學習導向之無限區域網路入侵偵測機制

楊敦仁、曹偉駿

E-mail: 9806146@mail.dyu.edu.tw

摘 要

自無線區域網路問世後，讓大眾能隨時隨地的享用網路資源，無需再受實體媒介的限制。雖然無線架構帶來相當多的便利，但卻也讓大量的資訊暴露在無形的環境之中，因此駭客可以輕易地竊聽傳輸中的資料，盜用無線設備之資源，致使入侵偵測系統為達到無線區域網路安全所不可或缺的。然而，一般無線區域網路之入侵偵測系統僅應用單一偵測架構來偵測網路上的攻擊行為，同時，亦有低偵測率、過多誤報警訊與誤判情況的問題，導致系統維護人員除了需不時關切警訊是否有用外，還得注意法則庫的時效性。因此，本研究利用判別分析法並整合模糊關聯法則，藉以提出混合式入侵偵測機。首先，利用誤用偵測法比對過濾出已知攻擊行為，接著經由判別分析法來挖掘隱藏於正常行為的未知型攻擊，再將所得之未知型攻擊，由模糊關聯法則追蹤該攻擊行為的軌跡與特徵，更進一步地將攻擊法則自動新增至法則庫內，達到自我學習的效果，藉以改善無線區域網路入侵偵測系統之偵測率不佳與法則庫更新不便的問題。最後，本研究亦實際建構出一個具學習能力之入侵偵測系統，來驗證本機制的可行性。

