Available online at www.sciencedirect.com
ScienceDirect
Computer Standards & Interfaces 31 (2009) 258–260
COMPUTER STANDARDS & INTERFACES
www.elsevier.com/locate/csi

Comment on Saeednia et al.'s strong designated verifier signature scheme

Ji-Seon Lee*, Jik Hyun Chang

Department of Computer Science, Sogang University, Sinsu-Dong, Mapo-Gu, Seoul 121-742, Republic of Korea

Received 18 June 2007; received in revised form 10 January 2008; accepted 24 February 2008
Available online 6 March 2008

Abstract

In 1996, Jakobsson et al. proposed a designated verifier signature scheme in which only one specified person, called a designated verifier, can be convinced of the validity of the signature and the identity of the signer. This is possible by giving the designated verifier the ability to simulate a signature him/herself in an indistinguishable way. Therefore, the other third party cannot determine whether the signature is from the signer or the designated verifier. However, in some circumstances, the third party may be convinced that a signature intended for the designated verifier is actually generated by the signer.

In 2003, Saeednia et al. proposed a strong designated verifier signature scheme to overcome this problem. However, we found that Saeednia et al.'s scheme would reveal the identity of the signer if the secret key of this signer is compromised. In this paper, we provide a new strong designated verifier signature scheme that provides signer ambiguity, even if the secret key of the signer is compromised. We also analyze the proposed scheme.

Keywords: Strong designated verifier signatures; Signer ambiguity; Key compromise

1. Introduction

Digital signature schemes are used to provide security services such as user authentication, data integrity, and non-repudiation. Traditionally, the signer uses his/her secret key to sign messages by using some signature schemes, and the recipient of the signature verifies the validity of it using the signer's public key. In 1996, Jakobsson et al. firstly proposed a designated verifier signature scheme that the authentication of a message is provided without having a non-repudiation property of traditional signatures [1]. That is, only one specified recipient, called a designated verifier, can be convinced of the validity of the signature. This is achieved by enabling the specified recipient to simulate a signature which is indistinguishable from the signer's signature. Therefore, when Bob is designated as a verifier of a signature from Alice, he will certainly trust that it originated from Alice upon verifying it, because he knows that he did not generate it. However, the third party Cindy has no reason to accept that Alice is the signer of such a signature because she knows that Bob has the ability to generate a signature in an indistinguishable way. Therefore, a designated verifier signature scheme provides signer ambiguity in the sense that one cannot verify whether the signer or the designated verifier issued the signature. Given a designated verifier signature and two potential signing public keys, it is computationally infeasible for the third party to determine under which of the two corresponding secret keys the signature was generated. A designated verifier signature scheme has many applications for electronic voting or electronic auction.

Even though signer ambiguity exists in a designated verifier signature scheme, it does not prevent a third party from checking the correctness of the signature. This is due to the fact that to verify a designated verifier signature, only the public keys of the signer and the designated verifier are needed. This could make the signer's identity revealed. If a designated verifier signature is captured on the line by an eavesdropper and he/she knows that the specified recipient has not received the signature yet, the eavesdropper can verify the signature using the public keys of the two participants and identify the signer. To overcome this problem, Saeednia et al. [2] proposed a strong designated verifier signature scheme based on the Schnorr signature scheme [3] and Zheng's signcryption scheme [5]. The strongness property refers to the requirement of the designated

* Corresponding author. Tel.: +82 10 6425 3168; fax: +82 2 704 8273.
E-mail address: jslee702@sogang.ac.kr (J.-S. Lee).

0920-5489/$ - see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.csi.2008.02.003

verifier to use his/her secret key to verify the validity of a signature. This means that only the designated verifier can verify the signature in the normal communication. Since the designated verifier still has an ability to generate an indistinguishable signature from the signer's signature, the signer ambiguity is preserved in the strong designated verifier scheme.

We point out that, in Saeednia et al.'s scheme, the signature can be verified not only with the designated verifier's secret key but also with the signer's secret key. This could make the signer's identity revealed. If the secret key of a signer is compromised and an eavesdropper captures the signature before it has been received by the designated verifier, the eavesdropper can verify the signature with the signer's secret key and be convinced that the signature is from that signer. Because protecting the identity of the signer is the goal of a strong designated verifier signature scheme, it is desirable that the eavesdropper cannot verify the signature even with the secret key of the signer.

