An Attack on a Certificateless Signature Scheme

Xuefei Cao[1], Kenneth G. Paterson*[2], and Weidong Kou[1]

[1] Chinese State Key Laboratory of Integrated Services and Networks, Xidian University, Xi'an 710071, China
xfcao@mail.xidian.edu.cn
[2] Information Security Group, Royal Holloway, University of London, Egham, Surrey TW20 OEX, U.K.
kenny.paterson@rhul.ac.uk

Abstract. This paper demonstrates that a certificateless signature scheme recently proposed by Gorantla and Saxena is insecure. It is shown that an adversary who replaces the public key of a signer can then forge valid signatures for that signer without knowledge of the signer's private key.

Index terms: Certificateless public key signature; replacement attack; forgery

1 Introduction

In order to simplify certificate management in traditional PKI, Shamir [1] introduced the concept of ID-based public key cryptography (ID-PKC). However, key escrow is an inherent issue with ID-PKC because the Private Key Generator knows all the users' private keys within the system. Al Riyami and Paterson [2] introduced the concept of certificateless public key cryptography (CL-PKC) in an effort to remove this escrow property whilst maintaining the attractive properties of ID-PKC.

In a CL-PKC sytem, a Trusted Authority (TA) supplies each user with a partial private key (PPK). A user then combines his PPK with a user-selected secret value to obtain his private key. He also makes available a matching public key. The use of user-selected secret values in CL-PKC removes the key escrow property that is inherent in ID-PKC. Moreover, 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. However, 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.

Recently, Gorantla and Saxena [3] introduced an efficient certificateless signature scheme based on pairings (or bi-linear maps). One reason that their scheme is more efficient than previous proposals is that no pairing-based structural checks are made on the public key before it is used. This is in contrast to the

* This author would like to thank the organisers of CIS 2005 for their very kind hospitality during his visit to Xi'an.

certificateless signature scheme of [2], for example. Gorantla and Saxena claimed that, in the context of a security analysis of their new scheme, *"a replacement attack is not useful unless the adversary has the corresponding private key."* Implicitly, they also claimed that their scheme could withstand replacement attacks without any checks on the public key. In this paper, we show that, in fact, the Gorantla-Saxena scheme is insecure against replacement attack. We show that an adversary who replaces the public key of a user can trivially forge signatures of that user, without knowledge of the user's private key. The remainder of this paper is arranged as follows: Section 2 summarizes the Gorantla-Saxena scheme from [3]. Section 3 presents our replacement attack on the Gorantla-Saxena scheme. Section 4 sketches a variant of the Gorantla-Saxena which prevents our attack and so has improved security. Section 5 provides a conclusion.

2 The Gorantla-Saxena Certificateless Signature Scheme

Let G_1 and G_2 be additive and multiplicative cyclic groups of prime order q, respectively, and let P be an arbitrary generator of G_1. Let $e : G_1 \times G_1 \rightarrow G_2$ be a map with following properties:

1. Bilinear: For all $R, S, T \in G_1$,

$$e(R + S, T) = e(R, T)e(S, T) \text{ and } e(R, S + T) = e(R, S)e(R, T).$$

2. Non-degenerate: $e(P, P) \neq 1_{G_2}$.
3. Computable: There exists an efficient algorithm to compute $e(R, S)$ for all $R, S \in G_1$.

The Gorantla-Saxena scheme [3] is then composed of seven algorithms as follows:
`Setup`: The TA performs the follows steps:

1. Specifies G_1, G_2, q, e, P as described above.
2. Selects a secret master-key t at random from $\mathbb{Z}_q^*$ and sets the TA's public key Q_{TA} to be tP.
3. Chooses two hash functions $H_1 : \{0,1\}^* \times G_1 \rightarrow \mathbb{Z}_q^*$ and $H_2 : \{0,1\}^* \rightarrow G_1$.

