Constructing a Highly Efficient Integrated Access Control Scheme for Web Services

黃美治、曹偉駿

E-mail: 9510897@mail.dyu.edu.tw

ABSTRACT

Web services technology is an extreme efficient structure of information system for promoting enterprises to lower operating cost and raise profits. Nevertheless, with the pluralism of trading platforms, the security of transmitting message and how to execute the access control for information systems will become an important issue for securing the web service environment. Using certificate-based public key cryptosystems to solve the problems related to the demand of security under the current environment of web services causes rather complicated identity verifying and management. The methods of access control in operation can be divided into two kinds. One is that each user must register at different web sites, and therefore the system administrator will be busy in establishing the authority connection for these users; the other is at one specific web site, but every single site is connected with the others through the way of “ loosely coupled ”, but user may face the problem of different level of authority from a variety of web domains. For this reason, in the thesis the mechanism of integrated access control with high efficiency is constructed using the ECC-based self-certified public key cryptosystems and role-based access control scheme. The proposed mechanism can identify the user without employing certificates, and solve the limits of access authority across different web domains without any influence upon current system operations. Furthermore, after the comparisons with the current access control schemes for web services, we can find the proposed one will be superior to the others in terms of security and efficiency. We affirm that the proposed scheme will be able to lower the cost of maintenance and lighten the burden of system administrator, and thus promote the efficiency of access control to web services environments.

Keywords : Web Services ; Role-Based Access Control ; Elliptic Curve Cryptosystems ; Self-certified Public Key Cryptosystems ; Information Security

Table of Contents

REFERENCES

一、中文文獻 [1] 李宜儒, “ 網路服務應用在企業資訊整合的安全性議題及解決方案之研究, ” 國立台灣大學資訊管理學研究所碩士論文, 2004. 二、英文文獻 [2] J. F. Barkley, A. V. Cincotta and D. F. Ferraiolo, “ Role Based Access Control for the World Wide Web, ” Proceedings of the 20th National Information System Security Conference, pp. 331-341, 1997.

[3] D. W. Chadwick and A. Otenko, “ The PERIMIS X.509 Role Based Privilege Management Infrastructure, ” Proceedings of the 7th ACM