1.1. Contribution

In this paper, we propose a new strong designated verifier signature scheme which can be verified only with the designated verifier's secret key. Therefore, the proposed scheme provides signer ambiguity even in the situation in which the secret key of the signer is compromised. To achieve this goal, if an eavesdropper is trying to verify a signature with the secret key of the signer, he/she should have one more additional value which is protected under the DLP assumption. We devise a strong designated verifier signature scheme based on the Schnorr signature scheme [3] and Wang et el.'s authenticated encryption scheme [4].

1.2. Organization

The rest of this paper is organized as follows. In Section 2, we review Saeednia et al.'s strong designated verifier signature scheme and show that the identity of the signer can be revealed if the secret key of the signer is compromised. In Section 3, we propose a new strong designated verifier signature scheme that protects the signer in the situation in which the signer's secret key is compromised. We discuss its security properties in Section 4. Finally, we make a conclusion in Section 5.

2. Review of Saeednia et al.'s strong designated verifier signature scheme

Some common parameters are initially shared between the users: a large prime p, a prime factor q of $p-1$, a generator $g \in Z_q^*$ of order q, and a one-way hash function H that outputs values in Z_q. The signer Alice has her key pair (x_A, y_A), where x_A is a randomly selected secret key in Z_q^* and the corresponding public key $y_A = g^{x_A} \bmod p$. Likewise, the designated verifier Bob has his key pair (x_B, y_B).

2.1. Signature generation

(1) Alice selects two random values $k \in Z_q$ and $t \in Z_q^*$.

(2) Alice computes r and s as follows:

$$r = H\left(m, y_B^k \bmod p\right)$$
$$s = kt^{-1} - rx_A \bmod q.$$

(3) The signature is then $\sigma = (r,s,t)$.

2.2. Signature verification

Upon receiving m and σ, Bob can verify the validity of the signature by checking whether $r = H(m, (g^s y_A^r)^{tx_B} \bmod p)$.

2.3. Signature simulation

Bob can generate a transcript indistinguishable from Alice's signature as follows.

(1) Bob selects two random values $a \in Z_q$ and $b \in Z_q^*$.
(2) Alice computes r', s' and t' as follows.

$$r' = H\left(m, g^a y_A^b \bmod p\right)$$
$$s' = ab^{-1} r' \bmod q$$
$$t' = br'^{-1} x_B^{-1} \bmod q.$$

(3) The simulated signature is then $\sigma' = (r',s',t')$.

2.4. Weakness

We point out that if Alice's secret key is compromised and an eavesdropper gets the signature (r,s,t) before it has been received by Bob, the eavesdropper can verify the signature by checking the equality $r = H\left(m, \left(y_B^{s + rx_A}\right)^t \bmod p\right)$. In this case, the eavesdropper can verify the signature correctly, and he/she can confirm that the real signer is Alice. Because signer ambiguity is an important property of a strong designated verifier signature scheme, it is undesirable to construct a scheme that is verifiable even with the signer's secret key. Therefore, to make a strong designated verifier signature scheme more secure, the signature should be verified by only one specified person, who is the designated verifier.

3. Proposed scheme

In this section, we propose a new strong designated verifier signature scheme based on the Schnorr signature scheme and Wang et al.'s authenticated encryption scheme. The proposed scheme eliminates the above weakness of Saeednia et al.'s scheme. Our scheme uses the same parameters (p, q, g, H) as Saeednia et al.'s scheme. The two participants Alice and Bob have their key pairs (x_A, y_A) and (x_B, y_B), respectively. Each secret key is protected under the DLP assumption. DLP assumption means that, for any given $y \in Z_p^*$, it is computationally infeasible to derive $x \in Z_q^*$ such that $y = g^x \bmod p$.

3.1. Signature generation

(1) Alice selects a random value $k \in Z_q^*$.

(2) Alice computes r, s and t as follows:

$$r = g^k \bmod p$$
$$s = k + x_A r \bmod q$$
$$t = H\left(m, y_B^s \bmod p\right).$$

(3) The signature is then $\sigma = (r,t)$.

3.2. Signature verification

Upon receiving m and σ, Bob can verify the validity of the signature by checking whether $t = H\left(m, \left(ry_A^r\right)^{x_B} \bmod p\right)$.