關鍵詞 : 入侵偵測系統、判別分析、模糊關聯法則、無線區域網路

目錄

參考文獻

一、中文部份台灣電腦網路危機處理?協調中心，(2003)，802.11無線網路安全白皮書[線上資料]，來源: http://www.cert.org.tw/ 16[2009, June 19]。李駿偉、田筱榮、黃世昆，(2002)，入侵偵測分析方法評估與比較，資訊安全通訊。第八卷第二期8(2)，21-37。曹偉駿、梁成揚，(2008)，基於資料挖掘技術之Linux無線區域網路入侵偵測系統，第18屆資訊安全會議，179-192。二、英文部份Asaka, M., Onabuta, T., Inoue, T., Okazawa, S., & Goto, S. (2001). A new intrusion detection method based on discriminant analysis. IEICE TRANSACTIONS ON INFORMATION AND SYSTEMS E SERIES D, pp.570-577.Agrawal, R., & Srikant, R. (1994). Fast algorithms for mining association rules. Proceedings 20th Int. Conf. Very Large Data Bases.Balazinska, M., & Castro, P. (2003). Characterizing mobility and network usage in a corporate wireless local – area network. In J. Pieprzyk & H. Ghodosi (Eds.). Proceedings of the 1st international conference on Mobile systems. applications and services, (pp. 303 – 316), New York: Springer – Verlag.Boncella, R. J. (2006). Wireless Threats and Attacks. Handbook of information security.Boudriga, N., & Obaidat, M. S. (2006). Mobility, sensing, and security management in wireless ad hoc sensor systems. Computers & Electrical Engineering, 32(1 – 3), 266 – 276.Choi, Y. B., Muller, J. Kopek, C. V., & Makarsky, J. M. (2006) . Corporate Wireless LAN Security:Threats and an Effective Security Assessment Framework for Wireless Information Assurance. International Journal of Mobile Communications, 4(3), 266 – 290.Daniels, T., & Spafford, E. H. (1999). Identification of host audit data to detect attacks on low – level IP vulnerabilities. Journal of Computer Security, 7(1), 3 – 35.Debar, H., & Viinikka, J. (2005). Intrusion Detection: Introduction to Intrusion Detection and Security Information Management. Foundations of Security Analysis and Design III, Vol. 3665, pp. 207-236.Ettercap. (2005), sourceforge.net, [online] Available: http://ettercap.sourceforge.net/index.php/[2009, April 15].Fake AP Project. (2005), blackalchemy.to, [online] Available: http://www.blackalchemy.to/project/fakeap/[2009, june 23] .Florez, G., Bridges, S. A., & Vaughn, R. B. (2002). An improved algorithm for fuzzy data mining for intrusion detection. In L. Xu & L. Korba (Eds.), Proceedings of the North American Fuzzy Information Processing Society Conference, (pp. 457-462) , New York: Springer-Verlag.Gill, R., Smith, J., & Clark, A. (2006). Specification- Based Intrusion Detection in WLANs, Proceedings of 22nd Annual Computer Security Applications Conference, Miami.Guan, Y., Ghorbani, A. A., & Belacel, N. (2003). Y – means: A clustering method for intrusion detection. In D.T. Lee & B.S. Lin (Eds.). Proceedings of Canadian Conference on Electrical and Computer Engineering, (pp. 1 – 4), New Jersey: IEEE.Hall, J., Barbeau, M., & Kranakis, E. (2003). Detection of transient in radio frequency fingerprinting using phase characteristics of signals, Proceedings of the 3rd IASTED International Conference on Wireless and Optical Communications (WOC 2003), pages 13 – 18, Banff, Alberta, Canada, July. ACTA Press.Heady, R., Luger, G. Maccabe, A., & Servilla, M. (1990). The architecture of a network level intrusion detection system. Technical report CS90 – 20, University of New Mexico: Department of Computer Science.Hu, Y. C., Chen, R. S., & Tzeng, G.H. (2003). Discovering fuzzy association rules using fuzzy partition methods. Knowledge-Based Systems, 16(3), 137-147.Hossain, M. (2002). Integrating association rule mining and decision tree learning for network intrusion detection: a preliminary investigation. In I.F. Akyildiz, J.Y.B. Lin, & R. Jain (Eds.), Proceedings of the International Conference on Information Systems, Analysis and Synthesis, (pp. 65-70), New Orleans: IEEE.Iheagwara, C., Blyth, A., & Bennett, M. (2005) Architectural and Functional Issues in Systems Requirements Specifications for Wireless Intrusion Detection Systems Implementation. Proceedings of the Systems Communications, (pp. 434-441).Jain, A. K., Murty, M. N., & Flynn, P. J. (1999). Data clustering: a review. ACM Computing Surveys, 31(3), 264-323.Jha, S., & Hassan, M. (2002). Building agents for rule – based intrusion detection system. Computer Communications, 25(15), 1366-1373.Khoshgoftaar, T. M., Nath, S. V., Zhong, S., & Seliya, N. (2005). A clustering approach to wireless network intrusion detection. In J. Crowcroft (Ed.), Proceedings of International Conference on Tools with Artificial Intelligence, (pp. 190 – 196), London: ACM.Lazarevic, A., Ertoz, L., Kumar, V., Ozgur, A., & Srivastava, J. (2003). A comparative study of anomaly detection schemes in network intrusion detection, Proceedings of Third SIAM Conference on Data Mining.Lee, W., Stolfo, S. J., & Mok, K. W. (1999). A data mining framework for building intrusion detection models. In P. Druschel & M.F. Kaashoek (Eds.), Proceedings of the 1999 IEEE Symposium on Security and Privacy, 120-132, New York: IEEE.Lei, J., Fu, X., Hogrefe, D., & Tan, J. (2007). Comparative Studies on Authentication and Key Exchange Methods for 802.11 Wireless LAN. Computers & Security, 26(5), pp. 401-409.Liu, Y., Tian, D., & Li, B. (2006). A Wireless Intrusion Detection Method Based on Dynamic Growing Neural Network. Proceedings of the First International Multi-Symposiums on Computer and Computational Sciences. 2, 611- 615.Luo, J., Bridges, S., & Vaugham, R. B. (2001). Fuzzy frequent episodes for real – time intrusion detection. In D. Maughan & N.H. Vaidya (Eds.), Proceddings of IEEE International Conference on Fuzzy Systems, (pp. 368-371), Atlanta: IEEE.Ouyang, Y. C., Chang, R. L., & Chiu, J. H. (2003). A New Security Key Exchange Channel for 802.11 WLANs. Proceedings of 37th Annual International Carnahan Conference on Security Technology.Patcha, A., & Park, J. M. (2007). An overview of anomaly detection techniques: Existing solutions and latest technological trends. Computer Networks, 51, 3448-3470.Raya, M., Hubaux, J. P., & Aad, I. (2004). DOMINO: A System to Detect Greedy Behavior in IEEE 802.11 Hotspots. ACM MobiSys, June, Boston, USA.Sobh, T. S. (2006). Wired and wireless intrusion detection system: classifications, good characteristics and state – of – the – art. Computer Standards & Interfaces, 28(6), 670-694.Stearley, J. (2004). Towards informatic analysis of syslogs. In H. Krawczyk (Eds.), Proceedings of the IEEE International Conference on Cluster Computing, (pp. 309 – 318), San Francisco: IEEE.Tajbakhsh, A., Rahmati, M., & Mirzaei, A. (2008). Intrusion detection using fuzzy association rules. Applied Soft Computing, 9(2), 462-469.Tsaur, W. J., & Yu, C. C. (2006). Design and Implementation of Highly Accurate Hierarchical Clustering Algorithm for Intrusion Detection. Journal of Internet Technology, Volume 7(2), 177-183.Tsaur, W. J., & Shieh, Y. C. (2003). Constructing fuzzy association rules for intrusion detection systems. In N. Koblitz (Eds.), Proceedings of the 2003 National Computer Symposium, (pp. 1256-1263), New York: Springer-Verlag.Void11. (2005), wirelessdefence.org, [Online] Available: http://wirelessdefence.org/Contents/Void11Main.htm [2009, May 12]Wang, S., Tao, R., Wang Y., & Zhang, J. (2003). WLAN ONLINE and It's Security Problems. Proceedings of the Fourth International Conference on Parallel and Distributed Computing, Applications and Technologies,

241- 244.Wall, D., Kanclirz, J. J., Jing, Y., Faircloth, J., & Barrett, J. (2004). Managing and Securing a Cisco SWAN, SYNGRESS.Wong, W. T., & Lai, C. Y. (2006). Identifying Important Feature for Intrusion Detection Using Discriminant Analysis and Support Vector Machine. Proceedings of the Fifth International Conference on Machine Learning and Cybernetics, Dalian, 13-16. August.