Analysis of Energy Profiles for Malware Detection in Mobile Environment

Ali Abdulmadzhidov, Emil Sharifullin

System and Network Engineering, Innopolis University

December 11, 2016

Abstract

> Mobile devices, like smartphones or IoT, are very popular nowadays. So is malware development targeted at them. There're various methods of detecting those malicious software: signature based, dynamic, heuristic e.t.c. In addition, we have a quite new way to recognise malware by the energy profile of the process. It is based on the fact that we can measure energy consumption of "healthy" device and having it as ideal, detect any suspicious processes that can have malicious properties.
>
> In this paper, we are going to check is it possible to detect different types of real or artificial-malware. As proof we'll try to implement research results in antivirus software based on the energy profile analyse method.

1. Introduction

Nowadays, mobile devices are very popular and their "expansion" is growing. In addition to usual smartphones, we have IoT that also uses same mobile OSs (iWatch, Samsung Gear). As a result, users trust very sensitive data to them, gave access to their bank accounts e.t.c. This fact makes mobile devices sweet target for developers of malware. According to McAfee mobile threat report [1], there're 1000 - 6000 virus detected per hour in various countries.

Currently we have many methods for finding malicious software: signature based, dynamic, heuristic, and so forth. Several researches proposed new way of detecting malware based on energy profile analyse. The main idea is, that every process has it's own energy consumption fingerprint and we can detect any unpredictable and suspicious activity comparing with "ideal" energy profile.

2. Related Work

For now few researchers has touched this theme.

Kim et al. **[2]** presented the way of detecting malware based on energy consumption. They proposed framework for finding and analysing energy-greedy anomalies on Windows Mobile OS using power signatures. Need of energy signatures prevent them from detecting new, unknown malware.

Liu et al. **[3]** proposed heuristic solution for devices on Symbian OS. Firstly tool writes user's behaviour and energy consumption on clean system and then real power usage is compared with that profile and if threshold is reached, tool supposes that malware is detected.

Hoffmann et al. **[4]** discussed the way to get energy fingerprints of different proccesses and then use them to detect and analyze malware.

3. Research Goals

- Prove or disprove ability of detection malicious behaviour based on energy consumption
- Draw relation between different types of malware and the energy consumption
- Implement research results into virus detection application

4. References

[1] http://www.mcafee.com/us/resources/reports/rp-mobile-threat-report-2016.pdf
[2] H. Kim, J. Smith, and K. G. Shin. Detecting Energy-Greedy Anomalies and Mobile Malware Variants. In International Conference on Mobile Systems, Applications and Services, MobiSys, 2008
[3] L. Liu, G. Yan, X. Zhang, and S. Chen. VirusMeter: Preventing Your Cellphone from Spies. In International Symposium on Recent Advances in Intrusion Detection, RAID, 2009.
[4] J. Hoffmann, S. Neumann, T. Holz. Mobile Malware Detection Based on Energy Fingerprints — A Dead End? Horst Gortz Institute (HGI), Ruhr-University Bochum, Germany 2013