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

第一章  緒論...................1   第一節  研究背景...............1
第二節  研究動機...............3   第三節  研究目的...............4
第四節  研究流程...............4 第二章  文獻探討.................6
第一節  手機病毒定義.............6   第二節  手機病毒之發展............6
第三節  手機病毒類別介紹...........8   第四節  手機病毒偵測相關之研究.......
第三章  手機病毒.............. 21   第五節  學習方法之介紹............15
第一節  手機病毒行為分析...........21   第四章  實驗與討論................31   第二節  手機病毒行為特徵之分析...
第二節  手機病毒行為特徵之分析...26 第三節  手機樣本資料之轉換..........35
第四章  實驗與討論................31   第四節  實驗設計與分析.          37
第一節  實驗環境與開發工具...      32   第五章  行動平台效能之分析............44
第二節  異常及正常樣本之收集.........33   第一節  系統效測量方法............46
第三節  多媒體訊息病毒之行為特徵 ....34   第二節  電池效能測量方法...........48
第四節  手機樣本資料之轉換..........35   第三節  實驗結論...............49
第五章  行動平台效能之分析............44   第一節  結論...............50
第二節  系統效測量方法............44   第二節  未來研究...............51
第六章  結論...................50   第一節  結論...............50
第二節  未來研究...............51 參考文獻 ..

REFERENCES


