A Study of Mobile Phone Virus Behavioral Analysis and Detection

陳志遠、姜琇森

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

ABSTRACT

Smartphones have recently become increasingly popular because they provide “ all-in-one ” convenience by integrating traditional mobile phones with handheld computing devices. In fact, hundreds of mobile viruses have emerged in the past two years, which can quickly spread through various means such as SMS/MMS, Bluetooth and traditional IP-based applications. Mobile viruses can cause the leakage of user privacy, extra service charges and depletion of battery power. Recent occurrences of mobile viruses like Cabir, Mabir and CommWarrior have created growing concerns over the security of data stored on mobile devices such as smart phones and PDAs. Thus, mobile devices security becomes an important issue.

Currently, anti-virus software is the primary mechanism to prevent computers from the damage of virus. Such mechanism relies on the update of virus signature to detect a new virus. However, six mobile viruses are created every month and most cannot be accurately detected until signatures have been generated for them. During this time period, systems protected by signature-based algorithms are vulnerable to attacks. Therefore, we plan to propose a behavioral detection method to detect unknown viruses. In our methodology, Ontology is adopted to support the behavioral description of mobile viruses. We try to study these characteristics and spreading behaviors of mobile virus in-depth analysis. Next we adopt the fuzzy theory and Associative Petri Net methods to construct a model.

Keywords : mobile security、virus detection、ontology、associative petri net

Table of Contents

REFERENCES

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.