Using Proxy Signature for Dynamic Delegation in Grids

Chi-Tung Chen[1], Ming-Tsun Lin[2], and Iuon-Chang Lin[3,*]

[1] Department of Distribution Management
National Chin-Yi University of Technology
Taichung, Taiwan
chi9695@ncut.edu.tw

[2] Department of Computer Science and Information Engineering
Asia University
Taichung, Taiwan
g96241006@ms1.asia.edu.tw

[3] Department of Management Information Systems
National Chung Hsing University
Taichung, Taiwan
iclin@nchu.edu.tw

Received 10 July 2009; Revised 15 August 2009; Accepted 5 September 2009

Abstract. GSI (Grid Security Infrastructure) was used proxy certificate for delegation in grid environment. However, the proxy certificate holder can not issue his own identity, not to prove that he is a known entity. Therefore, it can not satisfy the requirements of nonrepudiation and known signer in grids. In this paper, we propose a dynamic delegation scheme for grids using proxy signature. Our scheme can satisfy all the requirements of delegation.

Keywords: grid computing security, proxy signature, dynamic delegation

References

[1] A. S. Grimshaw, A. S. Humphrey, A. Natrajan, “A Philosophical and Technical Comparison of Legion and Globus,” *IBM Journal of Research & Development*, Vol. 48, pp. 233 - 254, March 2004.

[2] E. Cody, R. Sharman, R. H. Rao, S. Upadhyaya, “Security in Grid Computing: A Review and Synthesis,” *Decision Support Systems*, Vol. 44, pp. 749-764, March 2008.

[3] Y. S. Dai, M. Xie, K. L. Poh, “Reliability Analysis of Grid Computing Systems,” *Proceedings of Pacific Rim International Symposium on Dependable Computing*, Tsukuba-City, Ibarski, Japan, pp. 97-104, December 2002.

[4] I. Foster and C. Kesselman, *The Grid: Blueprint for a New Computing Infrastructure*. USA: Morgan Kaufmann, 1999.

[5] I. Foster, C. Kesselman, S. Tuecke, “The Anatomy of the Grid: Enabling Scalable Virtual Organizations,” International *Journal of High Performance Computing*, Vol. 15, No. 3, pp. 200-222, 2001.

[6] H. W. Lim. “On the Application of Identity-based Cryptography in Grid Security,” *PhD Thesis*, London University, 2006.

[7] R. Al-Khannak and B. Bitzer, “Load Balancing for Distributed and Integrated Power Systems using Grid Computing,” *Proceedings of International Conference on Clean Electrical Power*, Capri, Italy, pp. 123-127, May 2007.

[8] S. Bagchi, “Simulation of Grid Computing Infrastructure: Challenges and Solutions,” *Proceedings of Winter Simulation Conference*, Orlando, FL, U.S.A, pp. 1773-1780., December 2005.

[*] Correspondence author

[9] M. S. Hwang, J. L. Lu, I. C. Lin, “A Practical (t, n) Threshold Proxy Signature Scheme based on the RSA Cryptosystem,” *IEEE Transactions on Knowledge and Data Engineering*, Vol. 15, No. 6, pp. 1552-1560, 2003.

[10] S. H. Kim and S. Jin, “Grid ID Management based on Distributed Agents using SPML,” *Proceedings of 2006 IEEE International Symposium on Consumer Electronics (ISCE)* , St. Petersburg, Russia, pp. 1-6, June 2006.

[11] Q. Zeng, C. EIuang, D. Chen, H. Hu, “Supporting Secure Collaborative Computing in Grid Environments,” *Proceedings of Computer Supported Cooperative Work in Design*, Xiamen, China, pp. 413-418, May 2004.

[12] M. L. Bote-Lorenzo, Y. A. Dimitriadis, E. Gomez-Sanchez, “Grid Characteristics and Uses: A Grid Definition,” *Proceedings of the First European Across Grids Conference*, Santiago de Compostela, Spain, pp. 291-298, February 2003.

