休閒運動管理學刊
第二期 57 頁-63 頁
民國一〇四年九月

Journal of Leisure and Sports Management
No.2 pp.57~63
September 2015

A new anonymous proxy signature using a trusted party

Chun-Te Lee Huna-Mei Chu

Cheng Shiu University

Abstract

The development of information technology has changed everyday life in several ways. Some researchers [1-35] have attempted to find out how transmission of inform ation by a network affects people's everyday behavior, and to what degree does a pro xy digital signature scheme play a role in this affect. For example, in agent-based e-c ommerce and e-procurement systems, information security is a key element in the dev elopment of a network, making proxy digital authentication especially important in virt ual cyberspace. Recent studies [30] have proposed an argument for protecting the prox y signature, which is the concept of keeping the proprietary security keys from being leaked by agents during the agency process. This protection keeps the general characte ristics of information security from being accessed until the security key is changed b y the client during the agency period. However, this argument has been disproved [6]. So we propose a proxy digital signature policy that does not require any hash functi ons when compared to the thesis paper [6]. Our study presents a channel that does n ot require security to change a client's security key. The policy is based on a strategy of discrete logarithm complexity, which may also be applied to applications using tim e stamp technology.

Key Words: Proxy Signature, Anonymous Signature, Discrete Logarithm, Undenia bility, Unforgeability

1 Introduction

The development of information technology has changed everyday life in several ways. Some researchers [1-35] have attempted to find out how transmission of information by a network affects people's everyday behavior, and to what degree does a proxy digital signature scheme play a role in this affect. For example, in agent-based e-commerce and e-procurement systems, information security is a key element in the development of a network, making proxy digital authentication especially important in virtual cyberspace. In considering personal data privacy protection requirements for proxy digital signatures, designing an anonymous proxy signature mechanism has always been an interesting research topic.

A good anonymous proxy signature mechanism should be able to meet the following requirements:

Unforgeability [2, 4, 7, 18, 19, 24, 26, 30, 31, 62,]: Only a designated proxy signer can create a valid proxy signature for the original signer. That is to say, everyone cannot forge a valid proxy signature without the delegation of the original signer.

Verifiability [2, 4, 7, 8, 11, 18, 26, 30, 31]: A verifier can be convinced that the received message is signed by the proxy signer authorized by the original signer after checking and verifying the proxy signature.

Undeniability [4, 7, 8, 11, 18, 26, 30, 31]: The proxy signer is no denying that the signature he produced.

Identifiability [2, 4, 8, 11, 18, 30, 31]: Anyone including the original signer can decide the corresponding proxy signer’s identity from the proxy signature.

Anonymity [4, 7, 28, 30, 32]: The reporting studies about anonymous property in proxy signature plan purposes to protect the identity of the proxy signer, keeping the secrecy of the proxy signer to outsider.

II. Literature review

The study [6] mainly discussed the following

	Proxy signer P_s	Verifier
Anonymous proxy signature generation	$\sigma_i = r_i V,\ where\ i = 1\ to\ n,\ i \neq s$ $\sigma_s = psk_s * Y = r_s^{-1} * x_s^{-1} * H_0\left(m_w,\ m,\ V,\ U\right) * Y$ $p\sigma sum = \sum_{i=1}^{n} \sigma_i$ $A = r_s * c * psk_s P$ $B = r_s \sigma_s$ $C = r_s * p\sigma sum$ $D = r_s * c * V$ $L = c * x_s^{-1} * V$ $\sigma = \left(\sigma_1,\ \sigma_2, \ldots,\ \sigma_n,\ m,\ m_w,\ c,\ A,\ B,\ C,\ D,\ L,\ U,\ V\right)$ $\xrightarrow{\sigma}$	
Anonymous proxy signature verification		$checks$ $(e(D,\ \sum_{i=1}^{n} \sigma_i)) \bullet e(A,\ Y)?$ $= e(cV,\ C - B) \bullet e(L,\ H_0\left(m_w,\ m,\ V,\ U\right)Y) \bullet e(U,\ B)$

Fig. 1 Anonymous proxy signature generation phase and the verification phase of our scheme

III. Our Propose Scheme

(1) the parameter generation phase

The system center selects a large prime number p, follow by a primitive element g. The system center then announces parameters p and g.

(2) key generation phase

the original signer Alice selects $x_o \in Z_p^*$ as her private key and computes her public key as $y_o \equiv g^{x_o} (\bmod\, p)$, Each proxy signer $x_i \in U$ randomly selects $x_i \in Z_p^*$ as his/her private key and sets the corresponding public key as $y_i \equiv g^{x_i} (\bmod\, p)$.

