An Agent-Based Single Sign-On Scheme for Web Services Environments

林右明、曹偉駿

E-mail: 9510895@mail.dyu.edu.tw

ABSTRACT

Nowadays, web services ’ single sign-on schemes can provide a single authenticator for their verification purpose. However, users who enter most of these single sign-on systems receive less service from them, because all activities in these systems are limited in a single domain. If the users would like to enter other websites, the "log-in" process has to be done once again for accessing the web. In such a way, it is inconvenient and time-consuming for users. SAML standard was established based on OASIS, and it provides Web Services ’ single sign-on function; however, the system uses "re- direct" method for its verification purpose which not only increases the heavy loading of servers, but also costs the Internet flow and bandwidth. Furthermore, it may cause the potential attacks like the replay and man-in-the-middle attacks. On the other hand, Microsoft, one of the world well-known software builder, has create something similar called .NET Passport. Its function includes single sign-on as well; however, the privacy of user may suffer the risk of eavesdropping. Therefore, developing a trust model under a single sign-on system of web services environments with the help of secure agent platform is the main contribution of this thesis. In summary, the proposed single sign-on scheme can reduce the number of communications between users and servers, enhance the security of Internet services, provide the privacy of users, and promote the efficiency of system as well as less delay in the web services environments. In addition, this thesis further employs Lysa analysis tool to verify the security and correctness of the proposed scheme.

Keywords : Web Services ; Agent ; Single Sign-On (SSO) ; Information Security ; Lysa-Tool

Table of Contents

封面內頁 授權書 中文摘要 .....iv 英文摘要 .....v 誌謝 .....vi 目錄 .....vii 圖目錄 .....xiii 表目錄 .....xiii 第一章 緒論 .....1 1.1 研究背景與動機 .....1 1.2 研究目的 .....2 1.3 研究流程 .....3 1.4 論文架構 .....4 第二章 文獻探討 .....6 2.1 單一登入 .....6 2.2 網路服務(Web Services, WS) .....11 2.3 現行身分認證及單一登入標準 .....17 2.4代理人 (Agent) .....27 第三章 以代理人為基礎之適用於網路服務環境單一登入機制 .....35 3.1 系統架構 .....35 3.2 系統流程 .....38 3.3小結 .....45 第四章 安全性與效能分析 .....46 4.1 基於LYSA-Tool之安全性分析 .....47 4.2 效能分析 .....52 4.3 綜合比較 .....53 第五章 系統實作與模擬 .....55 5.1 軟硬體需求 .....55 5.2 系統設計流程 .....56 5.3 程式執行畫面 .....69 第六章 結論與未來發展方向 .....74 6.1 結論 .....74 6.2 未來發展方向 .....75 參考文獻 77

REFERENCES

1. 李長庚, 「一個開放的Web-Based Single Sign-On 服務架構」, 國立交通大學電機資訊研究所 碩士論文, 民國九十一年(指導教授:羅濟群)。 2. 林金龍, 「以P2P網路架構實作Single Sign-On機制之研究」, 世新大學資訊管理研究所碩士 論文, 民國九十四年(指導教授:廖鴻圖博士)。 3. 洪振偉, 「以派翠網方法建立一個安全的遷移式軟體代理人系統模型」, 台中健康暨管理學院資 訊科技與管理研究所碩士論文, 民國九十一年(指導教授:蔡進發博士)。 4. S. Adabala, et.al., “ Single Sign-On in In-VIGO: Role-based Access via Delegation Mechanisms Using Short-lived User Identities ”, 18th International Parallel and Distributed Processing Symposium (IPDPS'04), p. 22b, 2004. 5. J. Ametller, S. Robles, J. A. Ortega-Ruiz, “ Self-Protected Mobile Agents ”, Proceedings of the 3rd International Joint Conference on Autonomous Agents and Multiage System, pp. 362-367, 2004. 6. P. Ashley, M. Vandenwauver, and J. Clasessens, “ A Comparison of SESAME and SSL for Intranet and Internet Security in Information Security Management and Small System Security ”, Proceeding of IFIP TC11 WG11.1/WG11.2 Seventh Annual Working Conference on Information Security Management, Vol.154, pp. 60-69, 1998. 7. E. Bierman and E. Cloete, “ Classification of Malicious Host Threats in Mobile Agent Computing ”, Proceedings of SAICSIT, 2002. 8. D. Boneh and M. Franklin, “ Identity-Based Encryption from the Weil Pairing, ” Advances in Cryptology – Crypto ’ 2001, LNCS 2139, Springer-Verlag, pp. 213-229,

