IIM > Vol.2 No.4, April 2010

OPEN ACCESS

# A Collusion-Resistant Distributed Agent-Based Signature Delegation (CDASD) Protocol for E-Commerce Applications

PDF (Size:325KB) PP. 262-277 DOI: 10.4236/iim.2010.23031

Author(s)
Omaima Bamasak

ABSTRACT
Mobile agent technology is promising for e-commerce and distributed computing applications due to its properties of mobility and autonomy. One of the most security-sensitive tasks a mobile agent is expected to perform is signing digital signatures on a remote untrustworthy service host that is beyond the control of the agent host. This service host may treat the mobile agents unfairly, i.e. according to its ' own benefit rather than to their time of arrival. In this research, we present a novel protocol, called Collusion-Resistant Distributed Agent-based Signature Delegation (CDASD) protocol, to allow an agent host to delegate its signing power to an anonymous mobile agent in such a way that the mobile agent does not reveal any information about its host ' s identity and, at the same time, can be authenticated by the service host, hence, ensuring fairness of service provision. The protocol introduces a verification server to verify the signature generated by the mobile agent in such a way that even if colluding with the service host, both parties will not get more information than what they already have. The protocol incorporates three methods: Agent Signature Key Generation method, Agent Signature Generation method, Agent Signature Verification method. The most notable feature of the protocol is that, in addition to allowing secure and anonymous signature delegation, it enables tracking of malicious mobile agents when a service host is attacked. The security properties of the proposed protocol are analyzed, and the protocol is compared with the most related work.

KEYWORDS
Agent-Based Signature Delegation, Anonymous Digital Signature, Signature Fairness, Collusion-Resistant Signature

Cite this paper
O. Bamasak, "A Collusion-Resistant Distributed Agent-Based Signature Delegation (CDASD) Protocol for E-Commerce Applications," *Intelligent Information Management*, Vol. 2 No. 4, 2010, pp. 262-277. doi: 10.4236/iim.2010.23031.

References

[1] A. Asokan, V. Shoup and M. Waidner, " Optimistic Fair Exchange of Digital Signatures, " IEEE Journal on Selected Areas in Communication, Vol. 18, 2000, pp. 591-610.

[2] O. Bamasak, " Delegating Signing Power to Mobile Agents: Algorithms and Protocol Design, " PhD Thesis, School of Computer Science, the University of Manchester, UK, 2006.

[3] F. Bao, R. H. Deng and W. Mao, " Efficient and Practical Fair Exchange Protocols with Off-Line TTP, " Proceedings of the IEEE Symposium on Security and Privacy, 1998, pp. 77-85.

[4] M. Blum, " How to Exchange (Secret) Keys, " ACM Transactions on Computer Systems, Vol. 1, No. 2, 1983, pp. 175-193.

[5] C. Boyd and E. Foo, " Off-Line Fair Payment Protocols Using Convertible Signature, " Advances in Cryptology -Proceedings of Asiacrypt ' 98, Lecture Notes in Computer Science 1514, 1998, pp. 271-285.

[6] L. Chen, " Efficient Fair Exchange with Verifiable Confirmation of Signatures, " Advances in

• Open Special Issues
• Published Special Issues
• Special Issues Guideline

IIM Subscription

Most popular papers in IIM

About IIM News

Frequently Asked Questions

Recommend to Peers

Recommend to Library

Contact Us

Cryptology-Proceedings of Asiacrypt ' 98, Lecture Notes in Computer Science 1514, 1998, pp. 286-299.

[7] R. H. Deng, L. Gong, A. A. Lazar and W. Wang, "Practical Protocol for Certified Electronic Mail," Journal of Network and System Management, Vol. 4, No. 3, 1996, pp. 279-297.

[8] S. Even, O. Golreich and A. Lempel, "Randomized Protocol for Signing Contracts," Communications of the ACM, Vol. 28, No. 6, 1985, pp. 637-647.

[9] M. K. Franklin and M. K. Reiter, "Verifiable Signature Sharing," Advances in Cryptology-Proceedings of Eurocrypt ' 95, Lecture Notes in Computer Science 921, 1995, pp. 50-63.

[10] J. A. Garay, M. Jakobsson and P. MacKenzie, "Abuse- Free Optimistic Contract Signing," Advances in Cryptology-Proceedings of Crypto ' 99, Lecture Notes in Computer Science 1666, 1999, pp. 449-466.

[11] M. Jakobsson, K. Sako and R. Impagliazzo, "Designated Verifier Proofs and their Applications," Advances in Cryptology-Proceedings of Eurocrypt ' 96, Lecture Notes in Computer Science 1070, 1996.

[12] T. Okamoto and K. Ohta, "How to Simultaneously Exchange Secrets by General Assumptions," Proceedings of the 2nd ACM Conference on Computer and Communications Security, 1994, pp. 184-192.

