適用於入侵偵測之模糊關聯法則機制研究

施衣喬、曹偉駿

E-mail: 9222463@mail.dyu.edu.tw

摘 要

目前大多數入侵偵測系統的架構可分為主機式或網路式的方式來判別及防制電腦駭客，無論是哪種架構，都是以行為樣式比對的方法來判定是否為駭客入侵。而每種架構的偵測系統，其偵測是否為駭客入侵的技術也可大致區分為兩類，建立正常行為樣式的異常偵測技術；及建立不正常行為樣式的誤用偵測技術。但是若以單一種偵測技術判定是否有入侵行為時，通常都會發生誤報率或誤判率過高的情形，如何降低錯誤率是偵測技術需要探討的主題。此外，隨著網路使用量越來越高，在系統記錄檔中所記錄的資料也越來越多，如何能正確及有效率的從大量資料中，找出有用的使用者行為樣式也是入侵偵測研究的一個方向。在駭客入侵系統手法不斷翻新的情況下，要能防禦未知型的攻擊手法是入侵偵測系統的一項重點。針對上述情況，本論文提出一適用於主機式入侵偵測之模糊關聯法則機制，利用系統記錄檔為資料來源，先以模糊群集技術將資料分群，再由此結果導出較精確的關聯法則，並將這些法則建構於異常及正常的法則資料庫中，而日後若有新資料產生，則再以模糊漸進式關聯法則對新資料進行運算，以降低產生法則所需運算的時間，並獲得最新的關聯法則。此機制的設計不但能有效率地從大量資料中，精確地建立出使用者行為樣式，在綜合異常及誤用偵測技術後，能提供入侵偵測引擎更精確地判定是否為駭客入侵行為，進而降低錯誤率，並抵擋未知型的入侵手法。而在論文最後，也將開發一套系統驗證本論文提出之機制的成效。

關鍵詞 : 入侵偵測系統、資料探勘、模糊理論、群集技術、關聯法則、漸進式資料探勘

目錄

參考文獻

[1] An Introduction to Intrusion Detection, http://www.acm.org/crossroads/xrds2-4/intrus.html [2] FBI/CSI, http://www.gocsi.com/press/20020407.html [3] R. Agrawal, T. Imielinski, and A. Swami, "Mining Association Rules between Sets of Items in Large Database," Proceedings of the ACM SIGMOD Confe- rence on Management of Data, pp. 207-216, 1993.

[4] R. Agrawal, and R. Srikant, "Fast Algorithms for Mining Association Rules in Large Databases," Proceedings 20th International Conference Very Large Data Bases, pp. 478-499, 1994.

[5] N. Ayan, A. Tansel, and E. Arkun, "An Efficient Algorithm to Update Large Itemsets with Early Pruning, " Proceedings of the 5th ACM International Conference on Knowledge Discovery and Data Mining, pp. 287-291, 1999.

[6] J. C. Bezdek, "Pattern Recognition with Fuzzy Objec- tive Function Algorithms," Plenum, New York, 1981.

[7] E. Biermann, E. Cloete, L.M. Venter, "A Comparison of Intrusion Detection systems, Computers and Security," Vol. 20, Issue8, pp. 676-683, 2001.

[8] S.M. Bridges, R.B. Vaughn, "Fuzzy Data Mining and Genetic Algorithms Applied to Intrusion Detection," National Information Systems Security Conference, pp. 13-31, 2000.

[9] D.W. Cheung, S.D. Lee, and B. Kao, "A general incremental technique for maintaining discovered association rules," Proceedings of Database Systems for Advanced Applications, pp. 185-194, 1997.

[10] D.E. Denning, "An intrusion-detection model", IEEE Transactions on Software Engineering, Vol. SE-13, pp. 222-232, 1987.

[11] J.E. Dickerson, J. Juslin, O. Koukousoula, J.A. Dickerson, "Fuzzy intrusion detection," IFSA World Congress and 20th NAFIPS International

