基於情境感知之數位典藏網路服務環境的高安全存取控制機制

鄭博元、曹偉駿

E-mail: 9806119@mail.dyu.edu.tw

摘 要

我國數位典藏計畫推展至今，已累積了相當可觀的典藏資源，如何使用網路服務技術，在分散式架構基礎上，提供整體服務如單一登入機制之建立、內容使用之相互授權等，實為一重要課題。另外，網路服務存取控制策略當中，其中以角色為基礎的存取控制(role-based access control, RBAC)，雖然可大幅降低系統管理員的負擔，使得管理者有效率地檢視使用者目前的權限。然而，隨著網路安全問題層出不窮，現有存取控制機制是不夠的。因此本研究除了以情境感知機制彌補RBAC的不足，更進一步使用決策樹演算法挖掘隱藏情境。其中，情境感知技術能夠隨著不同的時空與環境狀態變化，動態地調整用戶存取限制，並依照通訊裝置的特色，提供適當的服務與存取內容，使得系統不論在安全性與執行效率，皆能夠獲得極佳改善。本機制首先建置點對點分散式協定，用以防止網路擁塞所造成的傳輸不順暢，並整合單一登入與跨網域RBAC，來改善數位典藏多系統權限不一與角色衝突的問題，更進一步藉由情境感知技術達到彈性授權之目的。最後，本研究建立一個系統雛型，用以印證本機制的可行性。

