Hindawi Publishing Corporation
Journal of Applied Mathematics
Volume 2012, Article ID 508981, 6 pages
doi:10.1155/2012/508981

Research Article

Attacks on One Designated Verifier Proxy Signature Scheme

Baoyuan Kang

Computer Science and Software Institution, Tianjin Polytechnic University, 399 Binshuixi road, Tianjin 300387, China

Correspondence should be addressed to Baoyuan Kang, baoyuankang@yahoo.com.cn

Received 5 April 2012; Accepted 5 June 2012

Academic Editor: Debasish Roy

In a designated verifier proxy signature scheme, there are three participants, namely, the original signer, the proxy signer, and the designated verifier. The original signer delegates his or her signing right to the proxy signer, then the proxy signer can generate valid signature on behalf of the original signer. But only the designated verifier can verify the proxy signature. Several designated verifier proxy signature schemes have been proposed. However, most of them were proven secure in the random oracle model, which has received a lot of criticism since the security proofs in the random oracle model are not sound with respect to the standard model. Recently, by employing Water's hashing technique, Yu et al. proposed a new construction of designated verifier proxy signature. They claimed that the new construction is the first designated verifier proxy signature, whose security does not rely on the random oracles. But, in this paper, we will show some attacks on Yu et al.'s scheme. So, their scheme is not secure.

1. Introduction

The concept of proxy signature was first introduced by Mambo et al. [1] in 1996. Proxy signature is very useful when a user, called an original signer, wants to delegate his or her signing rights to the other user, called a proxy signer. In a proxy signature scheme, the proxy signer can generate a valid signature on behalf of the original signer. Anyone can verify the authenticity of the purported signature by using the public keys of the original signer and proxy signer. But, when a verifier receives a proxy signature, he should not only verify the correctness by a given verification procedure, but also be convinced of the original signer' agreement on the signed message. Proxy signature schemes have been suggested for use in a number of applications, including electronic commerce, e-cash, and distributed shared object systems.

Unlike standard signature, In order to protect signature privacy, Jakobsson et al. [2] introduced a new primitive named designated verifier proofs in 1996. Such a proof enables

a prover convince a designated verifier that a statement is true, while the designated verifier cannot use the proof to convince others of this fact, since the designated verifier himself can simulate such a proof. Furthermore, Jakobsson et al. proposed a designated verifier signature scheme in the sense that only the designated verifier can be convinced that a signature is produced by the claimed signer. Jakobsson et al. also discussed a stronger concept called strong designated verifier signature in the same paper.

In 2003, based on the concepts of proxy signatures and designated verifier signatures, Dai et al. [3] consider a scenario where the proxy signer wishes to protect his signing privilege from knowing by other parties. In other words, the proxy signer only wants to convince the designated receiver that he has signed the specific message. They proposed such a scheme called designated verifier proxy signature, which provides authentication of a message without providing a nonrepudiation property of traditional digital signature. A designated verifier proxy signature scheme can be used to convince the designated verifier and only the designated verifier whether a signature is valid or not. This is due to the fact that the designated verifier can always generate a valid signature intended for himself that is indistinguishable from an original signature. This kind of signature is useful in electronic commerce applications. Unfortunately, Wang [4] pointed out there exists a forgery attack in Dai et al.'s scheme. Huang et al. [5] proposed a short designated verifier proxy signature from pairings to improve the communication efficiency. Lu and cao [6] proposed a designated verifier proxy signature with message recovery in 2005. Zhang and Mao [7] proposed a novel ID-based designated verifier proxy signature scheme. Although several designated verifier proxy signature schemes have been proposed. However, most of them were proven secure in the random oracle model, which has received a lot of criticism since the security proofs in the random oracle model are not sound with respect to the standard model. Recently, by employing Water's hashing technique [8], Yu et al. [9] proposed a new construction of designated verifier proxy signature scheme. They claimed that the new construction is the first designated verifier proxy signature scheme, whose security does not rely on the random oracles. But in this paper, we will show some attacks on their scheme. So, their scheme is not secure.