Conference, Vol. 3, pp. 1506-1510, 2001.
[12] U. Fayyad, G. Piatetsky-Shapiro, and P. Smyth, "The KDD process for extracting useful knowledge from volumes of data." Communications of the ACM, pp. 27-34, 1996.
[13] G. Florez, S.A. Bridges, R.B. Vaughn, "An Improved Algorithm for Fuzzy Data Mining for Intrusion Detection," Proceedings of the North American Fuzzy Information Processing Society Conference (NAFIPS- 2002), pp. 457-462, 2002.
[14] E. Forgy, "Cluster analysis of multivariate data: efficiency versus interpreability of classifications," Biomertrics, Vol. 21, pp. 768, 1965.
[15] G. Helmer, J. Wong, V. Honavar, L. Miller,"Automated Discovery of Concise Predictive Rules for Intrusion Detection," Journal of Systems and Software, Vol. 60, Issue3, pp. 165-175, 2002.
[16] R. Hart, D. Morgan and H. Tran, "An Introduction to Automated Intrusion Detection Approaches," Infor- mation Management and Computer Security 7, pp. 76-82, 1999.
[17] F. Hoppner, Frank Klawonn, Rudolf Kruse, Thomas Runkler, "Fuzzy Cluster Analysis," WILEY, 1999.
[18] Y.C. Hu, R.S. Chen, G.H. Tzeng, "Discovering fuzzy association rules using fuzzy partition methods," Knowledge Based Systems, Vol. 16, pp. 147-147, 2003.
[19] M. Hossain, "Integrating Association Rule Mining and Decision Tree Learning for Network Intrusion Detection: A Preliminary Investigation," International Conference on Information Systems, Analysis and Synthesis, Vol. 11, pp. 65-70, 2002 [20] James and P. Anderson, "Computer Security Threat Monitoring and Surveillance," Technical report, James P. Anderson Co., Fort Washington, PA., 1980.
[21] M.F. Jiang, S.S. Tseng, C.M. Su., "Two-phase clustering process for outliers detection," Pattern Recognition Letters, Vol. 22, pp. 691-700, 2001.
[22] L. Kaufman and P.J. Rousseeuw, "Finding Groups in Data: an Introduction to Cluster Analysis, " John Wiley & Sons, 1990.
[23] C. S. Kuo, T. P. Hong and S. C. Chi, "A study of fuzzy data mining algorithms for quantitative values," Graduate school of Management Science I-Shou University, Thesis, 1999.
[24] C.M. Kuok, A. Fu, and M. Wong, "Mining Fuzzy Association Rules in Databases," SIGMOD record , Vol. 17, No.1, pp. 41-46, 1998.
[25] C.H. Lee, C.R. Lin, and M.S. Chen, "Sliding-Window Filtering: An Efficient Algorithm for Incremental Mining," Proceedings of the ACM 10th International Conference on Information and Knowledge Management, pp. 263-270, 2001.
[26] W. Lee, S.J. Stolfo, P. Chan, E. Eskin, W. Fan, M. Miller, S. Hershkop and J. Zhang, "Real Time Data Mining-based Intrusion Detection," Proceedings of the 2001 DARPA Information Survivability Conference and Exposition (DISCEX II), pp. 89-100, 2001.
[27] W. Lee, S.J. Stolfo, "Data Mining Approaches for Intrusion Detection," Proceedings of the 7th USENIX Security Symposium, 1998.
[28] W. Lee, S.J. Stolfo, and K.W. Mok, "Mining audit data to build intrusion detection models," In 4th International Conference on Knowledge Discovery and Data Mining, pp. 66-72, 1998.
[29] W. Lee, S.J. Stolfo and K.W. Mok, "A Data Mining Framework for Building Intrusion Detection Models," Proceedings of the IEEE Symposium on Security and Privacy, pp. 120-132, 1999.
[30] Y. Li, N. Wu, X.S. Wang ,S. Jajodia, "Enhancing Pro- files for Anomaly Detection Using Time Granul- arities," Journal of Computer Security, pp. 137-158, 2002.
[31] T. Lunt, " Detecting Intruders in Computer Systems," Proceedings of the 1993 Conference on Auditing and Computer Technology, 1993.
[32] J. Luo and Susan M. Bridges, "Mining Fuzzy Association Rules and Fuzzy Frequency Episodes for Intrusion Detection," International Journal of Intelligent Systems, Vol. 15, pp. 687-703 ,2000.
[33] J. A. Marin, J., D. J. Ragsdale, and J. R. Surdu, "A Hybrid Approach to Profile Creation and Intrusion Detection," Proceedings of the DARPA Information Survivability Conference and Exposition - DISCEX , pp. 69-76 ,2001.
[34] B. Ozden, S. Ramaswamy and A. Silberschatz, "Cyclic association rules," Proceedings of the 14th Interna- tional Conference on Data Engineering, pp. 412-421, 1998.
[35] L. Portnoy, E. Eskin, and S.J. Stolfo, "Intrusion Detection with Unlabeled Data Using Clustering," Proceedings of the ACM CCS Workshop on Data Mining for Security Applications, 2001.
[36] S. Ramaswamy, S. Mahajan, and A. Silberschatz, "On the discovery of interesting patterns in association rules," Proceedings of the International Conference on Very Large Data Bases, pp. 368-379, 1998.
[37] S. H. Rubin, "A Fuzzy Approach Towards Inferential Data mining," Computers and Engine, Vol. 35, pp. 267-270, 1998 [38] R. Smith, A. Bivens, M. Embrechts, "Clustering Approaches for Anomaly Based Intrusion Detection," Walter Lincoln Hawkins Graduate Research Confe- rence, 2002.
[39] R. Srikant and R. Agrawal, "Mining Quantitative Association Rules in Large Relational Tables," Proceedings of ACM SIGMOD International Confe- rence on Management Data, Montreal Canada, pp. 1-12, 1996.
[40] W.J. Tsaur and I-Ming Fan, "Anomaly Detection Mechanisms for Web Severs in Linux Environments," Communications of the CCISA, Vol. 8, No. 4, 2002.
[41] T. Verwoerd and R. Hunt, "Intrusion Detection Techniques and Approaches,"Computer Communications, Vol. 25, pp. 1356-1365, 2002.
[42] L.A. Zadeh. Fuzzy Sets, Information Control, Vol. 8, pp. 338-353, 1965.

[43] O.R. Zaiane, M. Xin, J. Han, "Discovering Web Access Patterns and Trends by Applying OLAP and Data Mining Technology on Web Logs," Proceedings of Advances in Digital Libraries Conference (ADL- 98), pp. 19-29, 1998.