Assignment No 1

ANDROID MALWARE ANALYSIS

5 Research Papers Reviews.

**Research Methodology**

By

**Wasim Ahmad**

[wahmad@uetpeshawar.edu.pk](mailto:wahmad@uetpeshawar.edu.pk)

*3rd Semester MS Computer Science*

To

**Dr. Laiq Hasan**

**University of Engineering and Technology, Peshawar.**

1. **Static malware detection and attribution in android byte-code through an end-to-end deep system (** [**Click Here**](https://drive.google.com/file/d/1J_cILLhIUAUezUKT9diyKTh-3z8ykawJ/view?usp=sharing) **)**

**Contributions:**

As a remedy in this paper, they resolve the dilemma of Android malware detection and attribution through a proposed anti-malware system of deep learning models. The details for design, customization and implementation of all these models, whereas the motivation backing the selection of these models and hyper parameters are given section wise. For experiments, this paper also augment a large dataset of op-codes extracted from Android package kit(apks) and victories them through one-hot encoding. We aim to make this dataset freely available on demand.

**Limitations:**

Note that certain malware may just be perceivable by examining different aspects of an apks payload. Our rationality is to judge how far we can go with our technique while maintaining simplicity in the input. Our work can definitely be extended in future while taking into the account of other elements in the payload of an app.

1. **A TAN based hybrid model for android malware detection. (** [**Click Here**](https://drive.google.com/file/d/1D_VLOIGibMD_TUh7UTWVZz89Q3bi_8rj/view?usp=sharing) **)**

**Contributions:**

In this paper, proposed a novel mechanism for detecting Android malware applications by combining static and dynamic features influencing the malicious activity by exploring their conditional dependencies. The proposed mechanism can accurately capture the malicious behavior than existing static and dynamic analysis mechanisms. The tested applications are installed in the emulator and system call logs are collected. Then, these extracted features are transformed into the corresponding feature vector using a python code.

**Limitations:**

They didn’t describe the tools that they used for malware application detection in different android application. Used low level machine learning models for the analysis. Mostly they analysis with the help of API calls.

1. **Android Malware Detection based on Vulnerable Feature Aggregation. (** [**Click here**](https://drive.google.com/file/d/1YnFxaKerpWdnSC-8FtpAugSkUWtMgCYh/view?usp=sharing) **)**

**Contributions:**

This paper propose a light-weight malware detection framework that operates upon only 50 features. In this research the proposed system address the issue of temporal bias that exists in most of the prevailing malware detection approaches using machine learning. They do this by training their model on the standard DREBIN data set collected in the period of August 2010 to October 2012, and validating on a data-set that was collected in 2014.

The main limitation of this paper is they used very old and limited data. They used few Machine learning modals and also they used few android malware analysis tools while there are many tools available in market.

1. **Black box analysis of android malware detectors. (** [**Click here**](https://drive.google.com/file/d/1FI0Fc9HsFUhYfCz8KsVmnQDhltZUmsgI/view?usp=sharing) **)**

**Contributions:**

This paper results clearly show that fairly straightforward obfuscation techniques can be highly effective against a collection of strong malware detectors available on Virus Total. This research paper also indicate that there is a high degree of diversity among these malware detectors, in the sense that no single feature—or even a combination of features—seems to dominate the overall detection results. In addition, there appears to be some diversity even within a single malware detector, in the sense that different malware samples often yield different obfuscation profiles with respect to a given antivirus.

**Limitations:**

This research paper Test limited APKs.

1. **On machine learning effectiveness for malware detection in Android OS using static analysis** **data**

([**Click here**](https://drive.google.com/file/d/1ENbRX-OtqXkMagavGO0vuoe_6PnJGATz/view?usp=sharing))

**Contributions:**

In this paper evaluate the effectiveness and adequacy of well-known ML classifiers when applied on Android malware classification. More in this paper report on the most significant raw features over which each classifier builds its decision-making mechanism. This research also provide a detailed analysis of other similar related works. In this paper software for accomplishing the related analysis is freely available upon request. I believe this can facilitate other researchers to carry out similar analysis or reproduce the reported results.

**Limitations:**

This research paper only used the static method of android malware analysis and also used most of old techniques and the numbers of date are less.

THE END