Towards Privacy Risk Analysis in Android Applications Using Machine Learning Approaches

Kavita Sharma, Department of Computer Engineering, National Institute of Technology, Kurukshetra, India
B. B. Gupta, Department of Computer Engineering, National Institute of Technology, Kurukshetra, India

ABSTRACT

Android-based devices easily fall prey to an attack due to its free availability in the android market. These Android applications are not certified by the legitimate organization. If the user cannot distinguish between the set of permissions requested by an application and its risk, then an attacker can easily exploit the permissions to propagate malware. In this article, the authors present an approach for privacy risk analysis in Android applications using machine learning. The proposed approach can analyse and identify the malware application permissions. Here, the authors achieved high accuracy and improved F-measure through analyzing the proposed method on the M0Droid dataset and completed testing on an extensive test set with malware from the Androzoo dataset and benign applications from the Drebin dataset.

KEYWORDS

Android App Analysis, Android Permission, Mining, Permission Analysis, Risk Score, Static Analysis, String Matching

1. INTRODUCTION

In modern times, our life has become highly dependent on electronic gadgets, which primarily consists of mobile devices such as the laptop, smartphone, and other electronic gadgets. Today’s smartphone is helping us through many routine functions. Smartphone uses many operating systems such as Android, iOS, BlackBerry, Symbian, JME, and WinMobile, etc. Android OS is open source and freely available, such that the user can use the source code and can modify according to user requirements without any license and fees. The Android operating system provides many advanced services such as the Internet, MMS etc. that are user-friendly. When a user accesses the internet to download the apps on the device, it becomes vulnerable to a malware app that can infect the device; if the user could not identify that malware app due to lack of awareness. The smartphone is based on the novel technology and features (Sharma, 2016, Rastogi, 2015). This little device includes many advanced features such as GPS navigation, Wi-Fi access, and gesture motion detection etc. For the physical security, it provides the password locking system. The share of Android smartphone is increasing in the market and it has increased the security risk in parallel. Android Operating System is an open access system, so the attacker focuses on the Android operating system. The attackers target android apps by using them as a carrier of malicious code that is injected into the device when an unsuspecting user downloads and tries to install the app. The attacker has used the repackaged apps that are similar to an original app. It cannot be recognized by the user as repackaged app have the same name, same

DOI: 10.4018/IJESMA.2019040101

Copyright © 2019, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
size and same features. User downloads these apps from the android market and faces the significant challenges. Attacker develops many malware families (Faruki et al., 2015).

Modern malware families target and attack smartphone apps. When a user tries to install an application on the device, app requests user to acquire access permissions to use various services. Some permissions are by default, and some require consent from the user. If the user permits the app to access crucial resources, a hostile app can easily infect the device. The attacker can steal the confidential information present in the mobile device, change the wallpaper without user knowledge, send the SMS without user awareness and increase the user bill rates, generate a fake call and increase the call rates. Even if a device is in sleep mode, an attacker can connect to it with fake Wi-Fi access points. If there is any connection already established then the attacker can terminate it and steal user bank id, password, accounts information and user personal information (Erdogan, 2018; Arnerić, 2018; Sharma, 2018).

The smartphone is becoming increasingly ubiquitous (Xia et al., 2016). Apps are downloaded in Android devices by online marketplaces like third-party App Store or Google Play Store. The marketplaces behave as a centre of the hub where the developer publish their products. Here apps are paid or freely available. If an official market charges for their apps, then many unofficial markets provides without any charges. Nevertheless, if a user downloads the apps from any of these unofficial markets, then the risk is increased. Same issues arise in the official market when an untrusted developer distribute the malware apps (Sun et al., 2018).

According to Verizon’s 2015 data breach investigation report, about 0.03% of 10 million smartphone and mobile devices gets infected by the malware code per week. The Apps vulnerability consists of risky apps prone to man-in-middle attack or apps that store sensitive information insecurely. Currently, Android 7 Nougat is being used in the latest devices. According to Google CEO, 1.4 billion known users are using Android. A Recent version of the platform is Android Nougat 7.0 and 7.1. Today, 8 users out of 10 are using Android. The SAN report analysis reported outsourcing growth of 1.4 million in 2017. Recently android operating system is trying to provide the security against malware apps. Google Play provides the security via play store. The new age analytics aims to provide security to Android apps that are stored in the Android market (Malik & Kaushal, 2016). Here the focus is on the app relevant issues and categories of permission that are requested by the app before installation on the user system. According to the researchers, there is no android permission security in the Android application. Following are the identified research gaps:

- It requires checking the object and classes affected by various permissions described in the Androidmanifest.xml files.
- No technique, for the authentication approach to detect hazardous android app.
- Apps documentation is used, but that does not provide sufficient information.
- No appropriate technique is used in android market apps security.

Android apps can communicate with external serves by default. Unfortunately, the Android apps have been using a native library that is exploited by buffer overflow as discovered recently.

### 2. STRING MATCHING ALGORITHM

String matching algorithm is used to find the matched string or pattern. Approaches for string matching can be partitioned into two classes: first is one to one correspondence between elements of the Pattern (P) and Text (T). Another is appropriate string matching in similarity ratio between the P and T.
Design of Quality Aspects in Service Oriented Architecture through Service Level Agreements: The Streaming Case Study
Marco Massarelli, Claudia Raibulet, Daniele Cammareri and Nicolò Perino (2011).
*Engineering Reliable Service Oriented Architecture: Managing Complexity and Service Level Agreements* (pp. 1-21).
www.igi-global.com/chapter/design-quality-aspects-service-oriented/52188?camid=4v1a