A Study of Security Schemes for Mobile Agent Based Networks

何健豪、曹偉駿

E-mail: 9222317@mail.dyu.edu.tw

ABSTRACT

A mobile agent is an autonomous software program, which can be executed in different agent platforms for a specific task on behalf of a customer. Furthermore, a mobile agent has the mobility to travel from one host to another in the world of network systems. Besides, mobile agent technology is suitable for reducing the computational overhead of a local host and providing low cost of communications. Thus, the characteristics of mobile agents, autonomy and mobility, make them ideal for e-commerce applications. In the past few years, e-commerce has become flourishing and rising in most enterprises. The benefit of employing the mobile agent technology in the enterprises allows deployment of e-commerce services in a more flexible and customizable way. Moreover, it improves the competitive advantages and the efficiency of organizational operations. However, the explosion of e-commerce is forcing businesses and customers to focus on developing a secure transaction environment on Internet. Therefore, the security is one of the key issues for mobile agent technology while the mobile agents are applied to the developments of e-commerce. In order to protect the security of transactions in e-commerce, this thesis proposed an appropriate public key cryptosystem for the mobile agent based networks. The proposed cryptosystem is constructed by using the pairing-based cryptosystems, and is developed by integrating the identity-based public key cryptosystems with the self-certified public key cryptosystems. In addition, we further employ the integrated cryptosystems to design several security schemes for the mobile agent based networks. As far as mobile agent security is concerned, we devise a new proxy signature scheme, undetachable proxy signature, which is combined with the advantages of undetachable signature and proxy signature to protect mobile agents. We also develop a proxy authenticated encryption scheme to satisfy the basic security requirements of confidentiality, integrity, authenticity, and non-repudiation for mobile agents. As far as agent platform security is concerned, we apply the idea of proxy signature to construct a single sign-on (SSO) scheme for agent platforms. This scheme is based on the proposed cryptosystem to achieve the requirements of authentication and authorization. In summary, the proposed security schemes can make the mobile agent environments securely workable.

Keywords : mobile agent, proxy signature, authenticated encryption scheme, single sign-on, self-certified public key cryptosystems, pairing-based cryptosystems

Table of Contents

Chapter I. Introduction.............................. 1 1.1 Research Background.............................. 1 1.2 Research Motivation.............................. 4 1.3 Research Purpose.............................. 8 1.4 Research Procedure.............................. 10 1.5 Thesis Organization.............................. 13 Chapter II. Previous Works.............................14 2.1 Undetachable Signature.............................14 2.1.1 RSA-Based Undetachable Signature.................16 2.2 Proxy Signature.............................. 18 2.2.1 Proxy-Protected Proxy Signature..................19 2.2.2 Requirements of Proxy Signature..................21 2.2.3 Problems of Impersonation........................22 2.3 Authenticated Encryption Scheme....................23 2.4 Single Sign-On (SSO).............................. 24 2.5 Public Key Cryptosystems...........................26 2.5.1 Certificate-Based Public Key Cryptosystems........27 2.5.2 Identity-Based Public Key Cryptosystems.......... 28 2.5.3 Self-Certified Public Key Cryptosystems.......... 28 2.6 Elliptic Curve Theory and Its Applications......... 29 2.6.1 ECDLP.. 31 2.6.2 Weil Descent.............................. 33 2.6.3 MOV Attack.............................. 34 2.6.4 Bilinear Pairings.............................. 34 2.6.5 The BDH Assumption.............................. 38 2.6.6 IDPKC from Pairings............................ 39 Chapter III. Security Schemes for Mobile Agent Based Networks 3.1 Initialization.................................... 42 3.2 The Proposed Public Key Cryptosystems..............43 3.3 Undetachable Proxy Signature Scheme................45 3.4 Proxy Authenticated Encryption Scheme..............48 3.5 Single Sign-On Scheme..............................52 Chapter IV. Security Analyses and Performance Evaluation....57 4.1 Security Analyses 57 4.1.1 Security Consideration for Pairings..............57 4.1.2 Security of the Proposed PKC.....................58 4.1.3 Possible Attacks for Related Security Schemes.....60 4.1.4 Security Issues Related to Mobile Agents..........65 4.2 Performance Evaluation.............................67 Chapter V. Conclusions.............................. 74 Bibliography..76 Curriculum Vitae.......................................84

REFERENCES

[1] Paulo S. L. M. Barreto, H. Y. Kim, B. Lynn, and M. Scott, "Efficient Algorithms for Pairing-Based Cryptosystems," Advances in Cryptology - CRYPTO 2002, Lecture Notes in Computer Science, Vol. 2442, Springer-Verlag, pp. 354-368, 2002.

