Security analysis of the certificateless signature scheme proposed at SecUbiq 2006

Je Hong Park[1] and Bo Gyeong Kang[2]

[1] ETRI Network & Communication Security Division
jhpark@etri.re.kr
[2] Samsung Electronics Co., LTD
bogyeong.kang@samsung.com

Abstract. In this paper, we show that the certificateless signature scheme proposed by Yap, Heng and Goi at SecUbiq 2006 is insecure against a key replacement attack and a malicious-but-passive KGC attack, respectively. The former implies that anyone who replaces a signer's public key can forge valid signatures for that signer without knowledge of the signer's private key. The latter supposes the malicious-but-passive KGC, which generates system parameters based on the information of the target user to impersonate. Our results are based on the fact that the private key of the YHG scheme has the form of a BLS multisignature generated by the KGC and the user. Finally, we review the vulnerability of several certificateless signature schemes under theses attacks.

1 Introduction

The certificateless cryptosystem introduced by Al-Riyami and Paterson [1] is designed to overcome the key escrow limitation which is inherent in identity-based cryptosystems. Each user has a unique identifier, and a semi-trusted third party called the Key Generation Center(KGC) generates the partial private key associated with that identifier using its own master secret key and sends it to the user with that identifier. But the user also holds a secret value which is chosen by him/herself, and the user combines the partial private key with the secret value to generate his/her actual private key. That is, the user's private key is not generated by the KGC alone and so the KGC does not know the user's private key that implies the escrow freeness. Independent to the identifier, the user also publishes the public key, based on the secret value and system parameters. Note that the user's public key does not need to be certified by any trusted authority as in conventional PKIs. The structure of the certificateless scheme ensures that the key can be verified without a certificate. So its security model supposes the adversary who may attempt to replace a user's public key with a value of its own choice. This is called in general a *key replacement attack* [9, 4, 18, 6, 7] and, successfully applied to some certificateless signature schemes such as [1, 5].

In the original security model for certificateless cryptosystems [1], the KGC generates its master public/private key pair honestly, according to the scheme specification. However, the modified security model proposed by Au et al. [2]

removes this assumption. So the user's trust on the KGC is further relaxed. In detail, the KGC may not follow the scheme specification for generating system parameters and master key, while it does not actively replace a user's public key or corrupt the user's private key. The purpose of such a KGC is to compromise the target user's private key without being detected. Note that the *malicious* KGC is still *passive*, in the sense that the KGC would not actively replace the user public key or corrupt the user private key. It was shown in [2] that Al-Riyami-Paterson scheme [1] and Huang-Susilo-Mu-Zhang scheme [9] are vulnerable in this security model.

In SecUbiq 2006, Yap, Heng and Goi proposed a certificateless signature scheme (called the YHG scheme here) and claimed that their scheme is efficient, comparison to previous schemes [15]. Their improvement is supported by the lack of public key validation which requires pairing computations in the signature verification phase. We, however, show that the YHG scheme is insecure against a key replacement attack and a malicious-but-passive KGC attack, respectively. The former attack is based on the fact that the user private key of the YHG scheme has the form of a BLS multisignature [3] generated by the KGC and the user. We will apply a rogue attack for BLS multisignatures to the YHG scheme: Due to the lack of public key validation in the signature verification phase, a verifier cannot ensure that the signer knows the secret value. It implies that an adversary who replaces a signer's public key can forge signatures of that signer, without knowledge of the signer's private key. Additionally, we show that the malicious KGC can generate master public key using the target user's identifier and so it may impersonate that user easily, as described in [2]. Note that the Gorantla-Saxena scheme [5] and its improved scheme [17] are also vulnerable to this attack, due to structural similarity.

This paper is organized as the follows. We briefly review the YHG scheme in Section 2, and then analyze its security against two types of attacks in Section 3. We conclude in Section 4.

