Key Replacement Attack on a Certificateless Signature Scheme

Zhenfeng Zhang, **Dengguo Feng**,

State Key Laboratory of Information Security
Institute of Software, Chinese Academy of Sciences, Beijing 100080, P.R.China
zfzhang@is.iscas.ac.cn

Abstract. Yap, Heng and Goi propose an efficient certificateless signature scheme based on the intractability of the computational Diffie-Hellman problem, and prove that the scheme is secure in the random oracle model. This paper shows that their certificateless signature scheme is vulnerable to key replacement attacks, where an adversary who replaces the public key of a signer can forge valid signatures on any messages for that signer without knowing the signer's private key.

Keywords: Certificateless signature, key replacement attack, bilinear pairing, forgery

1 Introduction

In order to simplify certificate management as in traditional Public Key Infrastructure, Shamir [4] introduced the concept of identity-based public key cryptography (ID-PKC), in which the public-key of a user can be derived from his unique identifier information, whereas the only secret of a user is generated by a key generator center (KGC). Therefore, there is an inherent key escrow issue in such identity-based cryptosystems.

Certificateless public key cryptography (CL-PKC), introduced by Al-Riyami and Paterson [1], is intended to solve the key escrow issue which is inherent in identity-based cryptography [4], while at the same time, eliminate the use of certificates as in the conventional Public Key Infrastructure. Unlike ID-PKC, user's private-key of CL-PKC schemes is not generated by a Key Generation Center (KGC) alone. Instead, it is a combination of KGC-produced partial-private-key and an additional user-chosen secret. In this way, they successfully eliminate the built-in escrow properties, since KGC could not control the user's private-key entirely. Meanwhile, CL-PKC is not identity-based any longer, and an additional public-key must be generated from user's randomly-chosen secret information. However, in CL-PKC, a user does not need to obtain a certificate from the trusted authority in order to establish the authenticity of his public key. Therefore, one must then model attacks in which an adversary simply replaces a user's public key with a value of his choice, and show that such a public key replacement attack does not give the adversary an advantage in breaking any particular certificateless scheme.

Al-Riyami and Paterson established the security model for certificateless public key encryption scheme [1] and proposed efficient constructions. Although an certificateless signature scheme is also introduced and proposed in [1], the security model for certificateless signature scheme is not specified explicitly. A strict model for certificateless signature schemes was presented by Zhang et al. [6] and Hu et al. [3].

In a certificateless signature scheme, the security is assessed in terms of two different kinds of attackers. The first kind of attacker (or Type I attacker) is meant to represent a normal third party attack against the existential unforgeability of the system. Due to the uncertified nature of the public-keys produced by the users, one must assume that the attacker is able to replace these entities' public keys at will. This represents the attackers' ability to fool a user into accepting a signature using a public key that has been supplied by the attacker. Therefore, a certificateless signature is required to be secure against *key replacement attack*, a third party who can replace the user's public/secret key pair but does not know the user's partial private key issued by the KGC cannot generate valid signatures as the user either. The second kind of attacker (Type II attacker) represents a malicious key generation center, who is given the key generation center's long term secret, but may not replace entities' public keys.

Recently, Yap, Heng and Goi [5] proposed an efficient certificateless signature scheme based on the intractability of the computational Diffie-Hellman problem. The proposed scheme is very efficient as no pairing computation is needed in the signing algorithm, and only two pairing computations are needed in the verification algorithm. The author proved in the random oracle model that the certificateless signature scheme [5] is secure against a Type I adversary, and they also claimed that the scheme is existential unforgeable against a Type II adversary. However, this paper shows that their certificateless signature scheme is vulnerable to public key replacement attacks, where an adversary who replaces the public key of a signer can forge valid signatures on any messages for that signer without knowledge of the signer's partial private key.

The rest of the paper is organized as follows. In Section 2, we present a brief description of Yap, Heng and Goi's certificateless signature scheme. A public key replacement attack on the Yap-Heng-Goi scheme is presented in section 3. Section 4 provides a conclusion.

