情報保護學會論文誌
第19巻 第6號, 2009. 12

두 인증서 없는 서명 기법들에 관한 안전성 분석*

이 주 희,[1†] 심 경 아,[2‡] 이 향 숙[1]
[1]이화여자대학교, [2]국가수리과학연구소

Security Analysis of Two Certificateless Signature Schemes*

Ju-Hee Lee,[1†] Kyung-Ah Shim,[2‡] Hyang-Sook Lee[1]
[1]Ewha Womans University, [2]National Institute for Mathematical Sciences

요 약

인증서 없는 공개키 시스템은 기존의 공개키 암호시스템에서 인증서의 필요성을 제거하고 신원 기반 암호시스템에서 키 위탁 문제를 해결하였다. 본 논문에서는 Guo 등과 Wang 등에 의해서 제안된 각각의 인증서 없는 서명 기법들이 공격자 종류 I에 의해 키 대치공격에 취약하다는 것을 보인다. 다시 말해, 서명자의 공개키를 대치할 수 있는 능력을 가진 공격자가 서명자의 비밀키를 알지 못함에도 불구하고 서명을 위조할 수 있음을 보이고 이러한 공격을 방지하기 위한 대응법을 제안한다.

ABSTRACT

Certificateless cryptography eliminates the need of certificacates in the public key crytosystems and solves the inherent key escrow problem in identity-based cryptosystems. This paper demonstrates that two certificateless signature schemes proposed by Guo et al. and Wang et al. respectively are insecure against key replacement attacks by a type I adversary. We show that the adversary who can replace a signer's public key can forge signatures under the replaced public key. We then make a suggestion to prevent the attacks.

Keywords: Certificateless cryptography, Digital signature, Key replacement attack, Forgery

I. Introduction

In 1984, Shamir[11] introduced an identity (ID)-based cryptosystem to simplify key management procedures of the infrastructure (PKI). This notion is to use a binary string which can uniquely identify a user as the user's public key. Examples of such a binary string include email address, IP address and social security number, etc. Certificates are only needed for some trusted authorities called a Private Key Generator (PKG) which is responsible for generating private keys for users. An inherent problem of the ID-based cryptography is the key escrow problem, i.e., the private key of a user is known to the PKG. The PKG can decrypt any ciphertext and forge signature on any message for any user. In 2003, Al-Riyami and Paterson[1] introduced a certificateless Public Key Cryptosystem (CL-PKC) in order to avoid the inherent key escrow problem of identity-based cryptosystems and not to require certificates to guarantee the authenticity of public keys. A user's private key in a CL-PKC is not generated by the Key Generation Center (KGC) alone. Instead, it is a combination of some contribution of the KGC and some user's chosen secret, in such a way that

접수일(2009년 4월 16일), 게재확정일(2009년 10월 20일)

* 이 논문은 2008년 정부(교육과학기술부)의 재원으로 학술연구재단의 지원을 받아 수행된 연구임. (저자[1]-2단계 BK21 지원사업, 저자[1,2]-KRF-2008-313-C00118)

† 주저자, juheelee@ewhain.net
‡ 교신저자, kashim@nims.re.kr

the key escrow problem can be solved. Some additional user's public-key needs to be certified by any trusted authority and CL-PKC schemes are not purely ID-based. Al-Riyami and Paterson proposed a certificateless public-key signature (CLS) but they didn't formalize a security model for unforgeability. However, their CLS scheme was recently found vulnerable to a key replacement attack by Huang et al.[8]. Since Al-Riyami and Paterson's CLS scheme, several CLS schemes have been proposed[4,5,9]. They provided only informal analysis and were subsequently found to be vulnerable to key replacement attacks by type I adversaries[2]. Later, proven secure CLS schemes in the random oracle model[3,8,14] have been proposed. Recently, Liu et al.[10] proposed a provably secure CLS scheme in the standard model. In addition to these direct constructions, there exist a generic construction that converts existing signature schemes in different infrastructures into CLS schemes. Yum and Lee[13] proposed a generic construction for CLS schemes by combining any standard signature (SS) scheme with any ID-based signature (IBS) scheme. Subsequently, Hu et al.[7] showed that this construction is insecure against key replacement attacks and then proposed its improved version by modifying the input of signing algorithm. In particular Hu et al.[7] established a simplified definition and formal security model for CLS schemes which are shown to be more versatile than the previous ones[8]. Recently, Au et al.[2] suggested a malicious-but-passive KGC attack where a KGC may not generate master public/secret key pair honestly to mount the attack, they then modified Hu et al.'s model for capturing the attack. They also showed that Al-Riyami and Paterson's scheme and its variants [2,7,9] are insecure against the malicious-but-passive KGC attacks and the security of the CLS scheme converted from the modified Yum-Lee's construction is preserved in their new model.