(3) delegation signing phase

the original signer Alice selects $x_1 \in Z_p^*$ as her pseudo private key and computes her pseudo public key as $y_1 \equiv g^{x_1} (\bmod\, p)$, Without loss of generality, the proxy signer $x_i \in U$ randomly selects $x_2 \in Z_p^*$ as his/her pseudo private key and sets the corresponding pseudo public key as $y_2 \equiv g^{x_2} (\bmod\, p)$. the original signer Alice sends her pseudo public key y_1 to the proxy signer Bob, the proxy signer Bob calculate $a \equiv x_i y_2 + x_2 (\bmod\, \phi(p))$, then transmits parameter $\{a, y_2\}$ to the original signer Alice.

(4) delegation verification phase

The original signer Alice calculate

$b \equiv (x_o w + x_i) y_1 y_2 + (x_1 + x_2) c (\bmod \phi(p))$, then transmits {b, c} to the proxy signer Bob, where w is the expiration time of the delegation, and the signing power in the warrant.

(5) APS generation phase

The proxy signer Bob calculates:

$$(b + mc)M \equiv (x_0 w + x_i) y_1 y_2 M + (x_1 + x_2 + m) cM (\bmod \phi(p))$$

where $M \equiv g^{m} (\bmod p)$,

then calculates

$d_1 \equiv (b + mc) M (\bmod \phi(p))$,

$d_2 \equiv y_1 y_2 M (\bmod \phi(p))$

$d_2 \equiv g^{d_1} (y_0^{w} y_i)^{-d_2 (cm)^{-1}} (\bmod p)$,

$r_1 \equiv (y_i g)^{k_1} (\bmod p)$,

$d_2^{x_i} \equiv [(gd_2)^{m} r_1^{-s_1}]^{r_1^{-1}} y_i^{-1} (\bmod p)$,

$r_2 \equiv d_2^{k_2} (\bmod p)$,

$m \equiv x_t + k_t s_t (\bmod \phi(p))$, t=1, 2.

The proxy signer Bob sends data {m, d_t, r_t, s_t} to the verifier R, t =1, 2.

(6) APS verification phase

The verifier R calculates

$y_i \equiv [g^{d_1} y_0^{-wd_2} d_2^{-cm}]^{d_2^{-1}} (\bmod p)$, then verifies

$(gd_2)^{m} \equiv [y_i (d_2^{m} r_2^{-s_2})^{r_2^{-1}}]^{r_1} r_1^{s_1} (\bmod p)$.

If the above equation is valid, then accept the message m, else reject.

VI. Correctness

Theorem

In the verification phase, the proxy signers can check whether the equation holds.

Proof.

$g^{d_1} \equiv (y_0^{w} y_i)^{d_2} d_2^{cM} (\bmod p)$,

$(gd_2)^{m} \equiv (y_i d_2^{x_i})^{r_1} r_1^{s_1} (\bmod p)$,

$d_2^{m} \equiv d_2^{x_i r_2} r_2^{s_2} (\bmod p)$, $\therefore$ We prove the theorem. Q. E. D.

V. Conclusion

In this study, we propose an effective period where an authorized person can provide authorization while commissioning a request, so that agents can only execute an agent signature at the appointed time without prior notice of permission to the authorized agents. The advantage of this proxy mechanism is in making the recipient able to verify, during proxy signature certification, that it is still within the commissioned time limit, to effectively prevent the abuse of agency authority by agents after the authorization period is over. In addition, the method as applied in the research [6] must have a hash function H(), while our method does not need a hash function. In information security research, the method designed in this study has a competitive advantage. In the post-PC era when the emphasis is on mobile information, the applied practice of using a time stamp [5] in computing devices has thus become relatively more simplified. Thus, designing a proxy signature mechanism for use within a limited bandwidth and equipment environment is an objective that we will continue pursue.

Reference

1. H. Bao, Z. Cao, S. Wang, “Improvement on Tzeng et al.'s nonrepudiable threshold multi-proxy multi-signature scheme with shared verification,” Appl. Math. Comput., pp. 1419-1430, 2005.
2. F. Cao, and Z. Cao, “A secure identity-based proxy multi-signature scheme, ”Information Sciences, pp.292–302, 2009.
3. D. Chaum, “Blind signatures for untraceable payments, ”Advances in Cryptology - Crypto '82, Springer-Verlag, pp.199-203, 1983.
4. J. J.-R. Chen and Y. Liu,2000, “A Traceable Group Signature Scheme,” Mathematical Computer Modelling, pp 147-160.
5. J. J.-R. Chen and Y. Liu, 2000, Vol. 15, No. 2, March, “An ID-based digital multisignatures scheme with time stamp technique,” International Journal of Computer systems Science & Engineering, pp.105-109.
6. J.-S. Chou , S.-C. Hung , and Y. Chen, “An Efficient Secure Anonymous Proxy Signature Scheme,” eprint/2011/498, 2011.
7. Y. F. Chung, Z. Y. Wu, and T. S. Chen, “Ring signature scheme for ECC-based anonymous signcryption, ”Computer Standards & Interfaces, pp.669-674, 2009.
8. C. L. Hsua, T. S. Wu, T. C. Wu, “Group-oriented signature scheme with distinguished signing authorities, ”Future Generation Computer Systems, pp.865–873, 2004.
9. J. H. Hu, and J. Z. Zhang, “Cryptanalysis and improvement of a threshold proxy signature scheme, ”Computer Standards & Interfaces, pp.169–173, 2009.
10. J. Li, Z. Cao, “An improvement of a threshold proxy signature scheme,” Comput. Res. Dev. 39 (11) pp. 1513-1518, 2002.
11. C. Y. Lin, T. C. Wu, F. Zhang, and J. J. Hwang, “New identity-based society oriented signature schemes from pairings on elliptic curves, ”Applied Mathematics and Computation, pp.245–260, 2005.
12. R. X. Lu, Z. F. Cao, and Y. Zhou, “Proxy blind multi-signature scheme without a secure channel, ”Applied Mathematics and Computation, pp.179–187, 2005.
13. H. F. Huang, and C. C. Chang, “A novel efficient (t, n) threshold proxy signature scheme, ”Information Sciences, pp.338–1349, 2006.
14. B. Kang, C. Boyd, and E. Dawson, “Identity-based strong designated verifier signature schemes: Attacks and new construction, ”Computers and Electrical Engineering, 2008.
15. S. Lal, V. Verma, “Identity base strong designated verifier proxy signature schemes, ”Cryptography eprint Archive Report 394, 2006.
16. Z. H. Liu, Y. P. Hu, X. S. Zhang, and H. Ma, “Secure proxy signature scheme with fast revocation in the standard model, ”The Journal of China Universities of 17 Posts and