[13] C. Wang and C. Yin, "Practical Implementations of a Non-disclosure Fair Contract Signing Protocol," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science, Vol. E89-A, No. 1, 2006, pp. 297-309.

[14] J. Zhou and D. Gollmann, "A Fair Non-Repudiation Protocol," Proceedings of 1996 IEEE Symposium on Security and Privacy, 1996, pp. 55-61.

[15] J. Zhou and D. Gollmann, "An Efficient Non-Repudiation Protocol," Proceedings of 1997 IEEE Computer Security Foundations Workshop (CSFW 10), 1997, pp. 126-132.

[16] M. Lin, C. Chang and Y. Chen, "A Fair and Secure Mobile Agent Environment Based on Blind Signature and Proxy Host," Computers & Security, Vol. 23, 2004, pp. 199-212.

[17] D. Chaum, "Blind Signatures for Untraceable Payments," Proceedings of CRYPTO ' 82, 1983, pp. 199-203.

[18] J. Kim, G. Kim and Y. Eom, "Design of the Mobile Agent Anonymity Framework in Ubiquitous Computing Environments," IEICE Transactions on Information and Systems, Vol. E89-D, No. 12, 2006, pp. 2990-2993.

[19] R. L. Rivest, A. Shamir and L. M. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Communication of Association for Computing Machinery, Vol. 21, No. 2, 1978, pp. 120-126.

[20] National Institute of Standard and Technology (NIST), Secure Hash Standard, Federal Information Processing Standards Publication (FIPS 180-1).

[21] M. Fowler, "UML Distilled: A Brief Guide to the Standard Object Modeling Language," 3rd Edition, The Addison-Wesley Professional, 2003.

[22] U. Wilhelm, "Cryptographically Protected Objects," Technical Report, Ecole Polytechnique Federale de Lausanne, Switzerland, 1997.

[23] F. Hohl, "Time Limited Blackbox Security: Protecting Mobile Agents from malicious Hosts," Mobile Agents and Security, Lecture Notes in Computer Science, Vol. 1419, 1998, pp. 92-113.

[24] S. Kremer and J. Raskin, "A Game-Based Verification of Non-Repudiation and Fair Exchange Protocols," Proceedings of the 12th International Conference on Concurrency Theory, Lecture Notes in Computer Science, Vol. 2154, 2001, pp. 551-566.

[25] S. Kremer and J. Raskin, "Game Analysis of Abuse-Free Contract Signing," Proceedings of the 15th IEEE Computer Security Foundations Workshop, 2002, pp. 206-220.

[26] "Grasshopper Mobile Agent Platform." http://www.grasshopper.de.

[27] M. Mambo, K. Usuda, and E. Okamoto, "Proxy Signatures for Delegating Signing Operation," Proceedings of the 3rd ACM Conference on Computers and Communications Security, 1996, pp. 48-57.

[28] N. Borselius, C. Mitchell and A. Wilson, "A Pragmatic Alternative to Undetachable Signatures," ACM SIGOPS Operating Systems Review, Vol. 36, No. 2, 2002, pp. 6-11.

[29] A. Romao and M. Silva, "Secure Mobile Agent Digital Signatures with Proxy Certificates," E-Commerce Agents, Marketplace Solutions, Security Issues, and Supply and demand, Lecture Notes in Computer Science, Vol. 2033, 2001, pp. 206-220.

[30] B. Lee, H. Kim, J. Baek and K. Kim, "Secure Mobile Agent Using Strong Non-designated Proxy Signature," Proceedings of the 6th Australian Conference on Information Security and Privacy, Lecture Notes in Computer Science, Vol. 2119, 2001, pp. 474-486.

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

[32] K. Zhang, "Threshold Proxy Signature Schemes," Proceedings of Information Security Workshop, Lecture Notes in Computer Science, Vol. 1396, 1997, pp. 282-290.

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

[34] K. Shum and V. Wei, "A Strong Proxy Signature Scheme With Proxy Signer Privacy Protection," Proceedings of the 11th IEEE International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, 2002, pp. 55-56.

[35] J. Herranz and G. Saez, "Fully Distributed Proxy Signature Schemes," Cryptology ePrint Archive, 2002. http:// eprint.iacr.org/2002/051.

[36] H. Wang and J. Pieprzyk, "Efficient One-Time Proxy Signatures," Proceedings of ASIACRYPT, Lecture Notes in Computer Science, Vol. 2894, 2003, pp. 507-522.

[37] Y. Yong, C. Xu, X. Huang and Y. Mu, "An Efficient Anonymous Proxy Signature Scheme with Provable Security," Computer Standards & Interfaces, Vol. 31, No. 2, 2009, pp. 348-353.

[38] Z. Shao, "Provably Secure Proxy-Protected Signature Schemes Based on RSA," Computers and Electrical Engineering, Vol. 35, No. 3, 2009, pp. 497-505.