Recently, Guo et al.[6] and Wang et al.[12] proposed new efficient CLS schemes based on Li et al.'s scheme[9]. Guo et al. proved its security against a type I adversary and a type II adversary in the random oracle model under the q-th Strong Diffie-Hellman assumption and the Computational Diffie-Hellman assumption, respectively, while Wang et al. didn't provide its formal security proof. In this paper, we show that two CLS schemes are insecure against key replacement attacks by a type I adversary.

The remainder of this paper is organized as follows. In Section 2, we review Wang et al.'s and Guo et al.'s CLS schemes. In Section 3, we present key replacement attacks on the schemes. Concluding remarks are given in Section 4.

II. Review of Two CLS Schemes

We first review Wang et al.'s and Gu et al.'s CLS schemes that follow Al-Riyami and Paterson's definition[1].

■ Wang et al.'s CLS Scheme

Setup. Given a security parameter k, the algorithm works as follows :

1. Run a generator to output descriptions of G_1 and G_2 of prime order q and a bilinear pairing $e : G_1 \times G_1 \to G_2$.
2. Choose an arbitrary generator $P \in G_1$.
3. Choose a random $s \in_R Z_q^*$, set $P_{pub} = sP$, and compute $g = e(P, P)$, where s is a master secret.
4. Choose cryptographic hash functions $H_1 : \{0,1\}^* \to Z_q^*$ and $H_{2:} \{0,1\}^* \times G_2 \to Z_q^*$.
5. The system parameters are

$$params = < G_1, G_{2,} e, q, P, P_{pub}, g, H_{1,} H_2 > .$$

Partial-Private-Key-Extract. This algorithm takes as input a security parameter k, the system parameters $params$, the master secret s and a user A's identity ID_A, and returns a partial private key corresponding to ID_A. It adopts the blind technique to remove a confidential and authentic channel between A and the KGC.

1. The user A chooses a value $k \in_R Z_q^*$, computes

kP and then sends $<ID_A, kP>$ to the KGC.

2. After receiving the message, the KGC checks that A has a claim to a particular online identifier ID_A. If it does, the KGC computes
$$D'_{ID_A} = [H_1(ID_A)+s]^{-1}P + s(kP),$$
and then sends it to A through an open channel.
3. On the receipt of D'_{ID_A}, A computes a partial private key D_{ID_A} as
$$D_{ID_A} = D'_{ID_A} - k(sP) = [H_1(ID_A)+s]^{-1}P.$$
Notice that A can verify the correctness of the output of the Partial-Private- Key-Extract algorithm by checking that
$$e(D_{ID_A},\ H_1(ID_A)P + P_{pub}) = g.$$

Set-Secret-Value. This algorithm takes as input the system parameters $params$ and an identity ID_A, and returns a secret value x_A corresponding to ID_A for a random $x_A \in_R Z_q^*$.

Set-Private-Key. This algorithm takes as input the system parameters $params$, a partial private key D_{ID_A} and a secret value x_A , and returns a (full) private key SK_{ID_A} as
$$SK_{ID_A} = x_A D_{ID_A} = x_A[H_1(ID_A)+s]^{-1}P.$$

Set-Public-Key. This algorithm takes as input the system parameters $params$, an identity ID_A, a secret value x_A and outputs a public key $PK_{ID_A} = < X_A, Y_A >$ corresponding to ID_A, where $X_A = x_A^{-1}P$ and $Y_A = x_A^{-1}P_{pub}$.

Sign. Given a message $m \in \{0,1\}^*$ and a private key SK_{ID_A},

1. Choose $a \in_R Z_q^*$, and compute $r = g^a \in G_2$ and $v = H_2(m \| r) \in Z_q^*$.
2. Compute $U = (a+v)\cdot SK_{ID_A} \in G_1$. Then $\sigma = (U, v)$ is a signature on m for $\{ID_A,\ < X_A, Y_A >\}$.

Verify. To verify a signature $\sigma = (U,\ v)$ on a message m for $\{ID_A,\ < X_A, Y_A >\}$,

1. Check whether the equality $e(X_A, P_{pub}) = e(Y_A, P)$ holds or not. If it holds, compute
$$r = e(U,\ H_1(ID_A)X_A + Y_A)\cdot g^{-v}.$$
2. Check whether the equality $v = H_2(m\|r)$ holds or not. If it holds, accept the signature.

