Cryptoanalysis on Zhou et al.s' User Authentication Scheme

Jue-Sam Chou[1], Xian-Wu Hou[2] , Yalin Chen [3]

[1] Department of Information Management, Nanhua University
Chiayi 622 Taiwan, R.O.C

[2] Department of Information Management, Nanhua University
Chiayi 622 Taiwan, R.O.C

[3] Institute of information systems and applications, National Tsing Hua University
Hsinchu30013, Taiwan, R.O.C

Summary

In this paper, we show that the end-to-end security protocol for mobile communications with end-user identification authentication due to Zhou et al. [1] has a serious flaw, it suffers from the impersonation attack. The protocol cannot achieve the claimed security.

1. Introduction

Diffie–Hellman key agreement protocol [2] is a famous scheme that two parties can establish a common secret session key over an insecure network. However, it does not authenticate the other party, thus suffers from the main-in-the-middle attack. In 1997, Pack [4] first discussed the certificate based protocols for wireless mobile communicate systems. In 2004, based on [4], Chang et al. [3] propose a certificate-based authentication combined with a session key agreement protocol. In their scheme, the session key agreement protocol is based on the Diffie-Hellman key exchange protocol. In 2005, Zhou et al. [1] pointed out that Chang et al.'s scheme is vulnerable to the impersonation attack, and proposed an improved scheme to prevent this security flaw. However, after our analysis, we find that Zhou's protocol is still insecure against the impersonation attack as well. We will show that by presenting a simple but powerful attack against their protocol.

The structure of this article is as follows. In section 2, we brief review Zhou et al.'s scheme. In section 3, we show the weakness found. Finally, a conclusion is given in section 4.

2. Review of Zhou et al.'s protocol

In a typical mobile communication system (e.g., GSM), communication between two mobile stations (MS) is usually established with the aid of two base stations (BS). It is usually that both the subscriber account information and the personal certificates of the

Manuscript received August 5 2006.
Manuscript revised August 18 2006.

mobile users are stored in the Subscriber Identity Module (SIM) card. Several parameters in Chang et al.'s protocol [3] which are also used in Zhou's protocol [1] are discussed as follows:

Let g be a generator of the multiplicative group Z_p^*, where p is a prime, and both g and p are made public. The private key of MS is $X_M \in Z_p^*$ and the public key is $Y_M = g^{-X_M} \bmod p$. Similarly, the private key and public key of BS are $X_B \in Z_p^*$ and $Y_B = g^{-X_B} \bmod p$, respectively. For simplicity, we will omit the operator " mod p" henceforth. The certificates of both MS and BS are represented in the following.

$$Cert_M = (ID_M, Y_M, data_M, [h(ID_M, Y_M, data_M)S_{CA}]),$$
$$Cert_B = (ID_B, Y_B, data_B, [h(ID_B, Y_B, data_B)S_{CA}]),$$

where $h(ID_i, R_i, data_i)S_{CA}$ means the hash value is signed by a CA's private key, S_{CA}. Both the private key X_M and the certificate $Cert_M$ of user M are stored in the SIM card. They wished their protocol [3] to be a perfect protocol. However, in 2005, Zhou et al. [1] pointed out that their protocol is insecure. Besides, they also proposed an improvement. In the following, we only show Chang et al.'s protocol in figure 1 and omit the details.

As for Zhou's protocol, we describe it as follows and illustrate it in figure 2.

(1) BS randomly selects a number R_B, then computes g^{R_B}, and sends g^{R_B}, $Cert_B$ to MS.

(2) MS randomly selects a number R_M, computes g^{R_M} and $sk_M = Y_B^{R_M} (g^{R_B})^{-X_M}$, where the public key of BS, Y_B, can be obtained from $Cert_B$. Finally, MS sends the message.

1. $BS \rightarrow MS : g^{R_B + X_B}, Cert_B$
2. $MS \rightarrow BS : g^{R_M + X_M}, Cert_M, f(sk_M, [ID_M, ID_B])$
3. $BS \rightarrow MS : f(sk_B, [ID_B, ID_M])$

$$sk_B = (Y_M \, g^{R_M + X_M})^{R_B} = (Y_B \, g^{R_B + X_B})^{R_M} = sk_M$$

Fig. 1. Chang's Protocol.

1. $BS \rightarrow MS : g^{R_B}, Cert_B$
2. $MS \rightarrow BS : g^{R_M}, Cert_M, f(2, sk_M, [ID_M, ID_B, g^{R_M}, g^{R_B}])$
3. $BS \rightarrow MS : f(3, sk_B, [ID_B, ID_M, g^{R_B}, g^{R_M}])$

$$sk_B = Y_M^{R_B} (g^{R_M})^{-X_B} = Y_B^{R_M} (g^{R_B})^{-X_M} = sk_M$$

Fig. 2. Zhou's Protocol.

