Security of Android apps

Olga Gadyatskaya

University of Luxembourg
olga.gadyatskaya@uni.lu

Thesis Details

Android is a booming eco-system with zillions of third-party apps, many app markets, various devices and multiple platform versions. With a high probability you yourself own (at least) one Android device. Why do not spend your Master thesis work pondering about Android security, and trying to improve it?

Below are some tentative thesis topics. In the SaToSS group, we have everything you need to start investigating Android: app datasets, devices, and tools. Android is not as complex as you might think of it. Usually, you will need to learn to install apps on a device/emulator, you will need to run and write relatively small Python programs, and you will need to understand some basic Machine Learning tools. If you are interested and want to spend more time on it, we can discuss about a student job.

Topic 1: Resource-based repackaging detection

Android apps are sources of revenue for their developers, yet it is very easy to plagiarize a third-party app by *repackaging* it. In this thesis you will design a new scheme for detecting repackaged Android apps by using resource files included in the packages. Resource files, such as images, strings, xml layouts, have shown their potential in detecting cloned apps [4]. Subsequent experiments have shown that particular resource file types can serve as better indicators of repackaging. This study, a result of a previous successful Master project, is published in [1]. In your thesis, you will focus on further improvements of the method. The improvements can be in the direction of *robustness* (currently it is very easy for the adversaries to slightly modify the resource files so that the method does not recognize them as identical); *scalability* (improving the performance by moving from pair-wise app comparison to search of the nearest neighbours in some ordered space); or you may focus on developing a *hybrid approach* that will fuse the resource-based detection with some code-based repackaging detection technique.

Details: 60% of time will be dedicated to research, and 40% to development of a prototype to validate the proposed approach. These figures are tentative, and can be further revised depending on how the research will develop.

Topic 2: Dataset building

One of the most challenging tasks in doing Android security is to collect the right dataset to validate the developed approach. In your thesis you will work on collecting a dataset of third-party apps to share with the community. The dataset will be focused on a particular task: *repackaged app detection* (a set of confirmed repackaged and non-repackaged app pairs [1]); *evolution of Android apps* (we want to collect many last-generation apps and check how do they cope with the recent changes in the Android platform architecture [3]); or *malware detection* (a representative set of recent malware samples). Dataset collection typically involves crawling apps from app markets, and querying different online services (e.g., VirusTotal).

Details: tentatively, 50% practical research; 50% development and querying online services.

Topic 3: App code analysis for anomaly detection

This thesis will focus on applying static analysis tools (e.g., [2, 5]) to Android apps in order to detect anomalies (e.g., malicious behaviors). Some theoretical work can also be considered (developing of a semantic model of Android apps expressed as a graph or a state machine).

The thesis work will be a part of the COMMA project (see my website for more details `http://satoss.uni.lu/members/olga/`). You will interact with other project members and will participate in project meetings.

Details: tentatively, 60% research, 40% development and experiments.

References

1. Gadyatskaya, O., Lezza, A.L., Zhauniarovich, Y.: Evaluation of resource-based app repackaging detection in Android. In: Proc. of NordSec. Springer (2016)
2. Zhauniarovich, Y., Ahmad, M., Gadyatskaya, O., Crispo, B., Massacci, F.: StaDynA: Addressing the problem of dynamic code updates in the security analysis of Android applications. In: Proc. of CODASPY. ACM (2015)
3. Zhauniarovich, Y., Gadyatskaya, O.: Small changes, big changes: An updated view on the Android permission system. In: Proc. of RAID. Springer (2016)
4. Zhauniarovich, Y., Gadyatskaya, O., Crispo, B., Spina, F.L., Moser, E.: FSquaDRA: Fast detection of repackaged applications. In: Proc. of DBSec. LNCS, vol. 8566, pp. 130–145. Springer (2014)
5. Zhauniarovich, Y., Philippov, A., Gadyatskaya, O., Crispo, B., Massacci, F.: Towards black-box testing of Android apps. In: Proc. of Software Assurance Workshop at ARES. IEEE (2015)