Fundamenta Informaticae 53 (2002) 131–134
IOS Press

Cryptanalysis of the Hwang-Shi Proxy Signature Scheme

Min-Shiang Hwang*
Department of Information Management, and
Graduate Institute of Networking and Communication Engineering
Chaoyang University of Technology
168 Gifeng E. Rd., Wufeng, Taichung County, Taiwan 413, R.O.C.
mshwang@mail.cyut.edu.tw

Cheng-Chi Lee†
Department of Computer and Information Science
National Chiao-Tung University
1001 Ta Hsueh Road, Hsinchu, Taiwan, R.O.C.
cclee@cis.nctu.edu.tw

Shin-Jia Hwang‡
Department of Computer Science and Information Engineering
TamKang University
Tamsui, Taipei Hsien,251,Taiwan, R.O.C.
sjhwang@mail.tku.edu.tw

Abstract. Recently, Hwang and Shi proposed an efficient proxy signature scheme without using one-way hash functions. In their scheme, an original signer needn't send a proxy certificate to a proxy signer through secure channels. However, there are two public key substitution methods that

*This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC89-2213-E-324-053.
Department of Information Management, and Graduate Institute of Networking and Communication Engineering, Chaoyang University of Technology, 168 Gifeng E. Rd., Wufeng, Taichung County, Taiwan 413, R.O.C.
†Address for correspondence: Department of Computer and Information Science, National Chiao-Tung University, 1001 Ta Hsueh Road, Hsinchu, Taiwan, R.O.C.
‡Address for correspondence: Department of Computer Science and Information Engineering, TamKang University, Tamsui, Taipei Hsien,251,Taiwan, R.O.C.

can be used to attack their scheme. In this article, we show that their scheme is vulnerable to the public key substitution attacks.

Keywords: Cryptography, Digital Signature, One-way Hash Function, Proxy Signatures.

1. Introduction

In 1996, Mambo, Usuda, and Okamoto first proposed a new category of signature scheme, called proxy signatures [7]. The proxy signature scheme allows a designed person, called a proxy signer, to sign on behalf of an original signer. Later, a number of various proxy signature schemes have been proposed [1, 5, 6, 9, 10]. Most of these schemes need one-way hash functions and secure channels to enhance their security.

Recently, Hwang and Shi proposed a new proxy signature scheme without using one-way hash functions [4]. In their scheme, an original signer needn't send a proxy certificate to a proxy signer through secure channels. However, there are two public key substitution attacks in Hwang-Shi's scheme. One is that the original signer can forge a valid proxy signature on behalf of the proxy signer. The other is that an attacker can forge a valid proxy signature on behalf of the original signer.

2. The Review Of The Hwang-Shi Proxy Signature Scheme

There are three public large prime numbers in Hwang-Shi's scheme [4]: P, Q, and P'. Q is a factor of $P-1$ and $P' > Q$. The public parameter g is a generator with order Q in Z_P and public parameter α is a primitive root in Z_P. We assume that Alice is an original signer and Bob is a proxy signer in this article. Alice and Bob have their secret key $x_A \in Z_Q$ and $x_B \in Z_Q$, and the corresponding public key $y_A = g^{x_A} \bmod P$ and $y_B = g^{x_B} \bmod P$, respectively. The steps of Hwang-Shi's scheme are briefly reviewed as follows.

1. Alice computes $r' = g^k \bmod P$, where k is a random integer in Z_Q. Next, Alice sends Bob (w, r'), where w is the warrant of the delegation.

2. Bob computes $r = g^a r' \bmod P$ and $r'' = y_A^a \bmod P$, where a is a random integer in Z_Q. Next, Bob sends Alice r''.

3. Alice computes $r = (r'')^{{x_A}^{-1}} r' \bmod P$, $W = (\alpha^w \bmod P') \bmod Q$, and $s' = (k + W r x_A) \bmod Q$. Alice sends s' to Bob.

4. Bob computes $W = (\alpha^w \bmod P') \bmod Q$ and checks the validity of s' by the equation $g^{s'} \equiv r'(y_A)^{rW} \bmod P$. If it holds, he then computes the proxy secret key $s = (s' + a + r x_B) \bmod Q$.

5. Bob can sign a message M on behalf of Alice using the proxy secret key s. The proxy signature on M is $(w, r, M, Sign_s(M))$.

6. A verifier can derive the corresponding proxy public key as follows.

$$g^s \equiv r(y_A)^{rW} y_B^r \bmod P, \tag{1}$$

where $W = (\alpha^w \bmod P') \bmod Q$. Then he/she uses the corresponding proxy public key g^s to verify the validity of $Sign_s(M)$.

3. Cryptanalysis

In this section, we propose two public key substitution attacks to Hwang-Shi proxy signature scheme. One is that the original signer, Alice, can forge a valid proxy signature on behalf of the proxy signer, Bob. The other is that an attacker, Eric, can forge a valid proxy signature on behalf of the original signer Alice.

