Security of Deputy Signature

Jonathan Jen-Rong Chen
Dept. of Information Management
Van Nung Institute of Technology
jonathan@cc.vit.edu.tw

Kai-Hsiung Ling
Dept. of Finance
The Overseas Chinese Institute of Technology

Yuan-Chi Liu
Department of International Trade
Ta-Hwa Institute of Technology
liu32717@ms45.hinet.net

Yen-Ling Pan
Institute of Information Management
National Defense Management College
i9203013@ms1.ndmc.edu.tw

Abstract

E-system, a new commerce model, is a new era for business direction. When a principal is absent (goes on an errand or on leave), a well-designed deputy system keeps the business operations working. In the network world, identity verification and any substitute for traditional signature can be done by digital signature [1]. Deputy signature guarantees the existence of deputy system in e-system. Current deputy mechanism addresses the verification of deputy signature. No research has been done on the prevention of the illegal use of deputy system when the principal returns and the deputy system is not in use. We propose a mechanism to solve the problem of illegal use of deputy system when the power of deputy system is not legally "ON."
Key words: information security, digital signature, deputy signature.

1. Introduction

In the information era, information technology is an important tool to support all work. The popularity of network changes the methods of information transfer and speeds up the development of e-commerce. As a new model of commerce, e-commercialization is a competitive goal for all business users. A well-designed deputy system is helpful to business operations in non-network system and is imperative in network system.

In a network environment, in addition to verifying the identity, digital signature can also be used to substitute for the traditional handwritten signature. During the principal's absence, deputy signature keeps the system running and the security of private key as well. The characteristics of deputy signature are as follows: private, identifiable, secure, and undeniable. Current deputy mechanism addresses the verification of deputy signature. No research has been done on the prevention of the illegal use of deputy system when deputy system is not in use. We propose a mechanism to solve the problem of illegal use of deputy system when the power of deputy system is not legally "ON." Our scheme provides a delegation time schedule for the receiver to solve the associated problem of deputy signature. Unauthorized deputy will be ruled out once the principal returns and the deputy's authority has lapsed.

The layout of this paper is as follows. Literature review is in Section 2. Section 3 introduces our scheme. In Section 4, we analyze the security of our scheme. Section 5 concludes the paper.

2. Literature Review

Digital signature fulfills the requirement of signature in network environment and enhances the feasibility of e-commerce. In the E-era, the un-deniability of digital signature enables e-documents to be widely and legally accepted. The principal uses his/her private key to sign and send documents. The receivers verify the documents by public key. When one cannot sign documents personally, deputy signature enables the deputy to keep the system working without using the original private key. Mambo et al [2,3] propose deputy signature in 1996. Deputy signature allows deputy to sign documents with equal efficacy. In general, deputy signature has properties as follows [11]:

A. Distinguish-ability: The difference between deputy signature and original signature is distinguishable.
B. Unforgeability: No one else can forge deputy signature other than the real deputy.
C. Verifiability: The receiver(s) can believe that the principal agrees to deputy signature for the documents.
D. Un-deniability: deputy cannot deny deputy signature.

Unfortunately, the Mambo deputy signature is deniable. Zhang [4], Lee et al [5], Sun and Hsieh [6] solve this problem in their schemes .

3. Our Scheme

3.1 Registration

First, firm should set up a system center. The manager of system center chooses a big prime p [7,8,9] to satisfy the following equations:

$$p = 4p_1q_1 + 1$$

where p_1, q_1 are big primes.
Let $n = p_1q_1$
Then, select a number g modulo p with order n, i.e., $g^n \equiv 1 \pmod{p}$, $g^{p_1} \neq 1 (\mathrm{mod}\, p)$, $g^{q_1} \neq 1 (\mathrm{mod}\, p)$.

{p,n,g} is the public key of the system center. $\{p_1, q_1\}$ is private key.
The principal (hereafter A) selects a number $x_A \in Z_n^*$, calculates:

$$y_A \equiv g^{x_A} \pmod{p} \quad \text{.....(1)}$$

and registers to system center. $\{y_A\}$ $\{x_A\}$ are the public key of A and private key, respectively.

If A is to assign B as his/her deputy to sign documents during $T_A = [t_1, t_2]$. B selects a number $x_B \in Z_n^*$, calculates:

$$y_B \equiv g^{x_B} \pmod{p} \quad \text{.....(2)}$$

and registers to system center, where $\{y_B\}$ $\{x_B\}$ are the public key of B and private key, respectively.

3.2 Delegation

Step 1: A selects a number $d_1 \in Z_n^*$ and calculates:

$$D_1 \equiv g^{d_1} \pmod{p} \quad \text{.....(3)}$$

Step 2: Calculate:

$$y_B + T_A \equiv x_A D_1 + d_1 E_1 \pmod{n} \quad \text{.....(4)}$$

Step 3: Send deputy certificate $\{T_A, D_1, E_1\}$ to B as shown in Diagram 1.

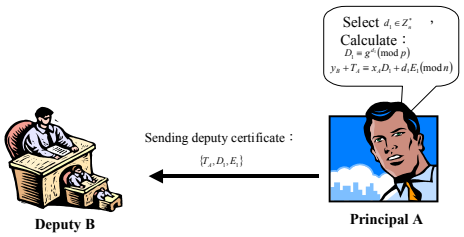

Diagram 1: Delegating deputy and sending deputy certificate

3.3 Generation of deputy signature

If B is going to sign on the message m during deputy time,

Step 1: Select a number $d_2 \in Z_n^*$ and calculate:

$$D_2 \equiv g^{d_2} \pmod{p} \quad \text{.....(5)}$$

Step 2: Calculate:

$$E_2 \equiv mx_B + d_2 D_2 \pmod{p} \quad \text{.....(6)}$$

Step 3: Sending deputy certificate $\{T_A, D_1, E_1\}$ and the digital signature $\{m, D_2, E_2\}$ with message m to a receiver C as shown in Diagram 2.

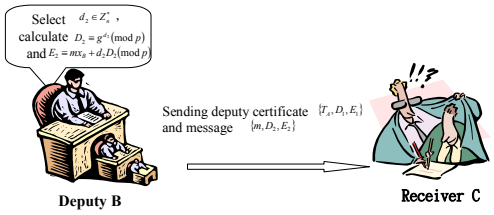

Diagram 2: Running of Deputy signature

3.4 Verification of deputy signature

The receiver C verifies:

$$g^{y_B + T_A} \equiv y_0^{D_1} D_1^{E_1} \pmod{p} \quad \text{.....(7)}$$

$$g^{E_2} \equiv y_B^m D_2^{D_2} \pmod{p} \quad \text{.....(8)}$$

If the equations above are valid, accept deputy B. If not, reject.

4. Security Analyses

Theorem 1: If A is honest, Eqs.(7)(8) are valid.

Proof:

To have base g for the both sides of Eq.(4) and obtain:

$$g^{y_B + T_A} \equiv g^{x_A D_1} g^{d_1 E_1} \pmod{p}$$
$$\equiv y_A^{D_1} D_1^{E_1} \pmod{p}$$

According to Eqs.(1)(3)

For the same reason, having base g for both sides of Eq.(6) and obtaining:

$$g^{E_2} \equiv g^{mx_B} g^{d_2 D_2} \pmod{p}$$
$$\equiv y_B^m D_2^{D_2} \pmod{p}$$

According to Eqs.(2)(5), the theorem 1 is proven.

Theorem 2: The difficulty of forging Eq.(1) is the complexity of discrete logarithm

Proof:

ElGamal [10] has proven that following equations to be discrete logarithm:

$$g^m \equiv y^r r^s \pmod{p} \quad \text{.....(9)}$$

Comparing Eq.(7) and Eq.(9), we find that if

$$y_B + T_A \equiv m \pmod{n} \quad \text{.....(10)}$$

then Eq.(7) is similar to Eq.(9). Namely, the complexity of Eq.(9) is discrete logarithm. So is Eq.(10). On the contrary, if Eq.(10) is the problem of discrete logarithm, So is Eq.(9). In addition, the complexity of forging Eq.(8) is at least equal to the complexity of Eq.(7). The proof is similar and omitted. Thus, theorem 2 is proven.

From the two theorems above, we know that if an attacker (A or B) is going to invade our system, he/she has to solve the complexity of discrete logarithm.

5. Conclusion

In recent years, along with the development of network, e-commerce is expanding rapidly. In addition to overturning the traditional model of transactions, this new business activity also provides ample business opportunity. Network is used for business activities and generates e-business. For e-business, information security is an important topic. In a non-e environment, deputy system can be done by written delegation certificate. In an e-environment, a trustable deputy signature is needed. Our deputy signature has the advantage of timing for the verification of deputy signature. No illegal deputy can be accepted once the principal returns and the deputy's authority has lapsed.

References

[1] Rivest R. L., Shamir A., and Adleman L., "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM*, Vol.21, No.2, pp.120-126, 1978.

[2] MAMBO, Masahiro, USUDA, Keisuke, and OKAMOTO, Eiji (1996b): "Proxy Signatures for Delegation Signing Operation," *Proceedings of third ACM Conference_on Computer and Communications Securit*y, New Delhi, pp. 48-57,1996

[3] MAMBO, Masahiro, USUDA, Keisuke, and OKAMOTO, Eiji (1996a): "Proxy Signatures: Delegation of the Power to Sign Message," *IEICE. Transaction Fundamentals*, Vol. E 79-A, no. 9, pp.1338-1354, 1996

[4] Zhang K., "Threshold Proxy Signature Schemes," *1997 Information Security Workshop*, Janpan, Sep. 1997, pp. 191-199.

[5] Lee N. Y., Hwang T. and Wang C. H., "On Zhang's nonrepudiable Proxy Signature Schemes," *Third Australasian Conference*, ACISP '98, 1998, pp. 415-422.

[6] Sun H. M., Hsieh B. T., "Remarks on two nonrepudiable proxy signature schemes," *Ninth National Conference on Information Security*, Taiwan, 1999, pp. 241-246.

[7] Gordon, "Strong RSA Key," *Electronics Letters*, Vol.20, pp.514, 1984.

[8] Harn L., "Public-key Cryptosytem Based on Factoring and Discrete Logarithms," *IEE Proc.-Comput. Digit. Tech.*, Vol.141, No.3, pp. 193-195, 1994.

[9] Tu K., "Comment: Public-Key Cryptosystem Design Based on Factoring and Discrete Logarithms," *IEE Proc.-Comput. Digit Tech.*, Vol.143, No.1, 1996.

[10] ElGamal T., "A public key cryptosystem and a signature scheme based on the discrete logarithm," *IEEE Transactions on Information Theory*, Vol.31, pp.469-472, 1985.

[11] 陳炳彰,孫宏民,黃宗立,"代理簽章之發展與演進", *資訊安全通訊*, Vol.7, No.3, June 2001