2 Review of YHG certificateless signature scheme

Throughout this paper, $(\mathbb{G}_1, +)$ and $(\mathbb{G}_2, \cdot)$ denote two cyclic groups of prime order q. A *pairing* is an efficiently computable, non-degenerate function $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ with the bilinearity property that $e(P + Q, R) = e(P, R) \cdot e(Q, R)$ and $e(P, Q + R) = e(P, Q) \cdot e(P, R)$ for $P, Q, R \in \mathbb{G}_1$. Let $H_1 : \{0,1\}^* \to \mathbb{G}_1$ and $H_2 : \{0,1\}^* \times \mathbb{G}_1 \to \mathbb{Z}_q^*$ be hash functions. These are used as a part of the system parameters generated by the KGC. The YHG certificateless signature scheme can be described as follows:

- Setup: Given a security parameter k, the KGC chooses an arbitrary generator $P \in \mathbb{G}_1$, selects a random $s \in \mathbb{Z}_q^*$ and sets $P_0 = sP$. Then the system parameters are $\mathsf{params} = \langle \mathbb{G}_1, \mathbb{G}_2, e, q, P, P_0, H_1, H_2 \rangle$. The message space is $\mathcal{M} = \{0,1\}^*$. The master secret key is $\mathsf{mk} = s$.

- Set Partial Private Key: Given the system parameters params, the master secret key mk and a user A's identifier ID_A, the KGC computes $Q_A = H_1(\mathsf{ID}_A) \in \mathbb{G}_1$ and outputs the partial private key $D_A = sQ_A$.
- Set Secret Value: Given the system parameters params, the user A selects a random value $x_A \in \mathbb{Z}_q^*$ as the user secret value.
- Set Private Key: Given the system parameters params and the partial private key D_A, the user A computes the user private key $S_A = x_A Q_A + D_A$.
- Set Public Key: Given the system parameters params and the secret value x_A, the user A computes the user public key $P_A = x_A P \in \mathbb{G}_1$.
- Signature Generation: Given the system parameters params, the identifier ID_A, a message $m \in \mathcal{M}$ and the private key S_A, the user A randomly chooses $r \in \mathbb{Z}_q^*$ and sets $U = rQ_A \in \mathbb{G}_1$. Then computes a signature $\sigma = (U, V)$ for the message m where $V = (r + h)S_A$ and $h = H_2(m, U)$.
- Signature Verification: Given a signature/message pair (σ, m), the signer's identifier ID_A and the signer's public key P_A, the verifier computes $h = H_2(m, U)$ and checks whether $e(P, V) = e(P_0 + P_A, U + hQ_A)$. If not, then rejects the signature else accepts it as valid.

The authors claim that this scheme is provably secure and more efficient then previously proposed schemes because fewer bilinear pairing computations are required [15]. As described above, this scheme requires only two pairing computations in the signature verification phase. This efficiency is induced from the lack of public key validation. We will show that this fact makes the YHG scheme vulnerable to the key replacement attack.

3 Security Analysis

3.1 Key replacement attack

Without loss of generality, the signer forwards his/her public key to the intended verifier(s) and announces his/her identifier. So an adversary who wants to forge a signature of a user A with the identifier ID_A runs as follows:

1. Randomly chooses $x \in \mathbb{Z}_q^*$ and computes a signature $\sigma = (U, V)$ for a message $m \in \mathcal{M}$ as follows:

$$U = rQ_A, h = H_2(m, U) \text{ and } V = (r + h)xQ_A,$$

   where $Q_A = H_1(\mathsf{ID}_A)$ and $r \in \mathbb{Z}_q^*$.
2. Sets $P'_A = xP - P_0$ as a public key of the user A.
3. Then sends the signature σ, the message m, the identifier ID_A and the public key P'_A to the verifier(s).

Then the verifier computes $h = H_2(m, U)$ and checks whether $\langle P, P_0 + P'_A, U + hQ_A, V\rangle$ is a valid Diffie-Hellman tuple. Since $e(P, V) = e(P, (r + h)xQ_A)$ and $e(P_0 + P'_A, U + hQ_A) = e(xP, (r + h)Q_A)$, $e(P, V) = e(P_0 + P'_A, U + hQ_A)$ and so $\langle P, P_0 + P'_A, U + hQ_A, V\rangle$ is valid. Hence σ is verified as a valid signature for the message m generated by the user A.

