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

中文摘要 ..................... iii
英文摘要 ..................... iv
致謝辭  ..................... v
內容目錄 ..................... viii
表目錄  ..................... ix
圖目錄  ..................... ix
第一章  緒論................... 1
第一節  研究背景與動機............ 1
第二節  研究目的............... 4
第二章  文獻探討................. 5
第一節  手機病毒定義............. 5
第二節  手機病毒的偵測方法.......... 8
第三章  研究方法與步驟.............. 14
第四章  手機病毒行為分析............. 33
第一節  樣本資料收集............. 33
第二節  行為分析............... 34
第五章  實驗與討論................ 48
第一節  實驗設計與流程............ 48
第二節  實驗結果評估與討論.......... 50
第六章  結論與貢獻................ 59

REFERENCES