The paper is organized as follows. In the next section, we will review Yu et al.'s designated verifier proxy signature scheme. The attacks on Yu et al.'s scheme are presented in Section 3. Finally, Section 4 concludes the paper.

2. Review of Yu et al.'s Designated Verifier Proxy Signature Scheme

In this section, we review the designated verifier proxy signature scheme proposed by Yu et al.. There are three participants in Yu et al.'s scheme, namely, Alice, Bob, and Cindy, who act as the original signer, the proxy signer, and the designated verifier, respectively. Yu et al.'s scheme consists of the following algorithms.

2.1. Setup

The system parameters are as follows. Let (G, G_T) be bilinear groups, where $|G| = |G_T| = p$ for some prime, g is a generator of G. e denotes an admissible pairing $G \times G \rightarrow G_T$. Pick $u', m' \in G$ and vectors $\vec{u} = (u_i), \vec{m} = (m_i)$ of length n, whose entries are random elements from G. The public parameters are (G, G_T, e, u', m', $\vec{u}$, $\vec{m}$).

2.2. Keygen

Alice picks randomly $x_a, y_a \in Z_p^*$ and sets her secret key $k_a = (x_a, y_a)$. Then she computes her public key:

$$pk_a = (pk_{ax}, pk_{ay}) = (g^{x_a}, g^{y_a}). \tag{2.1}$$

Similarly, Bob's secret key is $sk_b = (x_b, y_b)$, and the public key is

$$pk_b = (pk_{bx}, pk_{by}) = (g^{x_b}, g^{y_b}). \tag{2.2}$$

Cindy's secret key is $sk_c = (x_c, y_c)$, and the public key is

$$pk_c = (pk_{cx}, pk_{cy}) = (g^{x_c}, g^{y_c}). \tag{2.3}$$

2.3. DelegationGen

Let W be an n-bit message called warrant to be signed by the original signer and W_i denotes the i-bit of, and let $w \subseteq \{1, 2, \ldots, n\}$ be the set of all i for which $W_i = 1$. The original signer picks a random $r_a \in Z_p$ and computes the delegation $\sigma_\omega = (\sigma_{\omega_1}, \sigma_{\omega_2})$ and sends it to the proxy signer Bob, where

$$\begin{aligned} \sigma_{\omega_1} &= g^{x_a y_a} \left(u' \prod_{i \in w} u_i \right)^{r_a}, \\ \sigma_{\omega_2} &= g^{r_a}. \end{aligned} \tag{2.4}$$

2.4. ProxySign

Let M be an n-bit message to be signed by the proxy signer Bob and M_i denotes the i-bit of, and let $m \subseteq \{1, 2, \ldots, n\}$ be the set of all i for which $M_i = 1$. The proxy signature is generated as follows. First, the proxy signer Bob picks two random values $r'_a, r_b \in Z_p$. Then the proxy signature $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ on M is constructed as

$$\begin{aligned} \sigma_1 &= e\left(\sigma_{\omega_1} \left(u' \sum_{i \in w} u_i \right)^{r'_a} g^{x_b y_a} \left(m' \prod_{i \in m} m_i \right)^{r_b}, pk_{c_x} \right), \\ \sigma_2 &= \sigma_{\omega_2} g^{r'_a}, \\ \sigma_3 &= g^{r_b}. \end{aligned} \tag{2.5}$$

2.5. Verification

To check whether $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ is a valid proxy signature on the message M under the warrant, Cindy uses her secret key to verify whether the following equation holds:

$$\begin{aligned}\sigma_1 = {} & e(pk_{ax}, pk_{ay})^{x_c} e(pk_{bx}, pk_{by})^{x_c} \\ & \cdot e\left(u' \sum_{i \in w} u_i, \sigma_2\right)^{x_c} e\left(m' \prod_{i \in m} m_i, \sigma_3\right)^{x_c}.\end{aligned} \tag{2.6}$$

