MADAM: Effective and Efficient Behavior-based Android Malware Detection and Prevention

Abstract:

Android users are constantly threatened by an increasing number of malicious applications (apps), generically called malware. Malware constitutes a serious threat to user privacy, money, device and file integrity. In this paper we note that, by studying their actions, we can classify malware into a small number of behavioral classes, each of which performs a limited set of misbehaviors that characterize them. These misbehaviors can be defined by monitoring features belonging to different Android levels. In this paper we present MADAM, a novel host-based malware detection system for Android devices which simultaneously analyzes and correlates features at four levels: kernel, application, user and package, to detect and stop malicious behaviors. MADAM has been designed to take into account those behaviors characteristics of almost every real malware which can be found in the wild. MADAM detects and effectively blocks more than 96% of malicious apps, which come from three large datasets with about 2,800 apps, by exploiting the cooperation of two parallel classifiers and a behavioral signature-based detector. Extensive experiments, which also includes the analysis of a testbed of 9,804 genuine apps, have been conducted to show the low false alarm rate, the negligible performance overhead and limited battery consumption.
Existing system:

It has been recently reported[1] that almost 60% of existing malware send stealthy premium rate SMS messages. Most of these behaviors are exhibited by a category of apps called Trojanized that can be found in online marketplaces not controlled by Google. However, also Google Play, the official market for Android apps, has hosted apps which have been found to be malicious[2]. Along with the vast increase of Android malware, several security solutions have been proposed by the research community, spanning from static or dynamic analysis of apps, to applying security policies enforcing data security, to run-time enforcement. However, these solutions still present significant drawbacks. In particular, they are attack-specific, i.e. they usually focus on and tackle a single kind of security attack, e.g. privacy leaking, or privilege escalation (jail-breaking). Moreover, these frameworks generally require a custom OS. Apart from these ad hoc security solutions, in an attempt to limit the set of (dangerous) operations that an app can perform, Android has introduced its native security mechanisms in the form of permissions and apps isolation.

Disadvantage:

✓ Both permissions and isolation mechanisms have shown weaknesses
Proposed system:

The main novelty of MADAM is its cross-layer approach, and a novel integration of techniques (some of which already existing) that provides high efficacy with low overhead. MADAM has been conceived to prove that a multilevel approach makes it possible to dynamically detect most of current Android malware, right on the device with limited overhead. To verify that such approach is indeed viable, a large extensive set of tests have been performed to prove empirically its efficacy.
Advantages:

✓ MADAM is able to detect misbehaviors from malware behavioral classes that consider 125 existing malware families, which encompass most of the known malware.

✓ To the best of our knowledge, MADAM is the first system which aims at detecting and stopping at run-time any kind of malware, without focusing on a specific security threat, using a behavior-based and multi-level approach. Not only the accuracy of the runtime detection of MADAM is very high, but it also achieves low performance (1.4%) and energy overhead (4%).

Conclusion:

Starting from the end of 2011, attackers have increased their efforts toward Android smartphones and tablets, producing and distributing hundreds of thousand of malicious apps. These apps threaten the user data privacy, money and device integrity, and are difficult to detect since they apparently behave as genuine apps bringing no harm. This paper proposes MADAM, a multi-level host-based malware detector for Android devices.
Hardware Specification:

- System: Pentium IV 2.4 GHz.
- Hard Disk: 40 GB.
- Floppy Drive: 44 Mb.
- Monitor: 15 VGA Colour.
- Mouse: Logitech
- Ram: 512 Mb.
- MOBILE: ANDROID

Software Specification:

- Coding Language: Java 1.7
- Tool Kit: Android 2.3 ABOVE
- IDE: Android Studio
Reference:


