On the Security of a RSA-based Certificateless Signature Scheme

Debiao He [1], Muhammad Khurram Khan [2], and Shuhua Wu [3]
(Corresponding author: Debiao He)

School of Mathematics and Statistics, Wuhan University, Wuhan, China[1]
Center of Excellence in Information Assurance, King Saud University, Riyadh, Saudi Arabia[2]
Department of Networks Engineering, Information Engineering University, Zhengzhou, China[3]
(Email: hedebiao@163.com)

(Received Mar. 9, 2012; revised and accepted July 24, 2012)

Abstract

The certificatless cryptography has been studied widely since it could eliminate the need of certificates in the Public Key Infrastructure and solve the inherent key escrow problem in the identity-based cryptography. Recently, Zhang et al.'s proposed the first RSA-based certificateless signature scheme and demonstrated that their scheme is provably secure in the random oracle model. In this paper, we will show that Zhang et al.'s scheme is insecure against a type I adversary who can replace users' public keys. The analysis shows Zhang et al.'s scheme is not secure for practical applications.

Keywords: Cryptanalysis, certificateless cryptography, digital signature

1 Introduction

In traditional public key cryptography, a digital certificate, generated by a trusted third party, is needed to ensure the binding between the public key and the owner's identity. Then the system will face with the certificate management problem. To solve the problem, Shamir [9] proposed the identity-based (ID-based) cryptography. In the ID-based cryptography, the user's public key could be computed from his identity and the user's secret key is generated by the key generation centre (KGC). However, the ID-based cryptography suffers from the key escrow problem, i.e. the KGC knows all the user's secret keys. In 2003, Al-Riyami et al. [1] introduced the notation of the certificateless public key cryptography (CLPKC). In the CLPKC, a user's private key is a combination of a partial private key generated by the KGC and a secret key chosen by the user. Then the key escrow problem in the ID-based cryptography is solved.

Since the first certificateless signature (CLS) scheme proposed by Al-Riyami et al. [1], many CLS schemes [3-7, 10, 11, 14], based on the elliptic curve cryptography, have been proposed to improve performance and security. It is well known that RSA has been applied in the industry for decades and many companies have invested in expensive hardware or software implementations of RSA. To satisfy practical applications, Zhang et al. [15] proposed the first RSA-based CLS scheme. They also demonstrated that their scheme is provably secure in the random oracle model. However, we will show that Zhang et al.'s scheme is insecure against a type I adversary in this paper. That is, the type I adversary can forge a legal signature by replacing the user's public key with a new public key chosen by himself.

The rest of the paper is organized as follows. In Section 2, we review Zhang et al.'s CLS scheme. In Section 3, we show that Zhang et al.'s scheme is not secure against a type I adversary. Conclusions are given in Section 4.

2 Review of Zhang et al.'s CLS Scheme

Zhang et al.'s CLS scheme consists of the following seven polynomial-time algorithms.

Setup : Taking a security parameter k as input, the KGC generates a RSA group as follows.

1) KGC generates two random number p and q such as $\gcd(e,\varphi(n))=1$, where $n=pq$, e is KGC's public key and $\varphi(\cdot)$ is the Euler totient function.

2) KGC computes d such as $ed \equiv 1 \bmod \varphi(n)$.

3) KGC choose two crytographic hash functions $H_0 : \{0,1\}^* \to Z_n^*$ and $H_0 : Z_n^4 \times \{0,1\}^* \to \{0,1\}^l$.

4) KGC sets d as the master key msk and publishes the public parameters $params = \{n, e, H_0, H_1\}$.

$Partial-Key-Extract$: Taking a user with identity $ID \in \{0,1\}^*$ as input, KGC computes the partial key $d_{ID} \equiv H_0(ID)^{msk} \equiv H_0(ID)^d \bmod n$.

Set-Secret-Value: Taking *params* and an identity *ID* as inputs, the user randomly chooses x_{ID} and sets it as the secret value.

Set-Private-Key: Taking the partial private key d_{ID} and the secret value x_{ID} as inputs, the user sets the private key $SK_{ID} = \{x_{ID}, d_{ID}\}$.

Set-Public-Key: Taking the secret value x_{ID} of a user with identity ID, the user publishes his public key $PK_{ID} \equiv H_0(ID)^{x_{ID}} \bmod n$.

Sign: Taking a message m, *params* and , the private key $SK_{ID} = \{x_{ID}, d_{ID}\}$ as inputs, the user generates a signature as follows.