Telecommunications, 16(4): 116–124, 2009.
17. Z. Liu, Y. Hu, X. Zhang, H. Ma, “Provably secure multi-proxy signature scheme with revocation in the standard model,” Computer Communications, pp. 494-501, 2011.
18. M. Mambo, K. Usuda, E. Okamoto, “Proxy signature: delegation of the power to sign messages, “IEICE Trans. Fundam. Volume E79-A(9), September, pp.1338–1354, 1996.
19. L. J. Mordell, Diophantine equations, Academic Press. ISBN 0-12-506250-8, 1969.
20. S. Saeednia, “An identity-based society oriented signature scheme with anonymous signers, ”Information Processing Letters, pp.295–299, 2002.
21. Z. Shao, “Certificate-based verifiably encrypted signatures from pairings, ” Information Sciences, pp.2360–2373, 2008.
22. Z. Shao, “Improvement of identity-based proxy multi-signature scheme, ”The Journal of Systems and Software , pp.794–800, 2009.
23. Y. Sun, C. Xu, Y. Yu, Y. Mu, “Strongly unforgeable proxy signature scheme secure in the standard model,”Journal of Systems and Software’, pp.1471-1479, 2011.
24. Y. Sun, C. Xu, Y. Yu, B. Yang, “Improvement of a proxy multi-signature scheme without random oracles,”Computer Communications , pp. 257-263, 2011.
25. L. J. Wang and J. J.-R. Chen, “Novel Digital Multisignature Scheme,” ICIC Express Letters, Vol. 4, No. 4, 2010, pp.1251-1255.
26. B. D. Wei, F. G. Zhang, and X. F. Chen, “ID-based Ring Proxy Signatures, ”ISIT2007, Nice, France, pp.24–29, 2007.
27. T. S. Wu, and H. Y Lin, “Efficient self-certified proxy CAE scheme and its variants, ”The Journal of Systems and Software, pp.974–980, 2009.
28. K. L. Wu, J. Zou, X. H. Wei, and F. Y. Liu, “Proxy group signature: a new anonymous proxy signature scheme, ”Proceedings of the Seventh International Conference on Machine Learning and Cybernetics, Kunming, pp.12-15, 2008.
29. H. Xiong, J. Hua, Z. Chen, F. Li, “On the security of an identity based multi-proxy signature scheme, ”Computers and Electrical Engineering’, pp. 129-135, 2011.
30. A. Yang, and W. P. Peng, “A Modified Anonymous Proxy Signature With a Trusted Party, ”First International Workshop on Education Technology and Computer Science, 2009.
31. C. H. Yang, S.F. Tzeng, M. S. Hwang, “On the efficiency of nonrepudiable threshold proxy signature scheme with known signers, ”Syst. Softw. 73 (3) pp.507–514, 2004.
32. Y. Yu, C. Xu, X. Huang, and Y. Mu, “An efficient anonymous proxy signature scheme with provable

security, "Computer Standards & Interfaces, pp.348–353, 2009.

33. Y. Yu, C. X. Xu, X. S. Zhang, and Y. J. Liao, "Designated verifier proxy signature scheme without random oracles, "Computers and Mathematics with Applications, pp.1352–1364, 2009.
34. J. Zhang, and J. Mao, "A novel ID-based designated verifier signature scheme, "Information Sciences, pp.766–773, 2008.
35. J. H. Zhang, C. L. Liu, and Y. I. Yang, "An efficient secure proxy verifiably encrypted signature scheme, "Journal of Network and Computer Applications, pp.29–34, 2010.