R. A. Rueppel. Weaknesses in some recent key agreement protocols. *Electronics Letters*, 30(1):26–27, 1994.

[13] D. H. Seo and P. Sweeney. Simple authenticated key agreement algorithm. *Electronics Letters*, 35:1073–1074, 1999.