Provision of Deniability in E-mail Protocol

Hyo Kim

Division of Media Studies, Ajou University, Korea

Summary
E-mail is considered as one of the most important and most frequently used internet services. For privacy and security reasons, it is desirable that e-mail protocol provides deniability. Deniability ensures that a receiver can identify the source of a received message while a third party cannot. If deniability is provided in e-mail protocol, the third party would not be able to distinguish who created the e-mail between sender and receiver. However, current secure e-mail protocols such as PGP and S/MIME use digital signature which does not provide deniability. In this paper, I propose a new identity-based designated verifier signature scheme which can be applied to deniability in e-mail protocol.

Key words:
E-mail protocol, Deniability, Designated verifier signature.

1. Introduction

Pretty Good Privacy (PGP)[1] and S/MIME[2] are widely used e-mail service for message authentication. Both services use a combination of symmetric key encryption scheme for message confidentiality and digital signature scheme for message authentication. Digital signatures are good for message authentication since anyone can verify the validity of the signature using the signer's public key. However, for privacy reasons, the signer may not want anyone to be able to verify his/her signature. That is, the signer wants only a specified person can verify the signature. In this case, ordinary digital signature scheme is not a suitable to protect the signer's privacy.

Jakobsson et al.[3] proposed a concept of designated verifier signature scheme in 1996. A designated verifier signature scheme is a special type of digital signature which provides message authentication without non-repudiation. That is, designated verifier signature scheme provides deniability. This is possible by giving the ability of generating a signature which is indistinguishable from the signer's signature to the designated verifier. Suppose that Alice sends her designated verifier signature to Bob. Unlike the conventional digital signature scheme, Bob cannot prove to a third party that Alice has created the signature. This is accomplished by the Bob's capability of creating another signature designated to himself which is indistinguishable from Alice's signature. I call Bob a designated verifier. Jakobsson et al. also introduced a stronger version of a designated verifier signature scheme. In this stronger scheme, no third party can even verify the validity of the signature, since the designated verifier's secret key is required in the verifying phase.

Since Saeednia et al.[4] formalized the notion of strong designated verifier signature scheme and proposed an efficient scheme in their paper in 2003, and Susilo et al.[5] articulated the first identity-based strong designated verifier signature scheme in 2004, there have been several identity-based strong designated verifier signature schemes [6-8]. For example, identity-based signature scheme was firstly suggested by Shamir[9] and the practical identity-based signature scheme was proposed by Boneh and Franklin[10].

I found that strong designated verifier signature scheme would be applicable to deniable e-mail service directly. That is, the e-mail sender sends his/her mail with his/her strong designated verifier signature to the specific verifier. Upon receiving the e-mail and the signature, the verifier can confirm that the e-mail is from the real sender by checking the validity of the signature. However, the signature attached to the e-mail can also be generated by the verifier. Therefore, any third party cannot distinguish who is the e-mail sender.

Recently, deniable e-mail service using conventional signature scheme was proposed by Harn and Ren [11]. However, up to now there has been no effort to use designated verifier signature scheme for deniable e-mail service. In this paper, I propose a deniable e-mail service using designated verifier signature scheme.

The rest of the paper is organized as follows. In section 2, I give background information and security requirements to understand this paper. In section 3, I propose a new identity-based strong designated verifier signature scheme and construct e-mail services using the proposed designated verifier signature scheme. I give a conclusion in section 4.

2. Preliminaries

Let G_1 be an additive cyclic group with prime order q, G_2 be a multiplicative cyclic group of same order and P be a generator of G_1. Let $e: G_1 \times G_1 \rightarrow G_2$ be a bilinear mapping with the following properties:

Manuscript received November 5, 2008
Manuscript revised November 20, 2008

(1) The map e is bilinear, i.e. $e(aP,bP)=e(P,P)^{ab}$ for all $P,Q\in G_1,\ a,b\in Z_q^*$.
(2) There exists $P\in G_1,\ Q\in G_1$ such that $e(P,Q)\neq 1$.
(3) There exists an efficient algorithm to compute $e(P,Q)$ for all $P,Q\in G_1$.

The security requirements of our deniable e-mail service are as follows.

Unforgeability : Only the mail sender or the mail receiver can generate a signature in an indistinguishable way.