■ Guo et al.'s CLS Scheme

Algorithms in Guo et al.'s scheme except the following three algorithms are the same as those in Wang et al.'s scheme.

Set-Partial-Private-Key. Given a security parameter k, the master secret s and an identity ID_A, output $D_{ID_A} = [H_1(ID_A)+s]^{-1}P$ as a partial-private-key correspond to ID_A.

Set-Private-Key. Given a partial private Key D_{ID_A}, an identity ID_A and a secret value x_A, output $SK_{ID_A} = x_A^{-1}D_{ID_A} = [x_A(H_1(ID_A)+s)]^{-1}P$ as a (full) private key correspond to ID_A.

Set-Public-Key. Given an identity ID_A and a secret value x_A, compute $X_A = x_A P$, $Y_A = x_A P_{pub}$ and set $PK_{ID_A} = < X_A, Y_A >$.

The main difference of Wang et al.'s scheme from Guo et al.'s scheme is to use the blind technique for eliminating a secure channel between the signer and the KGC in Partial-Private-key-Extract stage.

III. Key Replacement Attacks on the Two CLS Schemes

Now, we present key replacement attacks on the two CLS schemes described in the previous section. In CLS schemes, there exist two types of adversaries with the following capabilities;

- **Type I** adversary A_I as a third party is not allowed to access to the master secret but A_I may replace user public keys of its choices.
- **Type II** adversary A_{II} as a malicious KGC is allowed to access to the master secret but not replace user public keys.

Now, we show that the two CLS schemes are insecure against key replacement attacks by a type I adversary.

■ Key Replacement Attack on Wang et al.'s Scheme

Suppose that a type I adversary A_I wants to forge a certificateless signature of Wang et al.'s scheme. We assume that A_I has obtained a certificateless signature $\sigma = (U, v)$ on m for $\{ID_A, PK_{ID_A}\}$ where $PK_{ID_A} =< X_A, Y_A >$, $U = (a+v) \cdot SK_{ID_A}$ and $v = H_2(m \| r)$. Then A_I can forge $\sigma' = (U', v')$ on the same message m for another public key pair $PK'_{ID_A} =< X_A', Y_A' >$, corresponding to ID_A as follows:

- A_I selects a random $t \in_R Z_q^*$ and computes a new public key pair being replaced as $X_A' = t^{-1} X_A = t^{-1} x_A^{-1} P$ and
  $Y_A' = t^{-1} Y_A = t^{-1} x_A^{-1} P_{pub}$.
- Next, A_I computes $U' = tU$ and sets $v' = v$. Then $\sigma' = (U', v')$ is a valid signature on m for $\{ID_A, PK'_{ID_A}\}$ since it satisfies the verification equations as follow;

$$e(X_A', P_{pub}) = e(t^{-1} X_A, sP) = e(t^{-1} s X_A, P)$$
$$= e(t^{-1} Y_A, P) \ = e(Y_A', P)$$

and $v = H_2(m \| r')$ since

$$r' = e(U', \ H_1(ID_A) X_A' + Y_A') \cdot g^{-v'}$$
$$= e(U, \ \ H_1(ID_A) X_A + Y_A) \cdot g^{-v}$$

i.e., $U' = \ t\,U = \ t(a+v) \cdot SK_{ID_A}$
$= (a+v)t \cdot SK_{ID_A} = (a+v) \cdot SK'_{ID_A}$

where $SK'_{ID_A} = t \cdot SK_{ID_A}$and SK'_{ID_A} is a valid private key of ID_A corresponding to the replaced public key $PK'_{ID_A} =< X_A', \ Y_A' >$.

This result shows that it is insecure against a type I adversary since the adversary can forge a user's certificateless signature under the replaced public key. The same attack can be applied to Li et al.'s[9] and to Guo et al.'s[6] CLS schemes since they use the same signing method as Wang et al.'s one.

IV. Conclusion

We presented the key replacement attacks on Wang et al. and Guo et al.'s CLS schemes. Their weakness against the attacks are due to the lack of binding technique between messages and user public keys being signed. These attacks can be prevented by adding a user public key PK_{ID} together with m to the input of the hash function, i.e., $h = H(m \| r \| PK_{ID})$ as described in [13].