2 Yap, Heng and Goi's Certificateless Signature Scheme

Let $(\mathcal{G}_1, +)$ and $(\mathcal{G}_2, \cdot)$ be two cyclic groups of order q, P be a generator of $\mathcal{G}_1$, $e : \mathcal{G}_1 \times \mathcal{G}_1 \to \mathcal{G}_2$ be an admissible bilinear pairing, which satisfies the following conditions:

1. Bilinearity: For any $P, Q, R \in \mathcal{G}_1$, we have $e(P+Q, R) = e(P, R)e(Q, R)$ and $e(P, Q + R) = e(P, Q)e(P, R)$. In particular, for any $a, b \in \mathbf{Z}_q$,

$$e(aP, bP) = e(P, P)^{ab} = e(P, abP) = e(abP, P).$$

2. Non-degeneracy: There exists $P, Q \in \mathcal{G}_1$, such that $e(P, Q) \neq 1$.
3. Computability: There is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in \mathcal{G}_1$.

The typical way of obtaining such pairings is by deriving them from the Weil-pairing or the Tate-pairing on an elliptic curve over a finite field. One can refer to [2] for a more comprehensive description on how these groups, pairings and other parameters should be selected for efficiency and security.

Yap, Heng and Goi's certificateless signature scheme [5] consists of seven polynomial-time algorithms:

• `Setup.` Given a security parameter k, this algorithm chooses two groups $\mathcal{G}_1$ and $\mathcal{G}_2$ of prime order q, specifies a bilinear pairing $e : \mathcal{G}_1 \times \mathcal{G}_1 \rightarrow \mathcal{G}_2$, and selects an generator $P \in \mathcal{G}_1$. It then picks at random $s \in \mathbf{Z}_q^*$ and set $P_{pub} = sP$. The algorithm also chooses cryptographic hash functions $H_1 : \{0, 1\}^* \rightarrow \mathcal{G}_1$, $H_2 : \{0, 1\}^* \times \mathcal{G}_1 \rightarrow \mathbf{Z}_q^*$.

The system's public parameters are `params` $= (\mathcal{G}_1, \mathcal{G}_2, e, P, P_{pub}, H_1, H_2)$. The master key is s.

• `Set-Partial-Private-Key:` Given `params`, master-key s and an identity ID_A, this algorithm computes $Q_A = H_1(ID_A) \in \mathcal{G}1$ and output a partial private key $D_A = sQ_A \in \mathcal{G}_1$.

• `Set-Secret-Value:` Given `params`, select a random value $x_A \in \mathbf{Z}_q$ where x_A is the secret value.

• `Set-Private-Key:` Set private key $S_A = (x_A Q_A + D_A)$.

• `Set-Public-Key:` Given `params` and the secret value x_A, this algorithm computes $P_A = x_A P \in \mathcal{G}_1$.

• `Sign:` Given `params`, ID_A, message m and private key S_A, the algorithm works as follows:

– Compute $Q_A = H_1(ID_A) \in \mathcal{G}_1$.
– Choose a random value $r \in \mathbf{Z}_q$ and set $U = rQ_A \in \mathcal{G}_1$.
– Set $h = H_2(m\|U) \in \mathbf{Z}_q$.
– Compute $V = (r + h)S_A$.
– Set $\sigma = (U, V)$ as the signature of m.

• `Verify:` Given signature σ, ID_A, m and P_A, this algorithm works as follows:

– Compute $Q_A = H_1(ID_A) \in \mathcal{G}_1$.
– Compute $h = H_2(m\|U) \in \mathbf{Z}_q$.

- Check whether $(P, P_0 + P_A, U + hQ_A, V)$ is a valid Diffie-Hellman tuple, i.e. by verifying whether $e(P, V) = e(P_0 + P_A, U + hQ_A)$. If not, then reject the signature else accept it.

The above certificateless signature scheme is efficient, since no pairing computation is needed in the signing algorithm, and two pairing computations are needed in the verification algorithm.

3 Public key replacement attack on the Yap-Heng-Goi Scheme

In [5], the author proved in the random oracle model that the certificateless signature scheme is secure against a type I adversary $\mathcal{A}_I$, who does not have access to master-key, but may replace public keys at will, and they also claimed that the scheme is existential unforgeable against a type II adversary $\mathcal{A}_{II}$, who does have access to master-key, but cannot replace public keys of entities.

However, their certificateless signature scheme is in fact insecure against a type I adversary $\mathcal{A}_I$. Precisely, an adversary $\mathcal{A}_I$ can replace an entity's public key, and then forge valid signatures on any messages for that signer without knowledge of the signer's partial private key. The details of the attack are shown as following.