Deniability: The mail sender can deny that he/she sent an e-mail to a specified receiver. The specified mail receiver cannot confirm any third party that the e-mail is from the e-mail sender.

3. Deniable E-mail Protocol

In this section, a new identity-based strong designated verifier signature scheme is proposed and applied to deniable e-mail protocol. The scheme will be discussed as it satisfies unforgeability and deniability.

3.1 New Identity-Based Strong Designated Verifier Signature Scheme (NIBSDVS)

In the proposed a new identity-based strong designated verifier signature scheme, there are five phases – Setup, Key extract, Signature generation, Signature verification, Signature simulation.

[Setup] The system parameters are generated as follows. The private key generator(PKG) chooses groups G_1 and G_2 of prime order q such that an admissible pairing $e:G_1\times G_1\to G_2$ can be constructed and pick a generator P of G_1. Now, the authority picks a $s\in Z_q^*$ as the master secret key and computes the corresponding public key $P_{pub}=sP$. $H_1(\cdot)$ and $H_2(\cdot)$ are two cryptographic hash functions, where $H_1:\{0,1\}^*\to G_1$ and $H_2:\{0,1\}^*\to Z_q^*$. The system parameters are $(G_1,G_2,P,P_{pub},H_1,H_2,e,q)$ and the master secret s is kept secret.

[Key extract] Given an identity ID_U, PKG computes $S_{ID_U}=sH_1(ID_U)$ and sends it to the user with identity ID_U. I remark $Q_{ID_U}=H_1(ID_U)$ as the public key of the user with identity ID_U. In this scenario, Alice is the signer with identity ID_A and has her public key $Q_{ID_A}=H_1(ID_A)$ and secret key $S_{ID_A}=sQ_{ID_A}$. Bob is the designated verifier with identity ID_B and has his public key $Q_{ID_B}=H_1(ID_B)$ and his secret key $S_{ID_B}=sQ_{ID_B}$.

[Signature generation] To sign a message m for Bob, Alice randomly chooses a number $k\in Z_q^*$ and computes the signature (σ,t) as follows.

$$t=kP$$
$$T=t+H_2(m,t)S_{ID_A}+kP_{pub}$$
$$\sigma=e(T,Q_{ID_B})$$

[Signature verification] Given system parameters, the signer's public key $Q_{ID_A}=H_1(ID_A)$, and the signature (σ,t) on a message m, Bob accepts the signature if and only if the following equation holds:

$$\sigma=e(t,Q_{ID_B})e(Q_{ID_A},S_{ID_B})^{H_2(m,t)}e(t,S_{ID_B})$$

[Signature simulation] Bob can produce the signature intended for himself by choosing one random number $k'\in Z_q^*$ and computes the signature (σ',t') as follows.

$$t'=k'P$$
$$\sigma'=e(t',Q_{ID_B})e(Q_{ID_A},S_{ID_B})^{H_2(m,t')}e(t',S_{ID_B})$$

3.2 Security Analysis

I show that the proposed scheme is correct, unforgeable, and provides deniable authentication.

Correctness : The correctness of the proposed scheme is justified as follows:

$$\begin{aligned}\sigma&=e(T,Q_{ID_B})\\&=e(t+H_2(m,t)S_{ID_A}+kP_{pub},Q_{ID_B})\\&=e(t,Q_{ID_B})e(H_2(m,t)S_{ID_A},Q_{ID_B})e(kP_{pub},Q_{ID_B})\\&=e(t,Q_{ID_B})e(S_{ID_A},Q_{ID_B})^{H_2(m,t)}e(kP,sQ_{ID_B})\\&=e(t,Q_{ID_B})e(Q_{ID_A},S_{ID_B})^{H_2(m,t)}e(t,S_{ID_B})\end{aligned}$$

Unforgeability : To forge a signature generated by Alice, the adversary should have the secret key of the signer. Likewise, to forge a simulated signature by Bob the adversary should have the secret of the designated verifier. Since all the secret keys are protected under DLP assumption, it is infeasible to forge a signature in the proposed scheme.