1) The user chooses two random numbers r_1 and r_2 and computes $R_1 \equiv H_0(ID)^{r_1} \bmod n$ and $R_2 \equiv H_0(ID)^{r_2} \bmod n$.

2) The user computes $h = H(R_1, R_2, ID, PK_{ID}, m)$, $u_1 \equiv d_{ID}^{r_1 - h} \equiv H_0(ID)^{d(r_1 - h)} \bmod n$ and $u_2 = r_2 - x_{ID} h$.

3) The user outputs $\delta = (u_1, u_2, h)$ as the signature of the message m.

Verify: Taking a signature $\delta = (u_1, u_2, h)$ on message m, *params* and , the public key PK_{ID} as inputs, a verifier executes as follows:

1) The verifier computes $R_1' \equiv u_1^e H_0(ID)^h \bmod n$ and $R_2' \equiv H_0(ID)^{u_2} PK_{ID}^h \bmod n$.

2) The verifier checks whether h and $H(R_1', R_2', ID, PK_{ID}, m)$ are equal. If they are equal, the verifier accepts the signature. Otherwise, he will reject the signature.

3 Cryptanalysis of Zhang et al.'s CLS Scheme

There are two types of adversary in CLS schemes [15]. The Type I attack is not allowed to access to the master-key but it is able to replace the user's public key at will. The Type II attacker represents a malicious KGC, which knows all users' partial private keys but it is not able to replace the user's public key. Zhang et al. [15] claimed their scheme could withstand both of the two adversaries. Inspired by Wang et al.'s work [12], we will show that the Zhang et al.'s CLS scheme is universally forgeable by the type I adversary, i.e., the adversary can forge a user's signature on any message at any time.

Let $\mathcal{A}$**1** be a type I adversary. He could forge a legal signature of the message m through the following steps.

1) $\mathcal{A}$**1** chooses a random number x_{ID}' and replaces the user public key PK_{ID} with $PK_{ID}' \equiv H_0(ID)^{x_{ID}'} \bmod n$.

2) $\mathcal{A}$**1** generates a random numbers r_1 and computes $R_1 \equiv H_0(ID)^{r_1} \bmod n$.

3) $\mathcal{A}$**1** generates a number r_2 and computes $R_2 \equiv H_0(ID)^{r_2} \bmod n$.

4) $\mathcal{A}$**1** computes $h = H(R_1, R_2, ID, PK_{ID}', m)$ and checks whether $r_1 - h$ is divisible by e. If $r_1 - h$ is not divisible by e, $\mathcal{A}$**1** repeats 2) and 3).

5) $\mathcal{A}$**1** computes $r_1 - h = e \cdot b$ and $u_1 \equiv H_0(ID)^b \bmod n$.

6) $\mathcal{A}$**1** outputs $\delta = (u_1, u_2, h)$ as the signature of the message m.

Since $u_1 \equiv H_0(ID)^b \bmod n$, $u_2 = r_2 - x_{ID}' h$, $h = H(R_1, R_2, ID, PK_{ID}', m)$ and $r_1 - h = e \cdot b$, then we have

$$\begin{aligned} R_1' &\equiv u_1^e H_0(ID)^h \equiv H_0(ID)^{be} H_0(ID)^h \\ &\equiv H_0(ID)^{r_1 - h} H_0(ID)^h \equiv H_0(ID)^{r_1} \equiv R_1 \bmod n \end{aligned} \quad (1)$$

$$\begin{aligned} R_2' &\equiv H_0(ID)^{u_2} PK_{ID}'^h \\ &\equiv H_0(ID)^{r_2 - x_{ID}' h} H_0(ID)^{x_{ID}' h} \bmod n \\ &\equiv H_0(ID)^{r_2} \equiv R_2 \bmod n \end{aligned} \quad (2)$$

and

$$h = H(R_1', R_2', ID, PK_{ID}', m) \quad (3)$$

So $\delta = (u_1, u_2, h)$ could pass the verification of the verifier and $\mathcal{A}$**1** could forge a legal signature.

Since r_1 is a random number and the output of hash function h can be treated as random number, then $e \mid r_1 - h$ holds with probability about $\frac{1}{e}$. $\mathcal{A}$**1** will succeed at rate about $\frac{1}{e}$ for very r_1. Consequently, the above attack can succeed once by trying about three values of r_1 on average if $e = 3$. Even if e is as large as 65537 ($2^{16} + 1$), trying 65537 times to get a successful attack seems not an issue for attacker $\mathcal{A}$**1**. It is well known that some security standards (e.g. PKCS #1 [8]), academic papers (e.g. [2]) and popular web sites ((e.g. wikipedia [15])) suggest that e can be set as 3 or 65537. Besides, the security analysis given in [13] does not excludes the case of small e. Then our attack is valid for practical applications.

