建構高效率之整合式網路服務存取控制機制

黃美治、曹偉駿

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

摘 要

網路服務技術是一個幫助企業降低營運成本並提高獲利極為有效的資訊系統架構。但隨著交易環境的多元化，訊息內容的安全與如何有效執行存取控制，將成為網路服務環境下一大課題。 目前網路服務環境的安全需求中，多採用憑證為基礎的公開金鑰密碼系統來解決相關的問題，這使得在身份驗證及管理上具有相當的複雜度。而在存取控制的方法上，現行作法可分為二大類。第一類是由使用者分別向不同的網路服務站台註冊以取得相關服務，但此方法存在著缺點為，系統管理者必須持續為短暫需求使用者建立使用權限；第二類則是使用者向單一站台註冊，而站台之間以鬆散偶合(Loosely Coupled)的方式連結，但此方法卻也有不同網域對於使用權限認定不一致的問題。 因此，本論文基於低運算量之『植基於ECC的自我認證公開金鑰密碼系統』與角色為基礎的存取控制方式，建構出具有高效率的整合式存取控制機制。是故，本機制能在不使用憑證的狀況下做到使用者身份識別，同時能在不影響現行企業內部存取控制的前提下，解決跨網域存取權限不一的問題。此外，與現行網路服務存取控制機制進行比較後發現，本機制不論在安全性與效率上都有較優的表現。相信本機制應用在企業網路服務上，可降低維護成本並且有效減輕系統管理者負擔，進而提升存取效率。

關鍵詞 : 角色為基礎的存取控制 ; 網路服務 ; 橢圓曲線密碼系統 ; 自我驗證公開金鑰密碼系統 ; 資訊安全

目錄

參考文獻

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,