具交談金鑰預測功能之無線區域網路安全防護機制

李哲維、曹偉駿

E-mail: 9607622@mail.dyu.edu.tw

摘 要

無線區域網路(Wireless Local Area Network；WLAN)提供今日使用者於機動性與便利性之資訊應用需求，卻也必須面臨異於以往的資訊安全風險。網路管理人員在進行WLAN安全防護措施時，普遍會面臨以下兩個問題：一、弱點偵防與檢測的工作需要耗費企業組織中大量的系統資源與稽核人力成本；二、WLAN環境下之Client端節點變動頻繁，使得無線存取點(Access Point)及使用者端稽核的工作面臨相當大的考驗。因此，本研究提出兼具高安全性與預測能力之WLAN安全防護機制，將可同時避免WLAN環境中的節點異動頻繁所造成之安全性衝擊、簡化並降低企業組織於稽核未經授權之AP時所需的網路專業門檻及人力物力、自動化檢測無線網路服務使用者之合法使用期限、預測並評估目前所使用的交談金鑰之風險等級。值得一提的是，使用者可視交談金鑰之風險等級預測結果，以評估是否需重新更換交談金鑰，如此一來除了可降低系統於產生交談金鑰時所耗費的運算資源，更可免除使用者須時常更新交談金鑰的困擾。相信本機制將可提供企業組織一兼具高安全性、便利性與低成本之WLAN安全解決方案。

關鍵詞 : 無線區域網路安全 ; 弱點檢測 ; 無線存取點 ; 橢圓曲線密碼系統

目錄

參考文獻

一、中文部份 謝燦榮(2005)，適用於多伺服器環境之兼具效率與安全的身份認證機制，大葉大學資訊管理系未出版之碩士論文，29-31。 二、英文部份 Alhazmi, O. H., & Malaiya, Y. K. (2005a). Modeling the Vulnerability Discovery Process. Proceedings of the 16th IEEE International Symposium on Software Reliability Engineering (pp. 1-10), USA:Dallas. Alhazmi, O. H., & Malaiya, Y. K. (2005b). Quantitative Vulnerability Assessment of Systems Software. Proceedings of Annua lReliability and Maintainability Symposium (pp. 615-620), USA:Alexandria. Ali, K. M., & Owens, T. J. (2007). Selection of an EAP Authentication Method for A WLAN. International Journal of Information and Computer Security 1(1/2), 210-233. Allen, J., Christie, A., Fithen, W., McHugh, J., Pickel, J., & Stoner, E. (2000). State of the Practice of Intrusion Detection Technologies. Software Engineering Institute Technical Report, CMU/SEI-99-TR-028, Carnegie Mellon University. Altrock, C. V. (1996). Fuzzy Logic & Neuro Fuzzy Applications In Business & Finance. Upper Saddle River, NJ:Prentice Hall PTR, 35-43. Anh, N. T., & Shorey, R. (2005). Network Sniffing Tools for WLANs: Merits and Limitations, Proceedings of the 2005 IEEE International Conference on Personal Wireless

Communications (pp. 389-393), India:New Delhi. Bittau, A., Mark, H., & Joshua, L. (2006). The Final Nail in WEP ' s Coffin, Proceedings of 2006 IEEE Symposium on Security and Privacy (pp. 386-400), USA:California. Corral G., Cadenas X., Zaballos A., & Cadenas, M. T. (2005). A Distributed Vulnerability Detection System for WLANs. Proceedings of First International Conference on Wireless Internet (pp. 86-93), Budapest:Hungary. Corral G., Zaballos A., Cadenas X., & Grane, A. (2005). A Distributed Vulnerability Detection System for an Intranet, Proceedings of the 39th Annual 2005 International Carnahan Conference on Security Technology (pp. 291-294), SPAIN:Las Palmas. Dantu, R., Clothier, G., & Atri, A. (2007). EAP Methods for Wireless Networks. Computer Standards and Interfaces, 29(3), 289-301. FuzzyTECH. (2007). FuzzyTECH Features Overview [Online]. Available: http://www.fuzzytech.com/e/ftpo.html [2007, March 15] Gerald, C., & Wheatley, P. (2003). Applied Numerical Analysis, Pearson Education. Gupta, M., Rees, J., Chaturvedi, A., & Chi, J. (2006). Matching Information Security Vulnerabilities to Organizational Security Profiles: A Genetic Algorithm Approach, Decision Support Systems, 41(3), 592-603. Herzog, P. (2003). Open-Source Security Testing Methodology Manual-Wireless Security Testing Section (OSSTMM WIRELESS). The Institute for Security and Open Methodologies. Il-Gon, K., & Jin-Young, C. (2004). Formal Verification of PAP and EAP-MD5 Protocols in Wireless Networks: FDR Model Checking. Proceedings of the 18th International Conference on Advanced Information Networking and Applications (pp. 264-269), Japan:Fukuoka. Jing, N., Wen, J. Luo, J. He, X. , & Zhou, Z. (2007). An Adaptive Fuzzy Logic Based Secure Routing Protocol in Mobile Ad Hoc Networks. Fuzzy Sets and Systems, 157(12), 1704-1712. Liu, Y., & Mana, H. (2005). Network Vulnerability Assessment using Bayesian Networks, Proceedings of the SPIE. 61-71. Sanguanpong, S., & Kanlayasiri, U. (2006). Worm Damage Minimization in Enterprise Networks, International journal of Human-Computer Studies, 65(1), 3-16. Tsaur, W. J. (2005). Several Security Schemes Constructed using ECC-Based Self-Certified Public Key Cryptosystems, Applied Mathematics and Computation, 168, 447-464. Tsaur, W. J., Wu, C. C., & Lee, W. B. (2004). A Smart Card-Based Remote Scheme for Password Authentication in Multi-server Internet services. Computer Standards and Interfaces, 27, 39-51. Urien P., Badra, M., & Dandjinou, M. (2004). EAP-TLS SmartCards, from Dream to Reality, Proceedings of the 2004 4th Workshop on Applications and Services in Wireless Networks (pp. 39-45), USA:Massachusetts. Venter, H. S., & Eloff, J. H. P. (2004). Vulnerability Forecasting-A Conceptual Model. Computers and Security, 23, 489-497. Wack, J., Miles, T., & Murugiah S. (2003). Guideline on Network Security Testing, Recommendations of the National Institute of Standards and Technology. Wilfred, L., Allan, W., & Dillon, T. S. (2006). Application of Soft Computing Techniques to Adaptive User Buffer OverflowControl on the Internet. IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, 36(3), 397-410. Willem, G., Ru, D., & Eloff, J. H. P. (1997). Enhanced Password Authentication through Fuzzy Logic, IEEE expert magazine, 12, 38-45. Xie, Y., & Burnham, K. (2006). Fuzzy decision support system for demand forecasting with a learning mechanism. Fuzzy Sets and Systems, 157(12), 1713-1725. Yue, M., & Xiuying, C. (2003). How to Use EAP-TLS Authentication in PWLAN Environment, Proceedings of the 2003 International Conference on Neural Networks and Signal Processing (pp. 1677-1680), China:Nanjing.