2.6. Transcript Simulation

Cindy can use her private key to compute a signature on an arbitrary message M^* with the warrant W^*. She picks two random values $r_1, r_2 \in Z_p^*$ and computes $\sigma^* = (\sigma_1^*, \sigma_2^*, \sigma_3^*)$, where

$$\begin{aligned}\sigma_2^* &= g^{r_1}, \\ \sigma_3^* &= g^{r_2}, \\ \sigma_1^* &= e(pk_{ax}, pk_{ay})^{x_c} e(pk_{bx}, pk_{by})^{x_c} \\ &\quad \cdot e\left(u' \sum_{i \in w^*} u_i, {\sigma_2}^*\right)^{x_c} e\left(m' \prod_{i \in m^*} m_i, {\sigma_3}^*\right)^{x_c}.\end{aligned} \tag{2.7}$$

3. Attacks on Yu et al.'s Designated Verifier Proxy Signature Scheme

In this section, we will give some attacks on Yu et al.'s designated verifier proxy signature scheme.

3.1. Attack 1

On receiving the delegation $\sigma_\omega = (\sigma_{\omega_1}, \sigma_{\omega_2})$ and the warrant, the attacker randomly selects $r_a^* \in Z_p$ and alters the delegation as $\sigma_\omega^* = (\sigma_{\omega_1}^*, \sigma_{\omega_2}^*)$, where

$${\sigma_{\omega_1}}^* = \sigma_{\omega_1} \left(u' \prod_{i \in w} u_i\right)^{r_a^*}, \tag{3.1}$$

$$\sigma_{\omega_2}^* = \sigma_{\omega_2} g^{r_a^*}. \tag{3.2}$$

3.2. Attack 2

On receiving the proxy signature $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ on one message M, everybody can forge another valid proxy signature $\sigma^* = (\sigma_1^*, \sigma_2^*, \sigma_3^*)$ on M as follows:

$$\begin{aligned} \sigma_1{}^* &= \sigma_1 \cdot e\left(\left(m' \prod_{i \in m} m_i\right)^{r_b^*}, pk_{cx}\right), \\ \sigma_2^* &= \sigma_2, \\ \sigma_3^* &= \sigma_3 g^{r_b^*} \end{aligned} \tag{3.3}$$

$r_b^* \in Z_p$ is a random number.

In fact, because $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ is valid proxy signature, the following verification equation holds:

$$\begin{aligned} \sigma_1 = {} & e(pk_{ax}, pk_{ay})^{x_c} e(pk_{bx}, pk_{by})^{x_c} \\ & \cdot e\left(u' \sum_{i \in w} u_i, \sigma_2\right)^{x_c} e\left(m' \prod_{i \in m} m_i, \sigma_3\right)^{x_c}. \end{aligned} \tag{3.4}$$

Then,

$$\begin{aligned} \sigma_1^* &= \sigma_1 \cdot e\left(\left(m' \prod_{i \in m} m_i\right)^{r_b^*}, pk_{c_x}\right) \\ &= e(pk_{ax}, pk_{ay})^{x_c} e(pk_{bx}, pk_{by})^{x_c} \cdot e\left(u' \sum_{i \in w} u_i, \sigma_2\right)^{x_c} e\left(m' \prod_{i \in m} m_i, \sigma_3\right)^{x_c} \\ &\quad \cdot e\left(\left(m' \prod_{i \in m} m_i\right)^{r_b^*}, pk_{c_x}\right) \\ &= e(pk_{ax}, pk_{ay})^{x_c} e(pk_{bx}, pk_{by})^{x_c} \\ &\quad \cdot e\left(u' \sum_{i \in w} u_i, \sigma_2\right)^{x_c} e\left(m' \prod_{i \in m} m_i, \sigma_3\right)^{x_c} \cdot e\left(m' \prod_{i \in m} m_i, g^{r_b^*}\right)^{x_c} \\ &= e(pk_{ax}, pk_{ay})^{x_c} e(pk_{bx}, pk_{by})^{x_c} \\ &\quad \cdot e\left(u' \sum_{i \in w} u_i, \sigma_2\right)^{x_c} e\left(m' \prod_{i \in m} m_i, \sigma_3 g^{r_b^*}\right)^{x_c} \\ &= e(pk_{ax}, pk_{ay})^{x_c} e(pk_{bx}, pk_{by})^{x_c} \\ &\quad \cdot e\left(u' \sum_{i \in w} u_i, \sigma_2\right)^{x_c} e\left(m' \prod_{i \in m} m_i, \sigma_3^*\right)^{x_c}. \end{aligned} \tag{3.5}$$