[2] S. Berkovits, J. D. Guttman, and V. Swarup, "Authentication for Mobile Agents," Mobile Agents and Security, Lecture Notes in Computer Science, Vol. 1419, Springer-Verlag, pp. 114-136, 1998.

[3] I. F. Blake, G. Seroussi, and N. P. Smart, Elliptic Curves in Cryptography, London Mathematical Society Lecture Note Series, Vol. 265, Cambridge University Press, 1999.

[4] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," Advances in Cryptology - CRYPTO 2001, Lecture Notes in Computer Science, Vol. 2139, Springer-Verlag, pp. 213-229, 2001.

[5] D. Boneh, B. Lynn, and H. Shacham, "Short Signatures from the Weil Pairing," Advances in Cryptology - ASIACRYPT 2001, Lecture Notes in Computer Science, Vol. 2248, Springer-Verlag, pp. 514-532, 2001.

[6] N. Borselius, C. J. Mitchell, and A. T. Wilson, "A pragmatic alternative to undetachable signatures", ACM Special Interest Group on Operating Systems, SIGOPS, Operating Systems Review, Vo. 36, No. 2, pp. 6-11, 2002.

[7] A. Caglayan and C. Harrison, Agent Sourcebook: A Complete Guide to Desktop, Internet, and Intranet Agents, John Wiley & Sons, Inc., 1997.

[8] D. M. Chess, "Security Issues in Mobile Code Systems," Mobile Agents and Security, Lecture Notes in Computer Science, Vol. 1419, Springer-Verlag, pp. 1-14, 1998.

[9] D. M. Chess, B. Grosof, C. G. Harrison, D. Levine, C. Parris, and G. Tsudik, "Itinerant Agents for Mobile Computing," IEEE Personal Communications Magazine, Vol. 2, No. 5, pp. 34-49, 1995.

[10] H. Y. Chien, "New Approach to Authorization and Authentication in Distributed Environments," Communications of the CCISA, Vol. 9, No. 3, pp.63-69, 2003.

[11] D. Coppersmith, J. Stern, and S. Vaudenay, "Attacks on the Birational Permutation Signature Schemes," Advances in Cryptology - CRYPTO '93, Lecture Notes in Computer Science, Vol. 773, Springer-Verlag, pp. 435-443, 1993.

[12] W. Diffie and M. E. Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory, Vol. IT-22, pp. 644-654, 1976.

[13] T. ElGamal, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Transactions on Information Theory, Vol. IT-31, No. 4, pp. 469-472, 1985.

[14] W. M. Farmer, J. D. Gutmann, and V. Swarup, "Security for Mobile Agents: Authentication and State Appraisal", Proceedings of the European Symposium on Research in Computer Security, ESORICS, Lecture Notes in Computer Science, Vol. 1146, Spring-Verlag, pp. 118-130, 1996.

[15] G. Frey, M. Muller, and H. G. Ruck, "The Tate Pairing and the Discrete Logarithm Applied to Elliptic Curve Cryptosystems," IEEE Transactions on Information Theory, Vol. 45 No. 5, pp. 1717-1719, 1999.

[16] G. Frey and H. G. Ruck, "A Remark Concerning m-Divisibility and the Discrete Logarithm in the Divisor Class Group of Curves," Mathematics of Computation, Vol. 62, No. 206, pp. 865-874, 1994.

[17] S. D. Galbraith, "Supersingular Curves in Cryptography," Advances in Cryptology - ASIACRYPT 2001, Lecture Notes in Computer Science, Vol. 2248, Springer-Verlag, pp. 495-513, 2001.

[18] S. D. Galbraith, K. Harrison, and D. Soldera, "Implementing the Tate pairing," Algorithmic Number Theory Symposium, ANTS-V, Lecture Notes in Computer Science, Vol. 2369, Springer-Verlag, pp. 324-337, 2002.

[19] M. Girault, "Self-Certified Public Keys", Advances in Cryptology - EUROCRYPT '91, Springer-Verlag, pp. 491-497, 1991.

