An Assessment Study of Virus Detection Techniques on Mobile Platform

楊智傑、姜琇森

E-mail: 322092@mail.dyu.edu.tw

ABSTRACT

The various portable mobile devices have recently become increasingly popular, especially Smartphone. In fact, hundreds of cell phone viruses have emerged in the past two years. The cell phone viruses targets industrial secrets and had caused the leakage of user privacy and enterprise ’s secrets. Thus, mobile devices security becomes an important issue. The virus detection needs to take the quite huge resources. However, the system resources are limited in a mobile platform. How to use the least system resources to gain the detection effect is a big challenge. Presently most of researches about cell phone viruses are focus on virus detection techniques development and the studies considerate the detection capability of cell phone viruses and resources consumption are less simultaneously in a mobile platform. In this study, we conduct a set of experiments to evaluate and analyze performance of the virus detection techniques (Bayesian network (BN), detection tree C5.0 and neural network) by utilizing five kinds of evaluation indexes. The five kinds of evaluation indexes are detection rate, false positive rate, overall accuracy rate, resources consumption and energy consumption. We collect 40 types of cell phone viruses (79 cell phone viruses) that are used to evaluate the detection capability of these techniques. In order to find out the best detection technique, we analysis the performance of these techniques in a mobile platform through detection rate, false positive rate, overall accuracy rate, and Receiver Operating Characteristic (ROC) curve. The detection tree C5.0 is better than other methods. Thus, we development a viruses filtering system base on detection tree C5.0 in the HTC HD2 cell phone with windows mobile 6.5. By experiment design, the 27 cell phone viruses that propagate with MMS are used to test the detection capability and the resources consumption and energy consumption in the detection process. Our experimental results give some practical and useful guidelines to mobile security researchers, so that they can acquire insight to apply these techniques to the area of cell phone virus detection in the mobile platform and devise more effective virus detection models.

Keywords : mobile platform、cell-phone viruses、data mining、detection evaluation

Table of Contents

REFERENCES

一、中文部份 李駿偉(2001)，入侵偵測系統分析方法效能之定量評估，私立中原大學資訊工程研究所未出版之碩士論文。 姜琇森，曹偉駿(2009)，行動惡意軟體行為分析與偵測技術之研究，資訊安全通訊，15(4)，30-51。 陳志遠(2009)，手機病毒行為分析與偵測之研究，私立大葉大學資訊管理研究所未出版之碩士論文。 陳展維(2003)，基於平滑支援向量機之電腦病毒偵測系統，國立台灣科技大學資訊工程研究所未出版之碩士論文。 謝侃盛(2009)，結合One-Class 與Multi-Class SVM之入侵偵測系統，私立開南大學資訊及電子商務研究所未出版之碩士論文。 二、英文部分 Bose, A., Hu, X., Shih, K. G., & Park, T. (2008). Behavioral detection of malware on mobile handsets. In D.