So, $\sigma^* = (\sigma_1^*, \sigma_2^*, \sigma_3^*)$ is a valid proxy signature on M.

3.3. Attack 3

Anyone who gets $g^{x_a y_a}$ can personate the original signer to delegate signing rights of the original signer. On the other hand, in some scenarios the original signer may reveal $g^{x_a y_a}$ without revealing his private key (x_a, y_a) to make confusion about the delegation of signing rights on purpose.

3.4. Attack 4

Similarly, anyone who gets $g^{x_b y_b}$ can personate the proxy signer to generate proxy signatures. On the other hand, in some scenarios the proxy signer may reveal $g^{x_b y_b}$ without revealing his private key (x_b, y_b) to make confusion about the production of proxy signatures on purpose.

4. Conclusion

A designated verifier proxy signature scheme can be used to convince the designated verifier and only the designated verifier whether a signature is valid or not. This is due to the fact that the designated verifier can always generate a valid signature intended for him that is indistinguishable from an original signature. This kind of signature is useful in electronic commerce applications. Recently, Yu et al. proposed a new construction of designated verifier proxy signature scheme. As for the security, they classified the potential adversaries into three kinds according to their attack power and proved that their scheme is unforgeable against all kinds of adversaries in the standard model. But, in this paper, we show some attacks on their scheme. So, their scheme is not secure.

References

[1] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures: delegation of the power to sign messages," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E79-A, no. 9, pp. 1338–1353, 1996.

[2] M. Jakobsson, K. Sako, and R. Impagliazzo, "Designated verifier proofs and their applications," in *Proceedings of the 15th Annual International Conference on Theory and Application of Cryptographic Techniques (EUROCRYPT '96)*, vol. 1070 of *Lecture Notes in Computer Science*, pp. 143–154, May 1996.

[3] J. Z. Dai, X. H. Yang, and J. X. Dong, "Designated-receiver proxy signature scheme for electronic commerce," in *Proceedings of IEEE International Conference on Systems, Man and Cybernetics*, vol. 1, pp. 384–389, IEEE Press, October 2003.

[4] G. Wang, "Designated-verifier proxy signatures for e-commerce," in *Proceedings of IEEE International Conference on Multimedia and Expo (ICME '04)*, vol. 3, pp. 1731–1734, IEEE Press, June 2004.

[5] X. Huang, Y. Mu, W. Susilo, and F. Zhang, "Short designated verifier proxy signature from pairings," in *Proceedings of the International Conference on Embedded and Ubiquitous Computing Workshops (EUC '05)*, vol. 3823 of *Lecture Notes in Computer Science*, pp. 835–844, December 2005.

[6] R. X. Lu and Z. F. Cao, "Designated verifier proxy signature scheme with message recovery," *Applied Mathematics and Computation*, vol. 169, no. 2, pp. 1237–1246, 2005.

[7] J. Zhang and J. Mao, "A novel ID-based designated verifier signature scheme," *Information Sciences*, vol. 178, no. 3, pp. 766–773, 2008.

[8] B. Waters, "Efficient identity-based encryption without random oracles," in *Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques: Advances in Cryptology (EUROCRYPT '05)*, vol. 3494 of *Lecture Notes in Computer Science*, pp. 114–127, Springer, Berlin, Germany, May 2005.

[9] Y. Yu, C. Xu, X. Zhang, and Y. Liao, "Designated verifier proxy signature scheme without random oracles," *Computers and Mathematics with Applications*, vol. 57, no. 8, pp. 1352–1364, 2009.