Investigation Leading to Behaviour-Based Hybrid Intrusion Detection System for Mobile Devices

A short abstract if you have one, or a link to your research if you have a web page

Smartphones nowadays have become immensely popular because they provide All-In-One expediency by integrating traditional mobile phones with hand-held computing devices making them more open and general purpose. However this flexibility leaves the Smartphones prone to attacks by malicious hackers. In the past few years, hundreds of malware have appeared to target these devices propagating through various means including SMS/MMS, Bluetooth and traditional IP-based applications. These malware not only pose a threat to mobile system data confidentiality, availability and integrity but can result in unwanted billing, depletion of battery power and denial-of-service (hereafter DOS) attack by generating malicious traffic hence seriously crippling the mobile network and service capacity.

Current Smartphones malware detection and prevention techniques are limited to Signature-Based antivirus scanners (hereafter SIDS). These can efficiently detect malware with a known signature, but they have serious shortcomings with new and unknown malware creating a window of opportunity for attackers. As Smartphones have become host for sensitive data and applications, extended malware detection and prevention techniques are necessary complying with the corresponding resource constraints.

A framework for Behaviour-Based Hybrid Intrusion Detection System is proposed to circumvent these shortcomings. This framework aims to provide protection against physical misuse using Machine Learning technique and detection of malicious applications using Knowledge Based Temporal Abstraction method. This research will be among the first to combine these two methods. Being platform independent is another novelty of the framework. A prototype has been partially implemented on Google Android and tested on emulators. Further validation will be performed on Smartphones to benchmark this framework.

Your field of study (or department or faculty)
Faculty of Computing

The number of years you have been working on your research
2 and a half years

The number of years (or months) that you think will be required to work on your research before submission
6 months