[20] W. H. He and T. C. Wu, "Cryptanalysis and Improvement of Petersen-Michels Signcryption Scheme," IEE Proceedings - Computer and Digital Techniques, Vol.146, No. 2, pp.123-124, 1999.

[21] F. Hohl, "Time Limited Blackbox Security: Protecting Mobile Agents form Malicious Hosts," Mobile Agents and Security, Lecture Notes in Computer Science, Vol. 1419, Springer-Verlag, pp. 92-113, 1998.

[22] Chien-Lung Hsu, Authenticated Encryption Schemes for Group Oriented Applications, Ph.D dissertation, National Taiwan University of Science and Technology, Taiwan, 2002.

[23] M. S. Hwang, "A remote password authentication scheme based on the digital signature method," International Journal of Computer Mathematics, Vol. 70, pp. 657-666, 1998.

[24] M. S. Hwang, C. C. Lee, and Y. L. Tang, "A Simple Remote User Authentication Scheme," Mathematical and Computer Modelling, Vol. 36, pp. 103-107, 2002.

[25] A. Joux, "A One-Round Protocol for Tripartite Diffie-Hellman," Algorithm Number Theory Symposium, ANTS-IV, Lecture Notes in Computer Science, Vol. 1838, Springer-Verlag, pp. 385-394, 2000.

[26] A. Jurisic and A. J. Menezes, "Elliptic Curves and Cryptography", Dr. Dobb's Journal, pp. 26-35, 1997.

[27] H. Kim, J. Baek, B. Lee, and K. Kim, "Secret Computation with Secrets for Mobile Agent using One-Time Proxy Signature," Proceedings of Symposium on Cryptography and Information Security, SCIS 2001, pp. 845-850, 2001.

[28] S. Kim, S. Park, and D. Won, "Proxy Signatures, Revisited," Proceedings of International Conference on Information and Communications Security, ICICS '97, Lecture Notes in Computer Science, Vol. 1334, Springer-Verlag, pp. 223-232, 1997.