This attack is based on the algebraic structure of a user's private key in the YHG scheme. Since the signer A's private key S_A has the form of a BLS multisignature [3] generated by the KGC and the signer A, we can apply a rogue attack using the key substitution trick. In general, a rogue attack for BLS multisignatures can be described as follows: Let $pk_A = x_A P$ and $pk_B = x_B P$ be two public keys of the user Alice and Bob, respectively. But Bob replaces pk_B by $pk_B - pk_A$. Then for a message m, $x_B H_1(m) = x_A H_1(m) + (x_B - x_A)H_1(m)$ can be regarded as a valid multisignature on m by both Alice and Bob. In the YHG scheme, the KGC plays the role of a honest user to generate a multisignature for the identifier ID_A of a user A and is prohibited to replace the user A's public key. But a third party can use this key substitution trick for BLS multisignatures to forge a YHG signature of the user A, based on two facts that the user A's public key is not certified and knowledge of the secret value corresponding to the signer's public key is not, even implicitly, checked in the signature verification phase.

To prevent this attack, therefore, the signature verification phase is required to demonstrate that the signer has knowledge of the secret value corresponding to the public key [4]. One instance to provide it is to modify the public key of a user A to include an additional value $x_A P_0$, where x_A is the secret value of the user A and then to add the public key validity check equation

$$e(P_0, P_A) = e(P, x_A P_0) \tag{1}$$

to the signature verification phase [4]. This equation basically ensures that the signer A's public key $\langle X, Y \rangle$ holds the relation $Y = sX$ where $Y = x_A P_0$ and $X = P_A$. Furthermore, it makes sure that the secret value x_A, chosen by the signer A, has been used correctly to obtain $S_A = x_A Q_A + D_A$ [6, 7]. Though an adversary is able to replace the public key P_A by P'_A, it is impossible to pass the equation (1) without knowledge of the discrete logarithm of P'_A. Unfortunately, this modification requires four pairing computations though only two are needed per signature if multiple signatures by the same signer are to be verified. Note that this modification only provides a way to defend our attack, and so does not guarantee the security against other attacks [8]. We provide such an example in the following subsection.

Remark 1. Independently, the same attack for the YHG scheme was proposed by Zhang and Feng [16], after we published a preliminary version of this paper [14]. While our attack chooses a random exponent $r \in \mathbb{Z}_q^*$ to construct U, they choose $U \in \mathbb{G}_1$ itself as a random factor of a forged signature $\sigma = (U, V)$. Since $V = (r+h)xQ_A = x(U + hQ_A)$, there is nothing to differentiate between two attacks.

3.2 Malicious-but-passive KGC attack

Although the above key replacement attack can be prevented by additional checking process, the following malicious-but-passive KGC attack is still applied

to the (modified) YHG scheme. Note that this attack is not captured in [15] because the security of the YHG scheme is only considered in the original security model of [1], but not of [2].

At first, fix a target user A with the identity ID_A. Then the malicious KGC randomly chooses $\alpha \in \mathbb{Z}_q^*$ and computes $P = \alpha H(\mathsf{ID}_A)$. Then the user A computes his/her public key and private key pair as follows:

$$P_A = x_A P = x_A \alpha H(\mathsf{ID}_A)$$
$$S_A = x_A Q_A + D_A = x_A(1/\alpha)P + D_A = (1/\alpha)P_A + D_A.$$

Since the KGC knows α, P_A and D_A, the private key S_A of the user A can be easily computed by the malicious KGC. As a result, we show that the (modified) YHG scheme is weak against the malicious-but-passive KGC attack though the scheme does not have the same key generation procedure as that of [1].

Remark 2. The Gorantla-Saxena scheme [5] and its improved scheme [17] have a similar structure with the YHG scheme. So, it is very easy to check that both schemes are also vulnerable to a malicious-but-passive KGC attack.

Besides [1, 9], it was shown that certificateless signature schemes in [12] and [13] are insecure against the malicious-but-passive KGC attack [8]. Additionally, the certificateless designated verifier signature scheme proposed by Huang et al. is vulnerable to the malicious-but-passive KGC attack as they follow the same system parameters and user key generation procedure as that of [1].

It can be easily checked that the mediated certificateless signature scheme proposed by Ju et al. [11] is vulnerable to key replacement and malicious-but-passive attacks. A mediated certificateless signature scheme uses an online semi-trusted entity called the Security Mediator(SEM) for easy revocation of the user signing key. Since a key replacement attack is not related to the partial private key generated by the KGC (and shared by the user and the SEM), the attack in [9] is applied to the Ju et al.'s scheme directly. Similarly, a malicious-but-passive KGC attack in [2] also works because the SEM does not participate in the system parameters generation phase.