REFERENCES

[1] S. Al-Riyami and K. Paterson, "Certificateless public key cryptogaphy," Advances in Cryptology, ASIACRYPT 2003, LNCS 2894, pp. 452-473, 2003.

[2] M.H. Au, Y. Mu, D.S. Wong, J.K. Liu, J. Chen, and G. Yang, "Malicious KGC attack in certificateless cryptography," ACM Symposium on Information, Computer and Communications Security, ASIACCS 2007, pp. 302-311, Mar. 2007.

[3] K.Y. Choi, J.H. Park, J.K. Hwang, and D.H. Lee, "Efficient certificateless signature schemes," International Conference on Applied Cryptography and Network Security, ACNS 2007, LNCS 4521, pp. 443-458, 2007.

[4] M. Gorantla, R. Gangishetti, M. Das, and A. Saxena, "An effective certificateless signature scheme based on bilinear pairings," International Workshop on Security in Information Systems, WOSIS 2005, pp. 31-39, May 2005.

[5] M. Gorantla and A. Saxena, "An efficient certificateless signature scheme," International Conference on Computational Intelligence and

Security, CIS 2005, LNCS 3802, pp. 110-116, 2005.

[6] L. Guo, L. Hu, and Y. Li, “A practical certificateless signature scheme,” International Symposium on Data, Privacy, and E-Commerce, IEEE ISDPE 2007, pp. 248-253, Jan. 2007.

[7] B. Hu, D. Wong, Z. Zhang, and X. Deng, “Key replacement attack against a generic construction of certificateless signature,” Australasian Conference on Information Security and Privacy, ACISP 2006, LNCS 4058, pp. 235-246, 2006.

[8] X. Huang, W. Susilo, Y. Mu, and F. Zhang, “On the security of certificateless signature scheme from ASIACRYPT 03,” International Conference on Cryptology and Network Security, CANS 2005, LNCS 3810, pp. 13-25, 2005.

[9] X. Li, K. Chen, and L. Sun, “Certificateless signature and proxy signature schemes from bilinear pairings,” Lithuanian Mathematical Journal, vol. 45, no. 1, pp. 95-103, Jan. 2005.

[10] J.K. Liu, M.H. Au, and W. Susilo, “Self-generated-certificate public key cryptography and certificateless signature/encryption scheme in the standard model,” ACM Symposium on Information, Computer and Communications Security, ASIACCS 2007, pp. 273-283, Mar. 2007.

[11] A. Shamir, “Identity-base cryptosystems and signature schemes,” Advances in Cryptology, CRYPTO 84, LNCS 196, pp. 47-53, 1985.

[12] C. Wang, H. Huang, and Y. Tang, “An efficient certificateless signature from pairings,” International Symposium on Data, Privacy, and E-Commerce, IEEE ISDPE 2007, pp. 236-238, Jan. 2007.

[13] D. Yum and P. Lee, “Generic construction of certificateless signature,” Australasian Conference on Information Security and Privacy, ACISP 2004, LNCS 3108, pp. 200-211, 2004.

[14] Z. Zhang, D.S. Wong, J. Xu, and D. Feng, “Certificateless public-key signature : security model and efficient construction,” International Conference on Applied Cryptography and Network Security, ACNS 2006, LNCS 3989, pp. 293-308, 2006.

<著者紹介>

이 주 희(Ju-Hee Lee) 학생회원
1996년 2월: 한남대학교 수학과 졸업
2002년 2월: 이화여자대학교 수학과 석사
2005년 3월 ~ 현재: 이화여자대학교 수학과 박사과정
<관심분야> 암호론, 정보보호

심 경 아 (Kyung-Ah Shim) 정회원
1992년 2월: 이화여자대학교 수학과 졸업
1994년 2월: 이화여자대학교 수학과 석사
1999년 2월: 이화여자대학교 수학과 박사
2000년 2월 ~ 2004년 2월: 한국정보보호진흥원 선임연구원
2004년 8월 ~ 2008년 8월: 이화여자대학교 수학과 연구교수
2008년 9월 ~ 현재: 국가수리과학연구소 선임연구원
<관심분야> 암호론, 정보보호

이 향 숙 (Hyang-Sook Lee) 정회원
1986년 2월: 이화여자대학교 수학과 졸업
1988년 2월: 이화여자대학교 수학과 석사
1993년 12월: Northwestern 대학 수학과 박사
1995년 3월 ~ 현재: 이화여자대학교 수학과 교수
<관심분야> 암호론, 정보보호