[13] D. F. Snelling, S. van den Berghe, V. Q. Li, “Explicit Trust Delegation: Security for Dynamic Grids,” *Fujitsu Scientific & Technical Journal*, Vol. 40, pp. 282-294, December 2004.

[14] M. Humphrey, M. R. Thompson, K. R. Jackson, “Security for Grids,” *Proceedings of the IEEE*, Vol. 93, No.3, pp. 644-652, February 2005.

[15] A. Chakrabarti, A. Damodaran, S. Sengupta, “Grid Computing Security: A Taxonomy,” *IEEE Security & Privacy*, Vol. 6, No. 1, pp. 44-51, 2008.

[16] J. Liu, R. Sun, W. Kou, X. Sun, “The Security Analyses of RosettaNet in Grid,” *Computer Standards & Interfaces*, Vol. 29, pp. 224-228, February 2007.

[17] G. Geethakumari, A. Negi, V. N. Sastry, “Dynamic Delegation Approach for Access Control in Grids,” in *Proceedings of First International Conference on e-Science and Grid Computing*, Melbourne, Australia, pp. 387-394, December 2005.

[18] G. Geethakumari, A. Negi, V. N. Sastry, “Grid Security through Delegation of Roles,” *Proceedings of 2006 IEEE Region 10 Conference (TENCON 2006)*, Hong Kong, China, pp. 1-4, November 2006.

[19] K. Bicakci, “One-time Proxy Signatures Revisited,” *Computer Standards & Interfaces*, Vol. 29, pp. 499-505, May 2007.

[20] C. C. Chang, I. C. Lin, J. H. Yang, “An Efficient Proxy Signature for Realizing Generalized Proxy Signature Policy,” *Proceedings of The 4th International Conference on Intelligent Information Hiding and Multimedia Signal Processing(IIHMSP08)*, Harbin, China, pp. 1537-1540, August 2008.

[21] M. S. Hwang, I. C. Lin, J. L. Lu, “A Secure Nonrepudiable Threshold Proxy Signature Scheme with Known Signers,” *Informatica*, Vol. 11, No. 2, pp. 1-8, 2000.

[22] Z. Shao, “Improvement of Efficient Proxy Signature Schemes using Selfcertified Public Keys,” *Applied Mathematics and Computation*, Vol. 168, pp. 222-234, September 2005.

[23] S. Zhao, A. Aggarwal, R. D. Kent, “PKI-based Authentication Mechanisms in Grid Systems,” *Processing of Networking, Architecture, and Storage (NAS)*, Guilin, Guangxi, China, pp. 83-90, July 2007.

[24] S. Piger, C. Grimm, R. Groeper, C. Kunz, “A Comprehensive Approach to Self-restricted Delegation of Rights in Grids,” *Proceedings of Cluster Computing and the Grid*, Lyon, France, pp. 114-121, May 2008.

[25] M. C. Li, J. Ma, H. Yao, “Recovery Mechanism of Online Certification Chain in Grid Computing,” *Proceedings of Availability, Reliability and Security (ARES)*, Vienna, Austria, pp. 558-562, April 2006.

[26] J. Novotny, S. Tuecke, V. Welch, “An Online Credential Repository for the Grid: Myproxy,” *Proceedings of High Performance Distributed Computing*, San Francisco, California, U.S.A., pp. 104-111, August 2001.

[27] S. Raghunathan, A. R. Mikler, C. Cozzolino, “Secure Agent Computation: X.509 Proxy Certificates in A Multi-lingual Agent Framework,” *Journal of Systems and Software*, Vol. 75, pp. 125-137, February 2005.

[28] V. Welch, I. Foster, C. Kesselman, O. Mulmo, L. Pearlman, S. Tuecke, J. Gawor, S. Meder, F. Siebenlist, “X.509 Proxy Certificates for Dynamic Delegation,” *Proceedings of 3rd Annual PKI R&D Workshop,* MD, U.S.A., pp. 42-58, April 2004.