4 Conclusion

We showed that the YHG certificateless signature scheme is vulnerable to a key replacement attack and a malicious-but-passive attack, respectively. In addition, we pointed out the same weakness of several certificateless signature schemes under these attacks.

References

1. S.S. Al-Riyami and K.G. Paterson. Certificateless public key cryptography. *Advances in Cryptology - ASIACRYPT 2003*, Lecture Notes in Comput. Sci., vol.2894, pp.452–473, 2003.

2. M.H. Au, J. Chen, J.K. Liu, Y. Mu, D.S. Wong and G. Yang. Malicious KGC attacks in certificateless cryptography. *Proc. of ASIACCS 2007*, pp.302–311, 2007.
3. A. Boldyreva. Efficient threshold signature, multisignature and blind signature schemes based on the gap-Diffie-Hellman-group signature scheme. *Public Key Cryptography - PKC 2003*, Lecture Notes in Comput. Sci., vol.2567, pp.31–46, 2003.
4. X. Cao, K.G. Paterson and W. Kou. An attack on a certificateless signature scheme. *Cryptology ePrint Archive*, Report 2006/367.
5. M.C. Gorantla and A. Saxena. An efficient certificateless signature scheme. *Computational Intelligence and Security - CIS 2005*, Lecture Notes in Articifical Intelligence, vol.3802, pp.110-116, 2005.
6. B.C. Hu, D.S. Wong, Z. Zhang and X. Deng. Key replacement attack against a generic construction of certificateless signature. *Information Security and Privacy - ACISP 2006*, Lecture Notes in Comput. Sci., vol.4058, pp.235–246, 2006. This is a preliminary version of [7]
7. B.C. Hu, D.S. Wong, Z. Zhang and X. Deng. Certificateless signature: A new security model and an improved generic construction. *Des. Codes. Crypt.*, vol.42, pp.109–126, 2007. This is a full version of [6]
8. X. Huang, Y. Mu, W. Susilo, D.S. Wong and W. Wu. Certificateless signature revisited. *Information Security and Privacy - ACISP 2007*, Lecture Notes in Comput. Sci., vol.4586, pp.308–322, 2007.
9. X. Huang, W. Susilo, Y. Mu and F. Zhang. On the security of certificateless signature schemes from Asiacrypt 2003. *Cryptology and Network Security - CANS 2005*, Lecture Notes in Comput. Sci., vol.3810, pp.13–25, 2005.
10. X. Huang, W. Susilo, Y. Mu and F. Zhang. Certificateless designated verifier signature schemes. *Proc. of AINA 2006*, pp.15–19, 2006.
11. H.S. Ju, D.Y. Kim, D.H. Lee, J. Lim and K. Chun. Efficient revocation of security capability in certificateless public key cryptography. *Proc. of KES 2005*, pp.453–459, 2005.
12. X. Li, K. Chen and L. Sun. Certificateless signature and proxy signature schemes from bilinear pairings. *Lithuanian Mathematical Journal*, vol.45, pp.76–83, 2005.
13. J.K. Liu, M.H. Au and W. Susilo. Self-generated-certificate public key cryptography and certificateless signature/encryption scheme in the standard model. *Proc. of ASIACCS 2007*, pp.273–283, 2007.
14. J.H. Park. An attack on the certificateless signature scheme from EUC Workshops 2006. *Cryptology ePrint Archive*, Report 2006/442.
15. W.-S. Yap, S.-H. Heng and B.-M. Goi. An efficient certificateless signature scheme. *Embedded and Ubiquitous Computing - EUC 2006 Workshops*, Lecture Notes in Comput. Sci., vol.4097, pp.322–331, 2006.
16. Z. Zhang and D. Feng. Key replacement attack on a certificateless signature scheme. *Cryptology ePrint Archive*, Report 2006/453.
17. J. Zhang and J. Mao. Security analysis of two signature schemes and their improved schemes. *Computational Science and Its Applications - ICCSA 2007*, Lecture Notes in Comput. Sci., vol.4705, Part I, pp. 589–602, 2007.
18. Z. Zhang, D.S. Wong, J. Xu and D. Feng. Certificateless public-key signature: Security model and efficient construction. *Applied Cryptography and Network Security - ACNS 2006*, Lecture Notes in Comput. Sci., vol.3989, pp.293–308, 2006.