The TA then publishes the system parameters $\langle G_1, G_2, q, e, P, Q_{TA}, H_1, H_2 \rangle$ along with descriptions of the message space $\mathcal{M} = \{0,1\}^*$ and the signature space $\mathcal{S} = G_1 \times G_1$.
`Partial-Private-Key-Extract`: The TA calculates $Q_A = H_2(ID_A)$, where ID_A is an identifier associated uniquely with A. The TA then sends the partial private key $D_A = tQ_A$ to A via a secure channel.
`Set-Secret-Value`: The user A selects a random value $s \in \mathbb{Z}_q^*$.
`Set-Private-Key`: A calculates his private key as $S_A = sD_A$.
`Set-Public-Key`: A calculates his public key as $P_A = sQ_{TA}$.
`Sign`: A signs a message $m \in \{0,1\}^*$ using private key S_A as follows:

1. Choose random $\ell \in \mathbb{Z}_q^*$.
2. Compute $U = \ell Q_A + Q_{TA}$.
3. Compute $h = H_1(m, U)$.
4. Compute $V = (\ell + h)S_A$.

User A's signature on m is the pair $\langle U, V \rangle$.
`Verify`: A verifier checks a purported signature $\langle U, V \rangle$ on message m given A's identifier ID_A and public key P_A as follows:

1. Compute $h = H_1(m, U)$
2. Check whether the equality

$$e(P, V)e(P_A, Q_{TA}) = e(P_A, U + hQ_A)$$

holds. The signature is accepted if it does and rejected otherwise.

Note that the verification equation in the above signature scheme is mathematically equivalent to checking:

$$e(P, V) = e(P_A, U + hQ_A - Q_{TA}).$$

This shows that signature verification needs only 2 pairing computations, rather than 3 as in the original presentation of [3].

3 An Attack on the Gorantla-Saxena Scheme

The above efficiency improvement leads to our replacement attack on the Gorantla-Saxena scheme. In our attack, the adversary chooses a random $k \in \mathbb{Z}_q^*$ and replaces A's public key with the value $P'_A = kP$. Notice that the verification equation, now involving P'_A, can be rewritten as:

$$e(P, V) = e(P, k(U + hQ_A - Q_{TA}))$$

which in turn is equivalent to the condition:

$$V = k(U + hQ_A - Q_{TA}).$$

Thus the adversary can perform the following steps to sign a message m without knowing A's private key:

1. Choose random $\ell \in \mathbb{Z}_q^*$.
2. Compute $U = \ell Q_A + Q_{TA}$.
3. Compute $h = H_1(m, U)$.
4. Compute $V = k(U + hQ_A - Q_{TA})$.

The adversary outputs the pair $\langle U, V \rangle$ as the forged signature. By construction, this signature will automatically satisfy the verification equation using the replaced public key $P'_A = kP$. (This fact can also be easily verified directly.)

This attack shows that the Gorantla-Saxena scheme, while relatively efficient, is not a secure certificateless signature scheme.

4 Improving the Gorantla-Saxena Scheme

The security of the Gorantla-Saxena scheme can be improved by modifying it so as to prevent the replacement attack above. This can be done by changing the scheme so that the verification procedure also demonstrates that the signer has knowledge of his secret value (the adversary in our attack does not). One way to do this is to extend a user A's public key to include an additional value sP (where s is A's secret value) and to replace the single verification equation by the pair of equations:

$$e(sP, Q_{TA}) = e(P, P_A) \text{ and } e(P, V) = e(P_A, U + hQ_A - Q_{TA})$$

where the second equation comes from our previous improvement over the verification equation of [3]. Unfortunately, the new verification procedure requires 4 pairing calculations (though only 2 are needed per signature if multiple signatures by the same signer are to be verified).

Note that we do not claim this modified scheme to be secure: a more formal security analysis would be needed in order to establish this.

5 Conclusion

We have shown that Gorantla and Saxena's certificateless signature scheme is insecure by demonstrating that it is vulnerable to a public key replacement attack. Further, we have provided an improvement in which signature verification additionally demonstrates that the signer has knowledge of his secret value. The improved scheme prevents our replacement attack.

References

1. A.Shamir. Identity-based cryptosystems and signature schemes. In *Advances in Cryptology – CRYPTO'84*, LNCS Vol. 196, Springer-Verlag, pp. 47-53, 1984.
2. S.S. Al-Riyami and K..G.Paterson. Certificateless public key cryptography. In *Advances in Cryptology – ASIACRYPT 2003*, LNCS Vol. 2894, Springer-Verlag, pp. 452-473, 2003.
3. M.C. Gorantla and A. Saxena. An efficient certificateless signature scheme. In *Computational Intelligence and Security (CIS) 2005*, LNAI Vol. 3802, Springer-Verlag, pp. 110-116, 2005.