Grunwald (Ed.), Proceeding of the 6th international conference on mobile systems, applications, and services (pp. 255-238), New York: ACM. Cheng, J., C., Wong, S. H. Y., Yang, H., & Lu, S. (2007). Smartsiren: virus detection and alert for smartphones. In E. Knightly (Ed.), Proceeding of the International conference on mobile systems, applications, and services (pp. 28-32), San Juan: Puetro Rico. Chiang, H. S., & Tsaur, W. J. (2009). Ontology-based Mobile Malware Behavioral Analysis. The Fourth Joint Workshop on Information Security, Kaohsiung, Taiwan: National Sun Yat-sen University. Cooper, G. F. (1984). NESTOR:A Computer-Based Medical Diagnostic That Integrates Causal and Probabilistic Knowledge. (HPP-84-48), California, Stanford: Stanford university, 437-451. Dunham, M. H. (2002). Data mining introductory and advanced topics. Upper Saddle River, New Jersey: Pearson education. F-Secure (2010). Antivirus software, internet security, anti spyware, virus protection & removal tool [Online]. Available: http://www.f-secure.com/ [2010, Marcy 16]. ITSX (2010). Information technology security experts [Online]. Available: http://www.itsx.com/ [2010, May 22]. Kim, H., Smith, J., & Shih, K. G. (2008).Detecting energy-greedy anomalies and mobile malware variants. In D. Grunwald (Ed.), Proceeding of the 6th international conference on Mobile systems, applications, and services (pp. 239-252), New York: ACM. Khayam, S. A., & Radha, H. (2005). A topologically-aware worm propagation model for wireless senor networks, Proceeding of the 25th IEEE International Conference on Distributed Computing Systems Workshops (pp. 210-216), Columbus, Ohio: IEEE computer society. Lauritzen, S. L.,& Spiegelhalter, D. J. (1988). Local computations with probabilities on graphical structure and their application to expert systems. Journal of the Royal Statistical Society, 15(5), 415-433. McGraw, G., & Morrisett, G. (2000). Attacking malicious code: a report to the infosec research council. IEEE Software, 17(5), 33-41. Mickens, J. W., & Noble, B. D. (2005). Modeling epidemic spreading in mobile environments. In M. Jakobsson & R. Poovendran (Eds.), Proceedings of the 4th ACM workshop on Wireless security (pp. 47-53), Cologne, Germany: ACM SIGMobile. Moran, C. J., & Bui, E. N. (2002). Spatial data mining for enhanced soil map modeling. International Journal of Geographical Information Science, 15(5), 533-549. Pearl, J. (1988). Probabilistic reasoning in intelligent systems: networks of plausible inference. San Francisco, California: Morgan Kaufmann publishers. Pelaez C. E., & Bowles, J. (1991). Computer viruses. Proceedings of the Twenty-Third Southeastern Symposium on System Theory (pp. 513-517), Columbia, South Carolina: IEEE computer society. Ruitenbeek, E. V., Courtney, T., Sanders, W. H., & Stevens, F. (2007). Quantifying the effectiveness of mobile phone virus response mechanisms. In T. Hoare (Ed.), Proceedings of the 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (pp. 790-800), Edinburgh, United Kingdom: IEEE computer society. Schmidt, A., Peters, Lamour, F. F., Scheel, C., Camtepe S. A., & Albayrak, S. (2009). Monitoring smartphones for anomaly detection. Mobile Networks and Applications, 14(1), 252-256. Shih, D. H., Lin, B., Chiang, H. S., & Shih, M. H. (2008). Security aspects of mobile phone virus: a critical survey. Industrial Management and Data Systems, 108(4), 478-494. Symantec (2010). Antivirus, anti-spyware, endpoint security, backup, storage solutions [Online]. Available: http://www.symantec.com/index.jsp [2010, May25]. Taejoon P., & Shih, K. G. (2005). Soft tamper-proofing via program integrity verification in wireless sensor networks. IEEE Transactions on Mobile Computing, 4(3), 297-309. Tan, P. N., Steinbach, M., & Kumar, V. (2006). Introduction to data mining. Boston, Massachusetts: Addison-Welsey. Toyssy S., & Helenius, M. (2006). About malicious software in smartphones. Journal in Computer Virology, 2(2), 109-119. Microsoft MSDN Library (2010). WindowsMobile.Status Namespace [Online]. Available: http://msdn.microsoft.com/en-us/library/microsoft.windowsmobile.status.aspx [2010, May 3]. Yap, T. S., & Ewe, H. T. (2005). A mobile phone malicious software detection model with behavior checker. Lecture Notes in Computer Science, 3597(1), 57-65. Zenkin,D. (2001). Fighting against the invisible enemy. Computers & Security, 20(4), 316-321. Zheng, H., Li, D., & Gao, Z. (2004). An epidemic model of mobile phone virus. In R. P. Luijten, L. A. DaSilvaL, & A. P. J. Engbersen (Eds.), Proceedings of the International Conference on Computer Communications And Network (pp. 1-5), Chicago, Illinois: IEEE computer society.