Symposium on Access Control Models and Technologies, pp. 135-140, 2002.
[4] M. Coetzee, and J. H. P. Eloff, " Towards Web Service Access Control, " Computers & Security, Vol. 23, pp. 559-570, 2004.
[5] M. Coetzee , and J. H. P. Eloff, " An Access Control Framework for Web Services, " Information Management & Computer Security , Vol. 13, No. 1, pp. 29-38, 2005.
[6] D. Ferraiolo, and R. Kuhn, " Role-Based Access Control, " Proceedings of the 15th NIST – NCSC National Computer Security Conference, 1992.
[7] D. F. Ferraiolo, J. F. Barkley, and D. R. Kuhn, " A Role Based Access Control Model and Reference Implementation within a Corporate Intranet, " ACM Transactions on Information Systems Security, Vol. 1, No. 2, pp. 34-64, 1999.
[8] M. Girault, " Self-Certified Public Keys, " Advances in Cryptology: EuroCrypt ' 91, Lecture Notes in Computer Science, Vol. 547, pp. 491-497, 1991.
[9] C. Gunther, " An Identity-Based Key-Exchange Protocol, " Advances in Cryptology EuroCrypt ' 91, Lecture Notes in Computer Science, Vol. 547, pp. 29-37, 1991.
[10] J. J. Hwang, B. M. Shao and P. C. Wang, " A New Access Control Method Using Prime Factorization, " The Computer journal, Vol. 35, No. 1, pp. 16-20, 1992.
[11] L. Javier, O. Rolf, and P. Gunther, " Authentication and Authorization Infrastructures (AAIs): A Comparative Survey " , Computers and Security, Vol. 23, pp. 578-590, 2004.
[12] N. Koblitz, " Elliptic Curve Cryptosystems, " Mathematics of Computation, Vol. 48, No. 17, pp. 203-209, 1987.
[13] J. T. Kohl, B. C. Neuman, and T. Y. T'so, " The Evolution of the Kerberos Authentication System, " Distributed Open Systems, IEEE Computer Society Press, pp. 78-94, 1994.
[14] M. Kudo and H. Satoshi, " XML Document Security Based on Provisional Authorization, " Proceedings of the 7th ACM Conference, pp. 87-96, 2000.
[15] B. B. L. Lim, Y. Sun and J. Vila, " Incorporating WS-Security into a Web Services -Based Portal, " Information Management & Computer Security, Vol. 12, No. 3, pp. 206-217, 2004.
[16] J. Lopeza, R. Oppligerb, G. Pernul, " Authentication and Authorization Infrastructures (AAIs): A Comparative Survey, " Computers & Security, Vol. 23, pp. 578-590, 2004 [17] S. Miller, B. Neuman, J. Schiller, and J. Saltzer, " Kerberos Authentication and Authorization System, " In Project Athena Technical Plan, Section E.2.1. Massachusetts Institute of Technology, 1988.
[18] V. S. Miller, " Use of Elliptic Curves in Cryptography, " Advances in Cryptology:Crypto ' 85, Springer-Verlag, pp. 417-426, 1986.
[19] J. Park and R. S. Sandhu, " RBAC on the Web by Smart Certificates, " Proceedings of the 4th ACM Workshop on Role-based Access Control, pp. 1-9, 1999.
[20] J. Park, R. S. Sandhu and G. J. Ahn, " Role-Based Access Control on the Web, " ACM Transactions on Information and System Security, Vol. 4, No. 1, pp. 37 – 71, 2001.
[21] H. Petersen, and P. Horster, " Self-Certified Keys Concepts and Applications, " Proceedings of Communications and Multimedia Security ' 97, pp. 102-116, 1997.
[22] O. Rolf, " Microsoft .NET Passport and Identity Management " , Information Security Technical Report, Vol. 9, pp. 26-34, 2004.
[23] S. Saeednia, " Identity-Based and Self-Certified Key-Exchange Protocols, " Information Security and Privacy: ACISP ' 97, pp. 303-313, 1997.
[24] R. Sandhu, and P. Samarati, " Access Control: Principles and Practices, " IEEE Communication Magazine, Vol. 32, No.9, pp. 40-48, 1994.
[25] R. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, " Role-Based Access Control: A Multi-Dimensional View, " Proceedings of 10th Annual Computer Security Applications Conference, Orlando, Florida, pp. 54-62, 1994.
[26] R. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, " Role-Based Access Control Model, " IEEE Computer, Vol. 29, No. 2, pp. 38-47, 1996.
[27] R. Sandhu, D. Ferraiolo and R. Kuhn, " The NIST Model for Role-Based Access Control:Towards A Unified Standard " , Proceedings of the fifth ACM Workshop on Role-based Access Control, 2000.
[28] A. Shamir, " Identity-Based Cryptosystems and Signature Schemes, " Proceedings of CRYPTO ' 84, pp. 47-53, 1985.
[29] Z. Tari and S. H. Chan, " A Role-Based Access Control for Intranet Security, " IEEE Internet Computing, Vol. 1, No. 5, pp. 24-34, 1997.
[30] W. J. Tsaur, " Several Security Schemes Constructed Using ECC-Based Self-Certified Public Key Cryptosystems, " Applied Mathematics and Computation, Vol. 168, No.1, pp. 447-464, 2005.
[31] S. Vanstone, " Elliptic Curve Cryptosystem - the Answer to Strong fast Public-Key Cryptography for Securing Constrained Environments, " Information Security Technical Report, Vol. 2, No. 2, Elsevier, pp. 78-87, 1997.
[32] H. A. Weber, " Role-Based Access Control: The NIST Solution, " , 2003.
[33] M. Winslett, N. Ching, V. Jones and I. Slepchin, " Using Digital Credentials on the World Wide Web, " Journal of Computer Security, Vol. 5, pp. 255-267, 1997.
[34] T. C. Wu, Y. S. Chang and T. Y. Lin, " Improvement of Saeednia ' s Self-Certified Key Exchange Protocols, " IEEE Electronic Letters,

Vol. 34, No. 11, pp. 1094-1095, 1998.
[35] T. C. Wu, “ Digital Signature/multi Signature Schemes giving Public Key Verification and Message Recovery Imultaneously, ” Computer Systems Science and Engineering, 2001.
[36] E. P. Xaier, “ XML Based Security for E-Commerce Applications ”, Proceedings of the Eighth Annual IEEE International Conference and Workshop on Engineering of Computer Based Systems, pp. 10-17, 2001.
[37] ITU-T Recommendation X.509 (ISO/IEC 9594-8), Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, 2001.
[38] Microsoft, [39] MySQL, [40] Public Key Infrastructure, [41] XML.org,