基於代理人之適用於網路服務環境單一登入機制

林右明、曹偉駿

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

摘 要

目前，大部分的網路服務單一登入機制皆僅提供單一認證伺服器的認證方式，使用者登入這些 單一登入系統，都必須由此認證伺服器來發放憑證，且僅限於同一個網域的服務，如果要前往其他 網域時，則必須再進行登入的動作，讓單一服務的使用者無法真正利用到單一登入的便利性。 由OASIS制定的SAML標準，提供了網路服務單一登入的功能，系統利用重新導向到認證伺服器的 方法來達到認證的目的，如此除了增加主機端的負載以及網路的流量與頻寬的浪費外，在安全上也存在重送攻擊以及中間人攻擊的風險。而微軟的.NET Passport雖然也提供單一登入的功能，但在使 用者的隱私上卻無法保障。 因此，本篇論文的主要目的在於透過安全代理人平台與網路服務緊密的整合，建立在信任模式 下的單一登入系統。利用代理人本身攜帶使用者的資訊，使得使用者與主機間的溝通次數減少，以 提高在網路服務環境的單一登入安全性、確保使用者的帳戶隱私內容，並且可以減少單一登入使用 者端與其他主機溝通的次數、減少分散式環境中網路流量，並提昇整體效能與降低因網路延遲所造 成網路服務主機相互溝通的問題。此外，本研究亦利用LySa工具程式探討本機制的安全性與正確性，以驗證本機制之效益。

關鍵詞 : 網路服務 ; 代理人 ; 安全性 ; 代理人 ; 便利性 ; 正確性 ; 伺服器 ; 單一登入 ; 資訊安全 ; Lysa分析工具

目錄

參考文獻

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.