

Security Schemes for Wireless Local Area Networks with Session Key Forecasting Capability

李哲維、曹偉駿

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

ABSTRACT

Wireless Local Area Networks (WLAN) provide the demand for information application in the mobility and the convenient capital for users. At the same time, users must to face the variance in the former information security risk. When the network administrator carries on the WLAN security protective measure, usually to face the following two questions generally: First, vulnerability detecting jobs are consuming the massive system resources and the audit manpower cost in enterprise; Second, under the WLAN environment, client nodes are variation frequently, and causes the wireless access point and the user auditing faced with the huge challenge. Therefore, this thesis proposes WLAN security schemes with highly secure and forecasting capability, it might simultaneously avoiding in client nodes are variation frequently that having the secure impact in WLAN environments, simplifying and reducing in auditing the unauthorized AP that needed the network specialized knowledge and the manpower resource in the enterprise to organize, automating detect the users' legitimate life which using the wireless network service, and forecasting and evaluating the risk of rank for a session key. Especially, users could estimate if he needs to regenerate a session key, depending on the forecasting result of the risk of rank for it. In such a case, this schemes cannot only reduce the operation resources of key generating, but also avoid the user to renew session key frequently. We affirm that the proposed schemes can provide the enterprise to achieve a highly secure, convenient and low-cost solution for WLAN.

Keywords : Wireless Local Area Network Security ; Vulnerability Detecting ; Access Point ; Elliptic Curve Cryptosystem

Table of Contents

中文摘要	iii	英文摘要	iii
iv 誌謝辭		v 內容目錄	
vi 表目錄		viii 圖目錄	
ix 第一章 緒論		1 第一節 研究背景	
1 第二節 研究動機與目的		1 第三節 研究流程	
3 第四章 論文架構		4	
第二章 文獻探討	6	第一節 系統弱點與系統安全	
6 第二節 弱點管理與檢測相關機制	7	第三節 基於模糊推論技術之網路安全等級預測機制	
10 第四節 WLAN安全機制之現有解決方案及其存在之弱點		12 第三章 兼具高安全性與交談金鑰預測能力之無線區域網路安全防護機制	
14 第一節 機制架構	14	第二節 建置階段	
15 第三節 註冊階段	17	第四節 登入階段	
18 第五節 檢測階段		19 第六節 交談金鑰產生階段及預測功能	
21 第七節 變更使用者密碼功能		33 第四章 安全性分析	
35 第五章 系統實作與模擬		39 第一節 實驗環境描述	
39 第二節 實驗步驟	42	第六章 討論與結論	
53 第一節 討論	53	第二節 結論	
56 參考文獻	57		

REFERENCES

- 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 Annual Reliability 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 WLAN Environment, Proceedings of the 2003 International Conference on Neural Networks and Signal Processing (pp. 1677-1680), China:Nanjing.