關鍵詞 : 數位典藏、網路服務、角色為基礎的存取控制、情境感知、決策樹

目錄

參考文獻

一、中文部份古一浩(2006)，Ajax範例活用辭典，台北:博碩文化。國立故宮博物院(2005)，如何數位典藏[線上資料]，來源: http://tech2.npm.gov.tw/da/ [2009, April 21]。曹偉駿，黃美治(2008)，設計高效?之網?服務存取控制機制，2008年民生電子研討會論文集，209-216。蔡永橙，黃國倫，邱志義(2007)，數位典藏技術導論，台北:中央研究院台大出版中心。二、英文部份Abdelzaher, T. F., Atkins, E. M., & Shin, K. G. (2000). Qos negotiation in real-time systems and its application to automated flight control. IEEE Transactions on Computers, 49(11), 1170-1183.Agreiter, B., Hafner, M., & Breu, R. (2008). A fair non-repudiation service in a web services peer-to-peer environment. Computer Standards & Interfaces, 30(6), 372-378.Al, A. D., & McNair J. (2008). On the interaction between localization and location verification for wireless sensor networks. Computer Networks, 52(14), 2713-2727.Baru, C., & Rajasekar, A. (1998). A hierarchical access control scheme for digital libraries. Proceedings of the Third ACM Conference on Digital Libraries (pp. 275-276), United States of America: Pittsburgh.Berson, A., Smith S., & Thearling, K. (2000). CRM Data Mining: Build Data Mining Application for CRM, New York: McGraw-Hill.Bradbury, D. (2007). Decoding digital rights management. Computers & Security, 26(1), 31-33.Chang, H. K. C., Hwang, J. J., & Liu, H. H. (2000). A novel access control method using morton number and prime factorization. Information Sciences, 130(1-4), 23-40.Coetzee, M., & Eloff, J. H. P. (2004). Towards web service access control. Computers & Security, 23(7), 559-570.Feigenbaum, J., Freedman, M. J., Sander, T., & Shostack, A. (2001). Privacy engineering for digital rights management systems, Proceedings of the ACM Workshop on Security and Privacy in Digital Rights Management (pp. 76-105), United States of America: Pennsylvania.Ferraiolo, D., & Kuhn, R. (1992). Role-based access controls. Proceedings of the Fifteenth National Computer Security Conference (pp. 554-563), United States of America: Baltimore.Han, S. C., & Xia, Y. (2009). Optimal node-selection algorithm for parallel download in overlay content-distribution networks. Computer Networks, 53(9), 1480-1496.Hulsebosch, B., Salden, A., & Bargh, M. (2004). Context-based service access for train travelers. Lecture Notes in Computer Science, 3295, 84-87.Janikow, C. Z. (1998). Fuzzy decision tree: Issues and methods. IEEE Transaction on Systems Man and Cybernetics Part B-Cybernetics, 28(1), 1-14.Kapsalis, V., Hadellis, L., Karelis, D., & Koubias, S. (2006). A dynamic context-aware access control architecture for e-services. Computers & Security, 25(7), 507-521.Lim, B. B. L., Sun, Y., & Vila, J. (2004). Incorporating WS-security into a web services-based portal. Information Management & Computer Security, 12(3), 206-217.Maniatis, P., Giuli, T., Roussopoulos, M., Rosenthal, D. S. H., & Baker, M. (2004). Impeding attrition Attacks in P2P systems. Proceedings of the Eleventh Workshop on ACM SIGOPS, Belgium: Brussels.Martin, F. J. P. (1999). Push vs. pull in web-based network management. Proceedings of Sixth IFIP/IEEE International Symposium on Integrated Network Management (pp. 3-18), England: Boston.Mengelberg, J. B. (2005). Teaching system access control. Journal of Issues in Informing Science and Information Technology, 2, 139-158.Muhlbauer, A., Naini, R. S., Salim, F., Sheppard, N. P., & Surminen, M. (2008). Location constraints in digital rights management. Computer Communications, 31(6), 1173-1180.Mundt, T. (2006). Two methods of authenticated positioning. Proceedings of the Second ACM International Workshop on Quality of Service & Security for Wireless and Mobile Networks (pp. 25-32), Spain: Malaga.OASIS. (1999). XML.org [online]. Available: http://www.xml.org [2009, January 6].Palomar, E., Tapiador, J. M. E., Julio, H. C. C., & Ribagorda, A. (2008). Secure content access and replication in pure P2P networks. Computer Communications, 31(2), 266-279.Park, J. S., & Hwang, J. (2003). Role-based access control for collaborative enterprise in peer-to-peer computing environments. Proceedings of the Eighth ACM Symposium on Access Control Models and Technologies (pp. 93-99), Italy: Como.Polat, K., & Gunes, S. (2009). A novel hybrid intelligent method based on C4.5 decision tree classifier and one-against-all approach for multi-class classification problems. Expert Systems with Applications, 36(2), 1587-1592.Quinlan, J. R. (1986). Induction on decision tree. Machine Learning, 1(1), 81-106.Quinlan, J. R. (1993). C4.5: Programs for Machine Learning. San Francisco: Morgan kaufmann.Quinlan, J. R. (2003). Online Tutorial [online]. Available: http://www.rulequest.com/ [2009, April 19].Romero, C., & Ventura, S. (2007). Educational data mining: A survey from 1995 to 2005. Expert Systems with Applications, 33(1), 135-146.Sandhu, R., Ferraiolo, D., & Kuhn, R. (2000). The NIST model for role-based access control: Towards a unified standard. Proceedings of the Fifth ACM Workshop on Role-based Access Control (pp. 111-119), Germany: Berlin.Sandhu, R., & Park, J. (2003). Usage Control: A vision for next generation access control. Lecture Notes in Computer Science, 2776, 17-31.Schilit, B., Adams, N., & Want, R. (1994). Context-aware computing applications. IEEE Workshop on Mobile Computing Systems and Applications (pp. 85-90).Shaw, M. J., Subramaniam, C., Tan, G. W., & Welge, M. E. (2001). Knowledge management and data mining for marketing. Decision Support Systems, 31(1), 127-137.Sheu, J. P. Tu, S. C., & Hsu, C. H. (2008). Location-free topology control protocol in wireless ad hoc networks. Computer Communications, 31(14), 3410-3419.Shih, D. H., Chiang, H. S., & Lin, B. (2007). A generalized associative petri net for reasoning. IEEE Transactions on Knowledge and Data Engineering, 19(9), 1241-1251.Stephanos, A. T., & Diomidis, S. (2004). A survey of peer-to-peer content distribution technologies. ACM Computing Surveys, 36(4), 335-371.Strembeck, M., & Neumann, G. (2004). An integrated approach to engineer and enforce context constraints in RBAC environments. ACM Transactions on Information and System Security, 7(3), 392-427.Tomur, E., & Erten, Y. M. (2006). Application of temporal and spatial role based access control in 802.11 wireless networks. Computers & Security, 25(6), 452-458.Tsaur, W. J., & Lin, Y. M. (2009). An agent-based single sign-on scheme for web services environments. Proceedings of the 2009 International Conference on Security and Management, United States of America: Las Vegas.Wu, E. H. K., Hsieh, M. I., & Lai, H. T. (2006). Low latency and efficient packet scheduling for streaming

applications. Computer Communications, 29(9), 1413-1421.Younas, M., Awan, I., & Duce, D. (2006). An efficient composition of web services with active network support. Expert Systems with Applications, 31(4), 859-869.Zhang, G., & Parashar, M. (2003). Dynamic context-aware access control for grid applications. Proceedings of the Fourth International Workshop on Grid Computing (pp. 101-108), United States of America: Washington.