3.3. Signature simulation

Bob can simulate the transcript $\sigma' = (r', t')$ for the message m by selecting a random number $k' \in Z_q^*$ and computes r' and t' as follows:

$$r' = g^{k'} \bmod p$$
$$t' = H\left(m, \left(r'y_A^{r'}\right)^{x_B} \bmod p\right).$$

4. Analysis of the proposed scheme

In this section, we show that the proposed scheme is correct, and satisfies unforgeability and signer ambiguity. We also show that our scheme overcomes the weakness of Saeednia et al.'s scheme.

4.1. Correctness

The signature (r,t) is verified correctly by Bob as

$$t = H\left(m, y_B^s \bmod p\right) = H\left(m, y_B^{k + x_A r} \bmod p\right) = H\left(m, \left(ry_A^r\right)^{x_B} \bmod p\right).$$

4.2. Unforgeability

To forge a signature σ, the adversary should know the secret key of the signer, which is protected under the DLP assumption. Moreover, to forge a simulated signature σ', the adversary should know the secret key of the designated verifier which is also protected under the DLP assumption.

4.3. Signer ambiguity

Let $(\bar{r}, \bar{t})$ be a signature that is randomly chosen from the set of all valid Alice's signatures intended to Bob. The probability $\Pr[(r,t) = (\bar{r}, \bar{t})]$ is $\frac{1}{q-1}$ because (r,t) is generated from a randomly chosen value $k \in Z_q^*$. Likewise, the probability $\Pr[(r', t') = (\bar{r}, \bar{t})]$ has the same value $\frac{1}{q-1}$ because it is generated from $k' \in Z_q^*$. This means that the transcripts simulated by Bob are indistinguishable from the signatures generated by Alice.

4.4. Security against signer's key compromise

In the proposed scheme, even if the secret key of the signer is compromised and an eavesdropper obtains the signature before the designated verifier receives it, the eavesdropper cannot verify the signature. This is because to verify a signature, the eavesdropper should know the value of k protected under the DLP assumption as well as the secret key of the signer. It can be shown as follows:

$$t = H\left(m, \left(ry_A^r\right)^{x_B}\right) = H\left(m, y_B^{k + x_A r}\right).$$

Therefore, the eavesdropper still cannot identify the signer.

5. Conclusion

In this paper, we propose a new strong designated verifier signature scheme. Compared to Saeednia et al.'s scheme, even if the secret key of the signer is compromised and the signature is captured by an eavesdropper before Bob receives it, there is no way to verify the signature and therefore identify the signer. Because the goal of a strong designated verifier signature scheme is to protect the identity of the signer, our scheme is more secure and suitable for the purpose of a strong designated verifier signature scheme.

References

[1] M. Jakobsson, K. Sako, R. Impagliazzo, Designated verifier proofs and their applications, Advances in Cryptology — EUROCRYPT '96, Lecture Notes in Computer Science, vol. 1070, Springer, Berlin, 1996, pp. 143–154.
[2] S. Saeednia, S. Kremer, O. Markowitch, An efficient strong designated verifier signature scheme, ICISC'03, Lecture Notes in Computer Science, vol. 2971, Springer, Berlin, 2004, pp. 40–54.
[3] C.P. Schnorr, Efficient signature generation for smart cards, Journal of Cryptology 3 (3) (1991) 161–174.
[4] G. Wang, F. Bao, C. Ma, K. Chen, Efficient authenticated encryption schemes with public verifiability, The 60th IEEE Vehicular Technology Conference (VTC 2004) — Wireless Technologies for Global Security, IEEE Computer Society, vol. 5, 2004, pp. 3258–3261.
[5] Y. Zheng, Digital signcryption or how to achieve cost(signature & encryption) << cost(signature)+cost(encryption), Advances in Cryptology — Crypto '97, Lecture Notes in Computer Science, vol. 1294, Springer, Berlin, 1997, pp. 165–179.

Jik Hyun Chang received the B.S. and M.S. degrees in Mathematics from Seoul National University, Korea. He received his Ph.D degree in the Department of Computer Science & Engineering from the University of Minnesota, USA. Since 1986, he serves as a professor at Sogang University, Korea. His research interests include algorithm design and analysis, and cryptographic algorithms.

Ji-Seon Lee received the B.S., M.S., and Ph.D degrees in Computer Science & Engineering from Sogang University, Korea. She is currently a post-doctoral associate at Korea University, Korea. Her research interests include cryptographic protocols and network security.