手機病毒行為分析與偵測之研究

陳志遠、姜琇森

E-mail: 9806270@mail.dyu.edu.tw

摘 要

近年來，由於整合手機和手提式電腦的優點而形成的智慧型手機(Smartphones)已經變得越來越流行。在過去的兩年之中，已有數百種的手機病毒出現，它們能透過各式各樣的方法迅速地傳播(例如SMS/MMS, Bluetooth等)。手機病毒可能造成使用者隱私的洩漏、額外的服務費用和電池耗盡等損害。Cabir、Mabir 和CommWarrior等手機病毒的出現已經造成行動設備資訊安全儲存的威脅。因此，行動設備的安全已經成為一個重要的議題。

防毒軟體是現今保護智慧型手機的主要機制。而此類的防毒機制主要依賴「病毒碼」的更新才能預防新病毒。據研究顯示目前的手機病毒以每月六隻的速度出現，若無法在更新病毒碼之前偵測到新病毒，系統在新病毒出現時而未能即時更新的期間內是極度危險與脆弱的。現階段對於手機病毒偵測的相關研究並不多，偵測技術與病毒過濾系統的發展都仍在探討階段。有鑑於此，本研究提出一種以行為分析為基礎的偵測方法來發現未知型的手機病毒。本體論(Ontology)、模糊理論(Fuzzy theory)和關聯派翠網路(APNs)等方法論被採用來支援手機病毒偵測。本研究藉由深入分析手機病毒的特徵與動態傳播行為來建構手機病毒的行為知識本體。

關鍵詞 : 行動安全、病毒偵測、本體論、關聯派翠網路

目錄

參考文獻

一、中文部份Chung, Christina Yip(1997), A survey of misuse detection systems.
[線上資料], 來源: http://seclab.cs.ucdavis.edu/~chungy/ doc/ MDS.htm[2009, May 1].Digital Times(2007), 手機產業現況[線上資料], 來源: http:// member.digitimes.com.tw/tw/rpt/rpt_abs.asp?showType=90&CnlID=3[2009, May 1].資策會資訊市場情報中心(2007), 手機惡意程式數量持續增長[線上資料], 來源: http://mic.iii.org.tw/intelligence/member_ login.asp?sid=0&iid=0&did=92495[2009, May 1].二、英文部分Agrawal R., & Srikant R. (1994). Fast algorithms for mining association rules, Proceedings of the 20th VLDB Conference (pp.487-499), Santago, Chile.Agrawal R., Imielinski T., & Swami A. (1993). Database mining: A performance perspective. IEEE Trans. Knowledge and Data