[29] N. Koblitz, "Elliptic Curve Cryptosystems", Mathematics of Computation, Vol. 48, No. 17, pp. 203-209, 1987.
[30] P. Kotzanikolaou, M. Burmester, and V. Chrissikopoulos, "Secure Transactions with Mobile Agents in Hostile Environments," Proceedings of the Fifth Australasian Conference on Information Security and Privacy, ACISP 2000, Lecture Notes in Computer Science, Vol. 1841, Springer-Verlag, pp. 289-297, 2000.
[31] L. Lamport, "Password Authentication with Insecure Communication," Communications of the ACM, Vol. 24, No. 11, pp. 770-772, 1981.
[32] B. Lee, H. Kim, and K. Kim, "Secure Mobile Agent Using Strong Non-designated Proxy Signature", Proceedings of the Sixth Australasian Conference on Information Security and Privacy, ACISP 2001, Lecture Notes in Computer Science, Springer-Verlag, 2001.
[33] I. C. Lin, M. S. Hwang, and L. H. Li, "A New Remote User Authentication Scheme for Multi-Server Architecture," Future Generation Computer Systems, Vol. 19, No. 1, pp. 13-22, 2003.
[34] I. C. Lin, H. H. Ou, and M. S. Hwang, "Two Secure Transportation Schemes for Mobile Agents," Information and Security, Vol. 8, No. 1, pp. 87-97, 2002.
[35] P. Maes, R. Guttman, and A. Moukas, "Agents That Buy and Sell," Communications of the ACM, Vol. 42, pp. 81-91, 1999.
[36] M. Mambo, K. Usuda, and E. Okamoto, "Proxy Signatures: Delegation of the Power to Sign Messages," IEICE Transactions on Fundamentals, Vol. E79-A, No. 9, pp. 1338-1354, 1996.
[37] M. Mambo, K. Usuda, and E. Okamoto, "Proxy Signatures for Delegating Signing Operation," Proceedings of the Third ACM Conference on Computer and Communications Security, ACM press, pp.48-57, 1996.
[38] A. J. Menezes, T. Okamoto, and S. Vanstone, "Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field," IEEE Transactions on Information Theory, Vol. 39, pp. 1639-1646, 1993.
[39] A. J. Menezes and S. A. Vanstone, "Elliptic Curve Cryptosystem and Their Implementation," Journal of Cryptology, Vol. 6, No. 4, pp. 209-224, 1993.
[40] V. S. Miller, "Use of Elliptic Curves in Cryptography," Advances in Cryptology - CRYPTO '85, Lecture Notes in Computer Science, Vol. 218, Springer-Verlag, pp. 417-426, 1985.
[41] H. Petersen and P. Horster, "Self-Certified Keys: Concepts and Applications", Proceedings of Communications and Multimedia Security '97, Chapman & Hall, pp. 102-116, 1997.
[42] R. L. Rivest, A. Shamir, and L. M. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, Vol. 21, No. 2, pp. 120-126, 1978.
[43] S. Saeednia, "Identity-Based and Self-Certified Key Exchange Protocols," Proceedings of the Second Australasian Conference on Information Security and Privacy, ACISP '97, Lecture Notes in Computer Science, Springer-Verlag, pp. 303-313, 1997.
[44] R. Sakai, K. Ohgishi, and M. Kasahara, "Cryptosystems Based on Pairing," Proceedings of Symposium on Cryptography and Information Security, SCIS 2000, 2000.
[45] H. Sakazaki, E. Okamoto, and M. Mambo, "Constructing Identity-Based Key Distribution Systems over Elliptic Curves", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E81-A, No.10, pp. 2138-2143, 1998.
[46] T. Sander and C. F. Tschudin, "Protecting Mobile Agents Against Malicious Hosts," Mobile Agents and Security, Lecture Notes in Computer Science, Vol. 1419, Springer-Verlag, pp. 44-60, 1998.
[47] T. Sander and C. F. Tschudin, "Towards Mobile Cryptography", Proceedings of 1998 IEEE Symposium on Security and Privacy, pp. 215-224, 1998.
[48] C. P. Schnorr, "Efficient Identification and Signatures for Smart Cards," Advances in Cryptology - CRYPTO '89, Lecture Notes in Computer Science, Vol. 435, Springer-Verlag, pp. 239-252, 1989.
[49] C. P. Schnorr, "Efficient Signature Generation by Smart Cards," Journal of Cryptology, Vol. 4, No. 3, pp. 161-174, 1991.
[50] A. Shamir, "Efficient Signature Schemes Based on Birational Premutations," Advances in Cryptology - CRYPTO '93, Lecture Notes in Computer Science, Vol. 773, Springer-Verlag, pp. 1-12, 1993.
[51] A. Shamir, "Identity Based on Cryptosystems and Signature Schemes," Advances in Cryptology - CRYPTO '84, Lecture Notes in Computer Science, Vol. 196, Springer-Verlag, pp. 47-53, 1984.
[52] J. H. Silverman, The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, Vol. 106, Springer-Verlag, 1986.
[53] N. P. Smart, "An Identity Based Authenticated Key Agreement Protocol Based on the Weil Pairing," Electronics Letters, Vol. 38, pp. 630-632, 2002.
[54] H. M. Sun, "On Proxy Multi-Signature Schemes," Proceedings of the International Computer Symposium, ICS 2000, pp.65-72, 2000.
[55] H. Takeda, K. Iino, and T. Nishida, "Agent Organization and Communication with Multiple Ontologies," International Journal of Cooperative Information Systems, Vol. 4, No. 4, pp.312-337, 1995.
[56] J. E. White, "Mobile Agents Make a Network an Open Platform for Third-Party Developers," IEEE Computer, Vol. 27, No. 11, pp. 89-90, 1994.
[57] T. C. Wu, Y. S. Chang, and T. Y. Lin, "Improvement of Saeednia's Self-Certified Key Exchange Protocols," IEE Electronic Letters, Vol. 34, No 11, pp. 1094-1095, 1998.

[58] T. S. Wu and C. L. Hsu, "Convertible Authenticated Encryption Scheme," Journal of Systems and Software, Vol. 62, No. 3, pp. 205-209, 2002.
[59] L. Yi, G. Bai, and G. Xiao, "Proxy Multi-Signature Scheme: A New Type of Proxy Signature Scheme," Electronics Letters, Vol. 36, No. 6, pp.527-528, 2000.
[60] X. Yi and C. K. Siew, "Secure Agent-Mediated Online Auction Framework," International Journal of Information Technology, Vol. 7, No. 1, 2001.
[61] F. Zhang and K. Kim, "ID-Based Blind Signature and Ring Signature from Pairings," Advances in Cryptology - ASIACRYPT 2002, Lecture Notes in Computer Science, Vol. 2501, Springer-Verlag, pp. 533-547, 2002.