Deniability: Let (σ'', t'') be a signature that is randomly chosen from the set of all valid Alice's signatures that are intended to Bob. The probability $\Pr[(\sigma, t) = (\sigma'', t'')]$ is $\frac{1}{q-1}$ because (σ, t) is generated from a randomly chosen value k. Likewise, the probability $\Pr[(\sigma', t') = (\sigma'', t'')]$ is $\frac{1}{q-1}$ because (σ, t) is generated from a randomly chosen value k'. What it means is that the transcripts simulated by Bob are indistinguishable from the signatures generated by Alice. Therefore, the proposed scheme guarantees deniable authentication.

3.3 Deniable E-mail Protocol using NIBSDVS

This section describe a scenario in which the proposed scheme NIBSDVS is used for deniable e-mail service. I assume that each user, Alice and Bob, has a pair of public and private key. Since the scheme is based on identity cryptography, the public keys of each user are identity information. For the message confidentiality, Alice encrypts the message m using Bob's public key. That is, Alice generates an encrypted e-mail message c, and then she generates a strong designated verifier signature on the encrypted e-mail c. Finally, Alice sends encrypted e-mail with the signature which has the form of $\{c, (\sigma, t)\}$ to Bob.

Upon receiving $\{c, (\sigma, t)\}$, Bob recovers the e-mail by decrypting c using his secret key. Since this is a decryption process which needs Bob's secret key, only Bob can recovers the e-mail. Bob then checks that the e-mail was sent from Alice by verifying (σ, t). If the verification succeeds, Bob confirms that the e-mail was sent by Alice. However, since Bob can also generate a signature on an encrypted e-mail c, the third party does not know who made the signature on an encrypted e-mail c. Deniability is guaranteed if Alice and Bob can generate a valid transcript $\{c, (\sigma, t)\}$. This means that since both Alice and Bob can generate a signature, the third party cannot confirm that who generates the signature. Even if Bob wants to give the e-mail to the third party, the third party would not believe that the e-mail was sent from Alice. This is because Bob also has an ability to generate a transcript $\{c, (\sigma, t)\}$. That is, Bob can generate an encrypted message c' and generates a strong designated verifier signature (σ', t') using signature simulation algorithm.

4. Conclusions

The paper proposes a new identity-based strong designated verifier signature. This newly proposed scheme was applied to deniable e-mail services. The proposed e-mail service enhances the security when the message confidentiality and signer privacy are important concerns. Hence, the scheme improves the privacy concern of PGP and/or S/MIME.

References

[1] S. Garfinkel, PGP: Pretty Good Privacy. Oreilly, 1994.
[2] B. Ramsdell, "Secure/multipurpose Internet mail extensions (S/MIME) version 3.1 message specification, RFC 3851, 2004.
[3] Jokobsson, M, Sako K. Impagliazzo R., "Designated verifier proofs and their applications," Advances of Cryptology - EUROCRYPT'96, LNCS 1716, pp.258-273, 1996.
[4] Saeednia S, Kremer S., Markowitch O, "An efficient strong designated verifier signature scheme," ICICS 2003, LNCS 2971, pp.40-54, 2003.
[5] Susilo W., Zhang F. Mu Y, "Identity-based srong designated verifier signature schemes," ACISP 2004, LNCS 3108, pp.313-324, 2004.
[6] Huang X., Susilo W., Mu Y., Zhang F., "Short identity-based strong designated verifier signature schemes," ISPEC 2006, LNCS 3903, pp.214-225, 2006.
[7] Kumar K. Shailaja G., Saxena A., "Identity based strong designated verifier signature scheme," Informatica 18(2), pp.239-252, 2007.
[8] Zhang J., Mao J, "A novel ID-based designated verifier signature scheme," Information Science 178 (2008), pp.766-773, 2008.
[9] Shamir A., "Identity-based cryptosystems and signature schemes," Advances of Cryptology – CRYPTO '84, LNCS 7, pp. 47-53, 1984.
[10] Boneh D., Franklin M., "Identity-based encryption from the Weil pairing," Advances of Cryptology – CRYPTO 2001, LNCS 2139, pp. 213-229, 2001.
[11] Harn, Ren, "Design of fully deniable authentication service for e-mail applications," IEEE Communication letters, Vol. 12, No. 3, 2008.

Hyo Kim received the M.S. degree in Communication from the University of Utah in 1998 and the Ph.D degree in Communication from the Rutgers University in 2003. He is a faculty member at Ajou University in Korea. His research interests include digital television broadcasting and the internet application research.