Eng, 5(6), 914-925.Bernaras, A., Laresogiti, I. & Corera, J. (1996). Building and reusing ontologies for electrical network applications. In W. Wahlster (Ed.) European Conference on Aritficial Intelligence, Budapest, Hungary, 298-302.Bose, A. & Shin, K. G., (2006). On mobile viruses exploiting messaging and bluetooth services. IEEE Securecomm and Workshops, (pp.1-10), New York.Bunge, M. (1977). Ontology I : The furniture of the world. Treaties on basic philosophy, 3, Boston, Mass: D. Reidel Publishing.Chandrasekaran B., Josephson J. R., & Benjamins, V. R. (1999). What are ontologies, and why do we need them? IEEE Intelligent Systems, 14(1), 20-26.Choi, Y. B., Bache, T. C., & Hill, L. L. (2007). The pricing of wireless phone services in the USA: Issues and development trends. International Journal of Mobile Communications, 5(2), 169-185.Christensen R. (1980). Entropy minimax sourcebook, Entropy Ltd., Lincoln, Massachusrtts.Dagon, D., Martin, T., & Starner, T. (2004). Mobile phones as computing devices: The viruses are coming. IEEE Pervasive Computing, 3(4), 11-15.Fernandez-Lopez, M., Gomez-Perez, A., Sierra, J. P., & Sierra, A. P. (1999). Building a chemical ontology using methontology and the ontology design environment. IEEE Intelligent Systems, 14(1), 37-46.Gruninger, M., & Fox, M. S. (1995). The logic of enterprise modeling, In J. Brown and D. O ' Sullivan (Series Ed.), Reengineering the Enterprise Chapman & Hall , 83-98.Guarino, N., & Welty, C. (2000). A formal ontology of properties, In R.Dieng & O. Corby (eds). Proc. of the 12th European Workshop on Knowledge Acquisition, Modeling and Management, London, 1937(pp.97-112).John, Y. J., & Gorman, G. E. (2002). Internet use in south korea. Online Information Review, 26(5), 335-344.Lee, J. S., Hsiang, J., & Tsang, P. H. (1997). A generic virus detection agent on the Internet, Proc. of the Thirtieth Hawaii International Conference on System Sciences, 4, 210-219.Luke, J., & Harris, C. J. (1999). The application of CMAC based intelligent agents in the detection of previously unseen computer viruses. International Conference on Information Intelligence and Systems, 662-666.Matthew G. S., Eleazar E., Erez Z., Manasi B., & Salvatore J. S. (2001). Malicious email filter-A UNIX mail filter that detects malicious windows executables. In Proc. of USENIX Annual Technical Conference – FREENIX Track. Boston, Massachusrtts:June.McAfee, white paper (2007). McAfee avert labs top 10 Threat Predictions for 2008. [Online]. Available: http://www.mcafee. com/us/local_content/white_papers/threat_center/wp_avert_predictions2008.pdf[2009, May 1].McGraw, G., Morrisett, G. (2000). Attacking malicious code : A report the infosec reserch council. Software, IEEE, 17(5), 33-41Morales, J. A., Clarke, P. J., Deng, Y., & Kibria, B. M. G. (2006). Testing and evaluating virus detectors for handheld devices. Journal in Computer Virology, 2(2), 135-147.Murata, T. (1989). Petri nets: Properties, analysis and application. Proceedings of the IEEE, 77(4), 541-580.Neches, R., Fikes R. E., Finin T., Gruber T. R., Senator, T., & Swartout W. R. (1991). Enabling technology for knowledge sharing, AI Magazine, 12(3), 36-56.Okanmoto, T., & Ishida, Y. (2002). An analysis of a model of computer viruses spreading via electronic mail. Systems and computers in Japan, 33(14), 2002.Pelaez, C. E., Bowles, J. (1991). Computer viruses, southeasterm Symposium, 23(10-12), 513-517.Phillippo, S. J. (1990). Practical virus detection and prevention. Viruses and their Impact on Future Computing Systems, IEE Colloquium on (pp. 2/1 -2/4), London.Rhodes C., & Nekovee M. (2008). Statistical mechanics and its applications. Physica A, 387(27), 6837-6844.Ross T. J. (2000). Fuzzy logic with engineering applications. McGraw-Hill, USA,.Shih, D. H., Chiang, H. S., & Yen, D. C. (2005). Classification methods in the detection of new malicious emails. Information Sciences, 172(1-2), 241-261.Shih, D. H., Chiang, H. S., & Chan, C. Y. (2004). Internet security: malicious emails detection and protection. Industrial Management and Data Systems, 104(7), 613-623.Shih, D. H., Chiang, H. S., & Lin B. (2007). A gneralized associative petri net for reasoning. IEEE Trans. Knowledge and Data Eng, 19(9), 1241-1251.Staab, S., Schnurr, H. P., Studer, R., & Sure, Y. (2001). Knowledge processes and ontologies. IEEE Intelligent Systems, 16(1), 26-34.Swarout, B., Ramesh, P., Knight, K., & Russ, T. (1997). Toward distributed use of large-scale ontology. In A.Farquhar, M. Gruninger, A. Gome-Perez, M. Uschool & ven der Vet P(Eds.), (pp138-148), AAAAI ' 97 Spring Symposium Series on Ontological Engineering, California:Stanford University.Teck Sung Yap, Hong Tat Ewe (2005). A mobile phone malicious software detection model with behavior checker. Springer-Verlag Berlin Heidelberg 2005, 57-65.Tesauro, G., Kephart, J. O., & Sorkin, G. B. (1996). Neural networks for computer virus recognition. IEEE Expert, 11(4), 5-6.T?yssy, S., & Helenius, M. (2006). About malicious software in smartphones. Journal in Computer Virology, 2(2), 109-119.Trend Micro, white paper (2006).The trend of threats today: 2005 annual roundup and 2006 forecast. [Online]. Available: http://www.pressebox.de/attachment/12230/TM_PI_Virenreport_2005.pdf[2009, May 20].Trend Micro, white paper (2007). The trend of threats today: 2007 annual roundup and 2008 forecast. [Online]. Available: http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/tre_threat_report.pdf[2009, May 20].Uschold, M., King, M., Moralee, S. & Zorgios, Y. (1995). The enterprise ontology. The Knowledge Engineering Review, 13(1), 31-89.Xie, L., Song, H., Jaeger, T., & Zhu S. (2008). A systematic approach for cell-phone worm containment. International World Wide Web Conference(pp.1083-1084), New York.Yang, J., He, X., & Lee, H. (2007). Social reference group influence on mobile phone purchasing behaviour: a cross-nation comparative study. International Journal of Mobile Communications, 5(3), 319-338.Yap, T. S., & Ewe, H. T. (2005). A mobile phone malicious software detection model with behavior checker. Lecture Notes in Computer Science, 3597, 57-65.Zenkin, D. (2001). Guidelines for the protecting the corporate against viruses. Computers & Security, 20, 671-675.Zheng, H., Li, D., & Gao, Z. (2006). An epidemic model of mobile phone virus. 2006 1st International Symposium on Pervasive Computing and Applications(pp.1-5), New York.