4 Conclusion

Recently, Zhang et al. [15] proposed a RSA-based CLS scheme and proved that it is secure in the random oracle

model. However, in this paper, we have demonstrated that their scheme is insecure against the Type I adversary.

Acknowledgments

The authors thank Prof. Min-Shiang Hwang and the anonymous reviewers for their valuable comments. This research was supported by the Specialized Research Fund for the Doctoral Program of Higher Education of China (No. 20110141120003), the National Natural Science Foundation of China (No. 61101112), and the Postdoctoral Science Foundation of China (No. 2011M500775).

References

[1] S. Al-Riyami and K. Paterson, "Certificateless public key cryptography," in *Proceedings of Asiacrypt '03*, pp. 452–473, 2003.

[2] D. Boneh, "Twenty years of attacks on the RSA cryptosystem," *Notices of the American Mathematical Society*, vol. 46, no. 2, pp. 203-213, 1999.

[3] K. Y. Choi, J. H. Park, and D. H. Lee, "A new provably secure certificateless short signature scheme," *Computers and Mathematics with Applications*, vol. 61, no. 7, pp. 1760-1768, 2011.

[4] H. Du and Q. Wen, "Efficient and provably-secure certificateless short signature scheme from bilinear pairings," *Computer Standards and Interfaces*, vol. 31, no. 2, pp. 390−394, 2009.

[5] D. He, J. Chen, and R. Zhang, "An efficient and provably-secure certificateless signature scheme without bilinear pairings," *International Journal of Communication Systems*, vol. 25, no. 11, pp. 1432-1442, DOI: 10.1002/dac.1330, 2011.

[6] X. Huang, Y. Mu, W. Susilo, D. Wong, and W. Wu, "Certificateless signature revisited," in *ACISP 2007*, pp. 308−322, 2007.

[7] C. Ma and J. Ao, "Certificateless group oriented signature secure against key replacement attack," *International Journal of Network Security*, vol. 12, no. 1, pp. 1-6, 2011.

[8] PKCS, Public key cryptography standards, PKCS #1 v2.1, RSA Cryptography Standard, Draft 2, 2001. (http://www.rsasecurity.com/rsalabs/pkcs/)

[9] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proceedings of Crypto '84*, pp. 47-53, 1985.

[10] R. Tso, X. Yi, and X. Huang, "Efficient and short certificateless signature," in *CANS 2008*, pp. 64-79, 2008.

[11] R. Tso, X. Yi, and X. Huang, "Efficient and short certificateless signatures secure against realistic adversaries," *Journal of Supercomputing*, vol. 55, no. 2, pp. 173-191, 2011.

[12] G. Wang, J. Yu, and Q. Xie, *Security Analysis of A Single Sign-On Mechanism for Distributed Computer Networks*. (http://eprint.iacr.org/2012/108.pdf)

[13] Wikipedia, *RSA (algorithm)*. (http://en.wikipedia.org/wiki/RSA_(algorithm))

[14] H. Xiong, Z. Qin, and F. Li, "A certificateless proxy ring signature scheme with provable security," *International Journal of Network Security*, vol. 12, no. 2, pp. 92-106, 2011.

[15] J. Zhang and J. Mao, "An efficient RSA-based certificateless signature scheme," *Journal of Systems and Software*, vol. 85, pp. 638-642, 2012.

Debiao He received his Ph.D. degree in applied mathematics from School of Mathematics and Statistics, Wuhan University in 2009. He is currently a lecturer of Wuhan University. His main research interests include cryptography and information security, in particular, cryptographic protocols.

Muhammad Khurram Khan received his Ph.D. degree from Southwest Jiaotong University, Chengdu, PR China in 2006. He is currently working as a research assistant professor at King Saud University, Kingdom of Saudi Arabia. He is the founding editor of Bahria University Journal of Information & Communication Technology. He has published more than 130 research papers in the journals and conferences of international repute. His areas of interest are biometrics, information security, multimedia security, and digital data hiding.

Shuhua Wu is a lectuer of Networks Engineering Department, Information Engineering University, Zhengzhou, China. Currently, he is a postdoctor at the Department of Computer Science and Engineering, Shanghai Jiaotong University. His research interests include cryptology and communication protocols.