FireMarking:Security-oriented suggestion system of Android applications

Kuniaki Katou (1210017)

School of Information Science,
Japan Advanced Institute of Science and Technology

March 20, 2015

Keywords: Android,secuirty.

The damage reports caused by Android malware are increasing recently. The report of G Data Inc. say it is increasing damages caused by Android applications annoying actions for users.The report of McAfee Inc. say it is increasing Android malware that abused weakness of regular services and applications to deceive application store and security products.So, Android markets of current security level is low.In addition, the report of Symantec Inc. say the increasing of Android malware is caused by consciousness of Android users.

From these three reports, I think that there are two causes of the expansion of the damage by the Android malwares. First, Android users cannot install applications by decision making based on sufficient information. Second,Android markets are not properly managed by the managers of that. This study suggests FireMarker to solve these two problems. FireMarker is security-oriented suggestion system that expresses the tendency of the Android markets statistically, and output risks of using Android markets and applications based on that tendency.

I divided users of FireMarker into three groups due to two problems and related works. These are Binarian and Analyst, End-user. Binarian want want to information occurred when they operated applications. Analyst analyzes the tendency of Android markets. End-user want to useful information of Android markets and applications for them.

I guessed their demands and thought conditions for satisfying them. As a result, FireMarker should be met the following three conditions. First, FireMarker controls Many computer and Android terminals to collect much information of applications. Second, it automatically moves applications to get information to occur when users operated applications. Third, it analyzes and evaluates, visualizes information to show risks of Android markets and applications for users. I designed FireMarker that has two systems. They are MarketDrone that investigates Android markets and digitize the tendency of them and FireMarking that output risks of Android markets and applications to users.

MarketDrone has four elements, Crawler and Dispatcher, Filter, Controller. Crawler downloads applications from Android markets. Dispatcher collects system logs and traffics occurred when other operated applications using many computers and Android terminals. Filter digitizes the tendency to Android markets based on system logs or traffics. Controller controls Crawler and Dispatcher, Filter and automates these processes. FireMarking outputs risks of Android markets and applications using the information output by MarketDrone.

This study implemented Crawler and Dispatcher, Filter among FireMarker as follows. I implemented Crawler that download application from Android markets called APKTOP. And I use existing crawler that download application from Android markets OperaMobileStore. I thought two designs, pattern A to pursue increasing the processing speed of a system and pattern B which made much of availability and implemented them. I implemented Filter that pay attention to the forced end and a demand of the administrator rights, FQDN, annoying advertisements and sort system logs or traffic of applications and digitize them.

Next, I made experiments to investigate Android markets called APKTOP and OperaMobileStore using these systems. The result of experiments show that four applications have the Adware in APKTOP and eight applications have the Adware in OperaMobileStore. Otherwise, some applications have advertising such as Estonia, Chinese, Russian and so on. And an application is trojan in APKTOP. As a result,FireMarker indicates OperaMobileStore is safer than APKTOP for Android users.

Finally, I organized the problems become clear by this experiment and discussed about those solutions. In that, I showed the method to evaluate risks of Android markets and applications from this results. FireMarker is possible as follows. Binarian are able to inspect the method suggested by them using a lot of applications. And they use the information of Android market as a data set by publishing the information to investigate each Android markets. Analyst get to the number of applications that require administrative rights or force a shutdown or show annoying ad, kinds of FQDN and so on. As a result, they find out the trend of Android markets easily. End-user are able to confirm the safety of Android markets and determine whether to use the Android applications in the Android markets.