An Efficient and Secure Communication Scheme for Trusted Computing Environments

Chun-Ta Li*

Department of Information Management
Tainan University of Technology
Tainan 710, Taiwan, ROC
th0040@mail.tut.edu.tw

Received 13 July 2009; Revised 19 August 2009; Accepted 8 September 2009

Abstract. Trusted computing and communications have gradually become an important part of e-business and e-government, including various distributed systems, network applications, and computer resources. The concept of trusted computing is to prevent damages by software and/or hardware attacks on the PC platform. As network-based and resource-constricted environments become more and more popular, in this paper, it is imperative to design secure and lightweight communication schemes to resist all possible attacks and threats. We integrated the concept of one-time signature and hash-chain into the scheme and thus the network-based communications can resist all the possible attacks and provide good security properties such as unforgeability and verifiability.

Keywords: hash chain, one-time signature, security, trusted computing and communications

References

[1] M. Crosbie, "Trusted Computing – Closing that Lingering Doubt," *Network Security*, Vol. 2006, No. 6, pp. 13-15, 2006.

[2] T. Garfinkel, B. Pfaff, J. Chow, M. Rosenblum, D. Boneh, "Terra: A Virtual Machine-based Platform for Trusted Computing," *ACM SIGOPS Operating Systems Review*, Vol. 37, No. 5, pp. 193-206, 2003.

[3] R. Oppliger and R. Rytz, "Does Trusted Computing Remedy Computer Security Problems?," *Security & Privacy*, Vol. 3, No. 2, pp. 16-19, 2005.

[4] D. Safford and M. Zohar, "Trusted Computing and Open Source," *Information Security Technical Report*, Vol. 10, No. 2, pp. 74-82, 2005.

[5] B. Gengler, "Trusted Computing Platform Alliance," *Network Security*, Vol. 2001, No. 3, pp. 6, 2001.

[6] R. Anderson, "Cryptography and Competition Policy – Issues with Trusted Computing," *Proceedings of the 22nd Annual Symposium on Principles of Distributed Computing*, pp. 3-10, 2003.

[7] S. Schoen, "Compatibility, Competition, and Control in Trusted Computing Environments," *Information Security Technical Report*, Vol. 10, No. 2, pp. 105-119, 2005.

[8] C. Jin, J. Liu, Q. Deng, "Network Virus Propagation Model Based on Effects of Removing Time and User Vigilance," *International Journal of Network Security*, Vol. 9, No. 2, pp. 156-163, 2009.

[9] H. C. Liao and Y. H. Wang, "A Memory Symptom-based Virus Detection Approach," *International Journal of Network Security*, Vol. 2, No. 3, pp. 219-227, 2006.

[10] T. Bhaskar, N. Kamath B, S. D. Moitra, "A Hybrid Model for Network Security Systems: Integrating Intrusion Detection System with Survivability," *International Journal of Network Security*, Vol. 7, No. 2, pp. 249-260, 2008.

* Correspondence author

[11] S. S. Kandeeban and R. S. Rajesh, "Integrated Intrusion Detection System Using Soft Computing," *International Journal of Network Security*, Vol. 10, No. 2, pp. 87-92, 2010.

[12] A. Mitrokotsa, N. Komninos, C. Douligeris, "Protection of an Intrusion Detection Engine with Watermarking in Ad Hoc Networks," *International Journal of Network Security*, Vol. 10, No. 2, pp. 93-106, 2010.

[13] J. Zeng and D. Guo, "Agent-based Intrusion Detection for Network-based Application," *International Journal of Network Security*, Vol. 8, No. 3, pp. 201-210, 2009.

[14] C. T. Li, C. H. Wei, Y. H. Chin, "A Secure Event Update Protocol for Peer-To-Peer Massively Multiplayer Online Games Against Masquerade Attacks," *International Journal of Innovative Computing, Information and Control*, article in press, 2009.

[15] C. H. Wei, Y. H. Chin, C. T. Li, "A Secure Billing Protocol for Grid Computing," *Proceedings of 2009 International Conference on Information Technology: New Generations*, Las Vegas, USA, pp. 320-325, April 2009.

[16] F. Dressler, "Authenticated Reliable and Semi-reliable Communication in Wireless Sensor Networks," *International Journal of Network Security*, Vol. 7, No. 1, pp. 61-68, 2008.

[17] C. T. Li and Y. P. Chu, "Cryptanalysis of Threshold Password Authentication Against Guessing Attacks in Ad Hoc Networks," *International Journal of Network Security*, Vol. 8, No. 2, pp. 166-168, 2009.

[18] C. T. Li, M. S. Hwang, Y. P. Chu, "Further Improvement on A Novel Privacy Preserving Authentication and Access Control Scheme for Pervasive Computing Environments," *Computer Communications*, Vol. 31, No. 18, pp. 4255-4258, 2008.

[19] M. L. Das, A. Saxena, D. B. Phatak, "Algorithms and Approaches of Proxy Signature: A Survey," *International Journal of Network Security*, Vol. 9, No. 3, pp. 264-284, 2009.

[20] M. H. Ibrahim, "Efficient Dealer-Less Threshold Sharing of Standard RSA," *International Journal of Network Security*, Vol. 8, No. 2, pp. 139-150, 2009.

[21] Y. Ming and Y. Wang, "An Efficient Verifiably Encrypted Signature Scheme without Random Oracles," *International Journal of Network Security*, Vol. 8, No. 2, pp. 125-130, 2009.

[22] H. H. Ngo, X. Wu, P. D. Le, C. Wilson, B. Srinivasan, "Dynamic Key Cryptography and Applications," *International Journal of Network Security*, Vol. 10, No. 3, pp. 161-174, 2010.

[23] H. Xiong, Z. Qin, F. Li, "Identity-based Threshold Signature Secure in the Standard Model," *International Journal of Network Security*, Vol.10, No. 1, pp. 75-80, 2010.

[24] C. T. Li, M. S. Hwang, Y. P. Chu, "A Secure and Efficient Communication Scheme with Authenticated Key Establishment and Privacy Preserving for Vehicular Ad Hoc Networks," *Computer Communications*, Vol. 31, No. 12, pp. 2803-2814, 2008.

[25] C. T. Li, M. S. Hwang, C. Y. Liu, "An Electronic Voting Protocol with Deniable Authentication for Mobile Ad Hoc Networks," *Computer Communications*, Vol. 31, No. 10, pp. 2534-2540, 2008.

[27] C. T. Li, M. S. Hwang, Y. P. Chu, "Improving the Security of A Secure Anonymous Routing Protocol with Authenticated Key Exchange for Ad Hoc Networks," *International Journal of Computer Systems Science and Engineering*, Vol. 23, No. 3, pp. 227-234, 2008.

[26] C. T. Li, M. S. Hwang, Y. P. Chu, "An Efficient Sensor-To-Sensor Authenticated Path-Key Establishment Scheme for Secure Communications in Wireless Sensor Networks," *International Journal of Innovative Computing, Information and Control*, Vol. 5, No. 8, pp. 2107-2124, 2009.

[28] C. T. Li, "An Enhanced Remote User Authentication Scheme Providing Mutual Authentication and Key Agreement with Smart Cards," *Proceedings of 2009 International Conference on Information Assurance and Security*, Xi'an, China, pp. 517-520, August 2009.