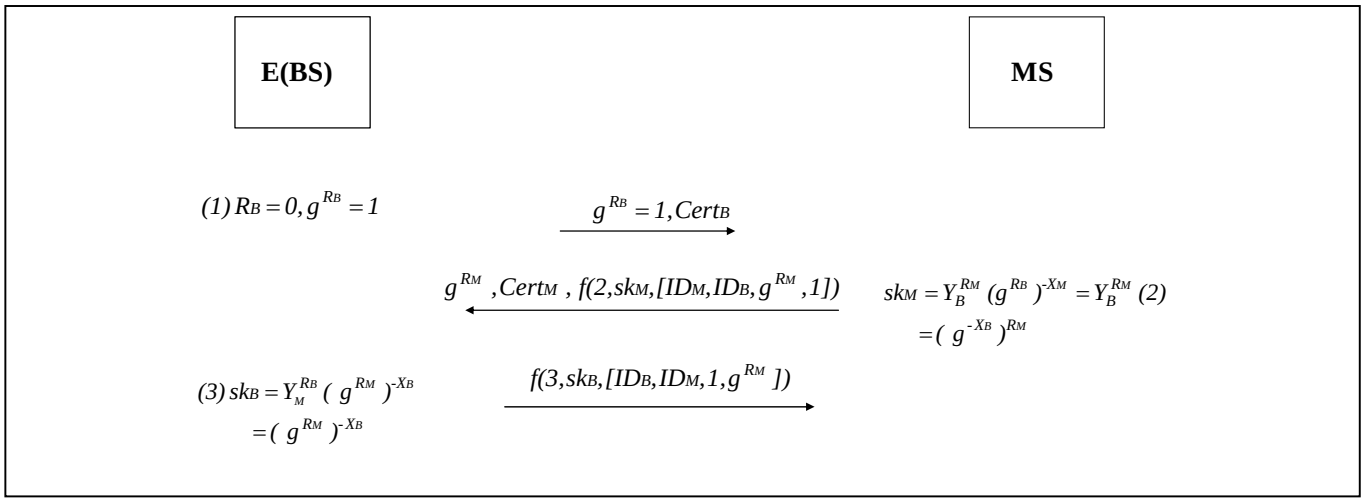

Fig. 3.Impersonation attack against Zhou's protocol.

< $g^{R_M}, Cert_M, f(2, sk_M, [ID_M, ID_B, g^{R_M}, g^{R_B}])$ > to BS.

(3) BS computes $sk_B = Y_M^{R_B} (g^{R_M})^{-X_B}$, and uses thus session key to check the validity of $f(2, sk_M, [ID_M, ID_B, g^{R_M}, g^{R_B}])$. Finally, BS sends the message $f(3, sk_B, [ID_B, ID_M, g^{R_B}, g^{R_M}])$ to MS. BS and MS can confirm each other's identity and session key after executing their protocol.

3. Cryptanalysis of Zhou et al.'s protocol

Although, Zhou et al. claimed that their scheme can resist against the impersonation attack. However, we still can find its mistake as illustrated in Fig. 3.

In our attack, we assume that an adversary E

(1) The adversary E selects R_B=0 and computes g^{R_B}=1, then he send 1, and $Cert_B$ to MS.

(2) MS randomly selects a number R_M, computes g^{R_M} and $sk_M = Y_B^{R_M} (g^{R_B})^{-X_M} = Y_B^{R_M} = (g^{-X_B})^{R_M}$, where the public key of BS, Y_B, can be obtained from $Cert_B$, then computes the hash value, $f(2, sk_M, [ID_M, ID_B, g^{R_M}, 1])$. Finally, MS sends the message < $g^{R_M}, Cert_M, f(2, sk_M, [ID_M, ID_B, g^{R_M}, 1])$ > to BS.

(3) Because R_B=0, the adversary E computes $sk_B = Y_M^{R_B} (g^{R_M})^{-X_B} = (g^{R_M})^{-X_B}$. Then E can check to see if the received hash code $f(2, sk_M, [ID_M, ID_B, g^{R_M}, 1])$ is valid using the computed session key sk_B. If it is valid, E sends

the message $f(3, sk_B, [ID_B, ID_M, 1, g^{R_M}])$ to MS.

It is obvious that E can cheat MS successfully.

Conversely, an adversary E can also successfully impersonate MS to BS in the same way. We omit the details.

4. Conclusion

We have shown that the Zhou et al.'s scheme suffers from the impersonation attacks. An adversary can utilize the simple method to impersonate one party to the other.

References

[1] Y. B. Zhou, Z. F. Zhang, and D. G. Feng, "Cryptanalysis of the End-to-End Security Protocol for Mobile Communications with End-User Identification/Authentication," *IEEE Communications Letters*, vol. 9, no. 4, April 2005.

[2] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inform. Theory*, vol. 22, pp. 644-654, Nov. 1976.

[3] C. C. Chang, K. L. Chen, and M. S. Hwang, "End-to-end security protocol for mobile communications with end-user identification/authentication," *Wireless Personal Communications*, vol. 28, pp. 95-106, Feb. 2004.

[4] C. S. Park, "On certificate-based security protocols for wireless mobile communication systems," *IEEE Network*, vol. 11, pp. 50-55, Sept./Oct.1997.

Jue-Sam Chou

received his Master degree in Applied Math. from National Chung Hsing University (NCHU) in Taichung, Taiwan in 1991, and received his Ph.D. degree in Computer Science and Information Engineering from National Chiao Tung University (NTCU) in Hsinchu, Taiwan. Currently, he teaches at Department of Information Mangement of Nanhua University as an Associate Professor. His primary research interests are information security.

Xian-Wu Hou

Currently, he is a student at Department of Information Mangement of Nanhua University in Taiwan for his Master degree. His primary research interests are information security.

Yalin Chen

She is now a PH. D. student at the departmetn of institute of information systems and applications in the school of National Tsing Hua University in Taiwan . Her primary research interests are information security,Computing complexity.