An adversary $\mathcal{A}_I$ first chooses a number $t \in \mathbf{Z}_q^*$ at random, and then replace the public of a signer with identity ID_A with the value $P_A = tP - P_0$. Then $\mathcal{A}_I$ forge a signature on any message m, without the knowledge of private key S_A of the signer, as following:

- Compute $Q_A = H_1(ID_A) \in \mathcal{G}_1$.
- Choose a random point $U \in \mathcal{G}_1$.
- Set $h = H_2(m \| U) \in \mathbf{Z}_q$.
- Compute $V = t(U + hQ_A)$.
- Output $\tilde{\sigma} = (U, V)$ as the signature of m.

Given the signature $\tilde{\sigma}$, ID_A, m and P_A, the corresponding verification algorithm will work as follows:

- Compute $Q_A = H_1(ID_A) \in \mathcal{G}_1$.
- Compute $h = H_2(m \| U) \in \mathbf{Z}_q$.
- Check whether $e(P, V) = e(P_0 + P_A, U + hQ_A)$, and accepted the signature only if it holds. Since $V = t(U + hQ_A)$ and $P_A = tP - P_0$, one can derive that

$$e(P, V) = e(P, t(U + hQ_A)) = e(tP, U + hQ_A) = e(P_0 + P_A, U + hQ_A).$$

As a result, the signature $\tilde{\sigma}$ can always pass the verification algorithm, and thus be accepted by any verifier as a valid signature on message m for a signer with identity ID_A and public key P_A.

Yap, Heng and Goi further extended their construction to achieve trust level 3 on KGC. In the extended construction, user A first fix its secret value x_A and its public key $P_A = x_A P$. Then, KGC generates the partial private key D_A for user A by returning sQ_A where $Q_A = H_1(ID_A \| P_A)$. By thie technique, the KGC who replaces user's public key will be implicated in the event of dispute: the existence of two working public keys for an identity can only result from the existence of two partial private keys binding that identity to two different public keys. Thus the KGC's misbehavior can be detected and proved.

It is easy to see that the extended construction is also insecure against a Type I adversary. The proposed public key replacement attack also works for the extended construction.

4 Conclusion

Yap, Heng and Goi [5] propose an efficient certificateless signature scheme recently, and prove that the scheme is secure in the random oracle model. This paper examines the security of their certificateless signature scheme against the key replacement attack, which is one basic attack against a certificateless public key scheme, and shows that it cannot resist such an attack, i.e. an adversary who replaces the public key of a signer can forge valid signatures on any messages for that signer without knowing the signer's private key.

References

1. S. Al-Riyami and K. Paterson, Certificateless public key cryptography, Advances in Cryptology-Asiacrypt'2003, *Lecture Notes in Computer Science*, vol. 2894, pages 452-473, Springer-Verlag, 2003.
2. D. Boneh and F. Franklin, Identity-based encryption from the Weil pairing, *SIAM Journal on Computing*, 32, 586-615, 2003.
3. B. C. Hu, D. S. Wong, Z. Zhang, and X. Deng. Key replacement attack against a generic construction of certificateless signature. In Information Security and Privacy: 11th Australasian Conference, ACISP 2006, *Lecture Notes in Computer Science*, vol.4058, pages 235-246. Springer-Verlag, 2006.
4. A. Shamir, Identity based cryptosystems and signature schemes, Advances in Cryptology-Crypto'84, *Lecture Notes in Computer Science*, vol. 196, pages 47-53, Springer-Verlag, 1984.
5. Wun-She Yap, Swee-Huay Heng, and Bok-Min Goi, An Efficient Certificateless Signature Scheme, X. Zhou et al. (Eds.): Emerging Directions in Embedded and Ubiquitous Computing, EUC Workshops 2006, *Lecture Notes in Computer Science*, vol. 4097, pages 322-331, Springer-Verlag, 2006.
6. Z. Zhang, D. Wong, J. Xu, and D. Feng. Certificateless public-key signature: Security model and efficient construction. In 4th International Conference on Applied Cryptography and Network Security, ACNS 2006, *Lecture Notes in Computer Science*, vol.3989, pages 293-308, Springer-Verlag, 2006.