Attack 1:
The original signer, Alice, chooses two random integers k' and a' in Z_Q, and computes $r = g^{a'} \bmod P$ and $W = (\alpha^w \bmod P') \bmod Q$. Then she updates her public key y_A to $y'_A = y_B^{-W^{-1}} g^{k'} \bmod P$. Next, Alice computes a valid proxy secret key $s' = a' + k'rW \bmod Q$ and uses s' to forge a valid proxy signature on behalf of Bob. A verifier can derive the corresponding proxy public key using Bob's public key, y_B, in Equation (1). The correctness of this attack can be proven as follows.

$$\begin{aligned} g^{s'} &\equiv r(y'_A)^{rW} y_B^r \bmod P, \\ &= g^{a'} (y_B^{-W^{-1}} g^{k'})^{rW} y_B^r \bmod P, \\ &= g^{a'} y_B^{-r} g^{k'rW} y_B^r \bmod P, \\ &= g^{a'+k'rW} \bmod P. \end{aligned} \tag{2}$$

Attack 2:
An attacker, Eric, chooses two random integers k' and a' in Z_Q, and computes $r = g^{a'} \bmod P$ and $W' = (\alpha^{w'} \bmod P') \bmod Q$, where w' is a forged warrant of the delegation by Eric. Then he updates his public key y_E to $y'_E = y_A^{-W'} g^{k'} \bmod P$. Next, Eric computes a valid proxy secret key $s' = a' + k'r \bmod Q$ and uses s' to forge a valid proxy signature on behalf of Alice. A verifier can derive the corresponding proxy public key using Alice's public key, y_A, in Equation (1). The correctness of this attack can be proven as follows.

$$\begin{aligned} g^{s'} &\equiv r(y_A)^{rW'} (y'_E)^r \bmod P, \\ &= g^{a'} (y_A)^{rW'} (y_A^{-W'} g^{k'})^r \bmod P, \\ &= g^{a'+k'r} \bmod P. \end{aligned} \tag{3}$$

4. Discussions and Conclusions

Although Hwang and Shi proposed an efficient proxy signature scheme without using one-way hash functions, we have shown that their scheme is vulnerable to public key substitution attacks in the above section. To withstand these attacks, we introduce two simple methods.

In the first method, we modify the warrant w such that the warrant includes public keys of original signer and proxy signer, and certificates of these public keys. The certificates are signed and issued by a trusted certificate authority (CA) [2, 3, 8]. In the method, anyone cannot easily substitute his/her public key and certificate unless he/she knows CA's private key. This method is also without using one-way hash functions. An original signer needn't send a proxy certificate to a proxy signer through secure channels as in Hwang-Shi's scheme.

In the second method, we give a slight improvement of Hwang-Shi's scheme as follows. We replace the symbol W with e in all steps of Hwang-Shi's scheme, where $e = h(w, y_A, y_B)$ and $h(\cdot)$ is a public one-way hash function. Although this method need to use a one-way hash function as [1, 5, 6, 9, 10], an original signer needn't send a proxy certificate to a proxy signer through secure channels as in Hwang-Shi's scheme.

Generally speaking, the warrant of the delegation w includes the original signer's and proxy signer's ID, the delegation period, the signing capability of the proxy signer, and the restricting documents to be signed [7]. In our first method, the warrant w additionally includes public keys of original signer and proxy signer, and certificates of the public keys. In our second method, the warrant w is not changed. The two improved schemes are more secure than Hwang-Shi's scheme.

References

[1] Hwang, M. S., Lin, I. C. and Lu, Eric J. L.: "A secure nonrepudiable threshold proxy signature scheme with known signers", *International Journal of Informatica*, **11 (2)**, 2000, 1–8.

[2] Hwang, M. S.: "A new dynamic cryptographic key generation scheme in a hierarchy", *Nordic Journal of Computing*, **6 (4)**, 1999, 363–371.

[3] Hwang, M. S.: "An asymmetric cryptographic scheme for a totally-ordered hierarchy", *International Journal of Computer Mathematics*, **73**, 2000, 463–468.

[4] Hwang, S. J. and Shi, C. H.: "A proxy signature scheme without using one-way hash functions". *Proceedings of 2000 International Computer Symposium (ICS2000)*, Taiwan, 2000.

[5] Kim, S., Park, S. and Won, D.: "Proxy signatures, revisted". *ICICS'97, Lecture Notes in Computer Science 1334, Springer-Verlag*, 1997, 223–232.

[6] Lee, N. Y., Hwang, T. and Wang, C. H.: "On Zhang's nonrepudiable proxy signature schemes". *Third Australasian Conference (ACISP'98)*, 1998, 415–422.

[7] Mambo, M., Usuda, K. and Okamoto, E.: "Proxy signatures: Delegation of the power to sign messages", *IEICE Trans. Fundamentals*, **E79-A (9)**, 1996, 1338–1354.

[8] Stallings, W.: *Cryptography and Network Security: Principles and Practice (2nd Edition*, Prentice Hall International, Inc., 1999.

[9] Sun, H. M.: "On proxy (multi-)signature schemes". *Proceedings of 2000 International Computer Symposium (ICS2000)*, Taiwan, 2000.

[10] Yi, L., Bai, G. and Xiao, G.: "Proxy multi-signature scheme: A new type of proxy signature scheme", *Electronics Letters*, **36 (6)**, 2000, 527–528.