2001 9. M. Burchholtz, C. Montangero, L. Perrone, and S. Semprini, “ For-LySa: UML for Authentication Analysis ”, Lecture Notes in Computer Science, Vol. 3267, pp. 93-107, 2004 10. T. Gross. “ Security Analysis of the SAML Single Sign-on Browser/Artifact Profile ”, 19th Annual Computer Security Applications Conference (ACSAC '03), p. 298-309, 2003. 11. H. Y. Chien, “ New Approach to Authorization and Authentication in Distributed Environments ”, Communications of the CCISA, Vol. 9, No. 3, pp.63-69, 2003. 12. M. Hansen, J. Skriver, H. R. Nielson, “ Using Static Analysis to Validate the SAML Single Sign-On Protocol ”, Proceedings of the workshop on Issues in the theory security, pp. 27-40, 2005 13. IBM “ Single Sign-On ”, http://www-128.ibm.com/developerworks/cn/security/se-sso/ index.html. 14. IBM, “ Build and Implement a Single sign-on Solution ”, http://www-106.ibm.com/ developerworks/web/library/wa-singlesign/#main, Technique Report. 15. J. Jeong et al., “ An XML-based Single Sign-On Scheme Supporting Mobile and Home Network Service Environments ”, IEEE Transactions on Consumer Electronics, Vol. 50, Issue. 4, pp. 1081-1086, 2004. 16. J. T. Kohl, B. C. Neuman, and T. Y. T'so, “ The Evolution of the Kerberos Authentication System ”, IEEE Computer Society Press Distributed Open Systems, pp. 78-94, 1994. 17. David P. Kormann and Aviel D. Rubin, “ Risks of the Passport Single Sign on Protocol ”, Computer Networks, Elsevier Science Press, vol. 33, pp. 51-58, 2000. 18. Microsoft, “ Implement a Single-Sign On solution by using basic authentication and Internet Explorer client ”, http://support.microsoft.com/default.aspx?scid=kb;EN-US; 837104., Technique Report. 19. Microsoft, “ Microsoft .NET Passport 2.5 Software Development Kit ”, http://msdn. microsoft.com/library/default.asp?url=/downloads/list/websrvpass.asp ,Technique Report. 20. N. Park, G. Lee, “ Agent-based Web Services Middleware ”, Global Telecommunications Conference, 2003. GLOBECOM '03. IEEE, Vol. 6, pp. 3186-3190, 2003. 21. J. Peters, “ Integration of Mobile Agents and Web Services ”, 1st European Young Researchers Workshop on Service Oriented Computing, pp. 53-58, 2005. 22. V. Renganarayanan, A. S. Helal, A. Nalla, “ Internet Agents for Effective Collaboration ” Lecture Notes in Computer Science, Vol. 2521, pp.33-47, 2002 23. V. Roth, “ Secure Recording of Itineraries through Co-operating Agent ”, ECOOP Workshop, pp. 1070-1077, 2002. 24. V. Roth, “ On the Robustness of Some Cryptographic Protocols for Mobile Agent Protection ”, Proceedings of the 5th International Conference on Mobile Agents, pp. 1-14, 2001 25. R. Sakai, K. Ohgishi, and M. Kasahara, “ Cryptosystems Based on Pairing, ” Symposium on Cryptography and Information Security, SCIS ’ 2000, 2000. 26. F. Satoh, T. Itoh. “ Single Sign On Architecture with Dynamic Tokens ”, Symposium on Applications and the Internet (SAINT'04), pp. 197-202, 2004. 27. R. Semancik, “ Internet Single Sign-On System ”, Informatics and Information Technologies Student Research Conference, pp. 116-123, 2005. 28. SeMoA, http://www.semoa.org/. 29. Single Sign-On. http://www.opengroup.org/security/sso/. 30. W. J. Tsaur and C. H. Ho, “ A Mobile Agent Protected Scheme Using Pairing-Based Cryptosystems ”, International Journal of Mobile Communications, Vol. 3, No. 2, pp. 183-196, 2005. 31. N.Wijngaards, B. Overeinder, M. Steen, F. Brazier, “ Supporting Internet-Scale Multi-Agent System ”, Data & Knowledge Engineering, Vol. 41, pp. 229-245, 2002. 32. T. White, “ Securing Mobile Agents Implemented in the Scheme Programming Language ”, Safety and Security in Multiagent Systems (SASEMAS), pp. 431-438, 2004 33. T. Zhang, J. Luo, W. Kong, “ An Agent-Based Web Service Searching Model ”, The 9th International Conference on Computer Supported Cooperative Work in Design Proceedings, pp. 390-396, 2005.