Data Analysis of Android Malware

Rafael Estrada[1], Aisha Ali-Gombe[2], Golden G. Richard III[2]
[1]Department of Mathematics, New Mexico Tech
[2]Center for Computation & Technology, Louisiana State University

https://cherrysystems.com/data-recovery-services/media-types/cell-phone/android-phone/

Abstract

Smartphones are ubiquitous now more than ever. More specifically, the Android OS. With these up and coming new cellular devices capable of bringing new upgrades such as: high resolution camera, fast LTE speed data, and large memory storage, there are indeed drawbacks. Cellular devices can contain what is known as malware . This malware may damage and corrupt phone data as well as extract private information. Mobile malware is a rising field of study in computer science. Data analysis must be conducted in order to fully understand the cause and effects of such detrimental malware.

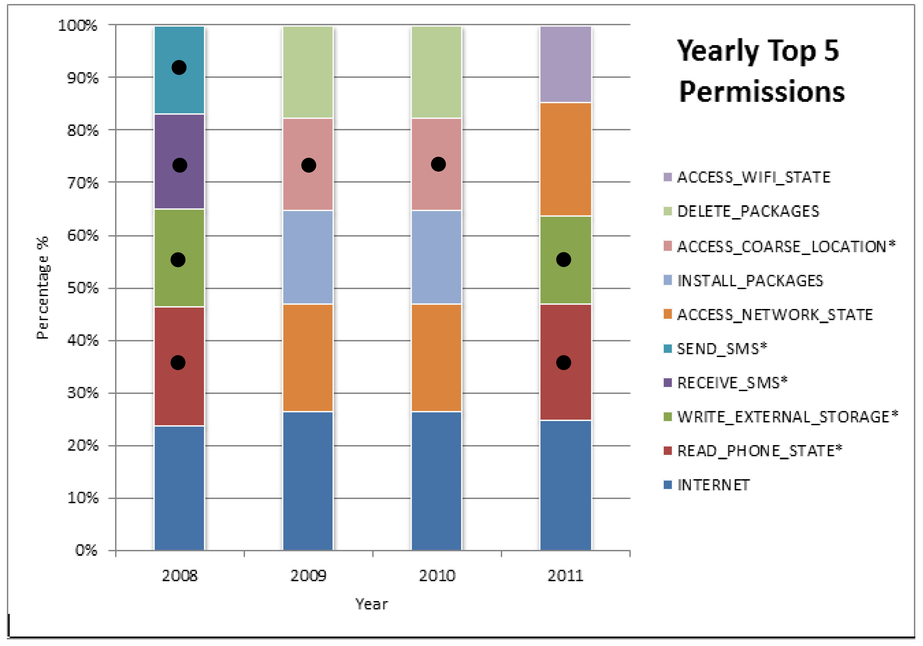
Background

Data Analysis on mobile malware is vast field of research. The research conducted for this program was to analyze folders containing numerous apk files (Android Package Kit) with possible malware samples. The end goal was to devise a scheme to display change in malware over time. The basis on examining these apk files was by the usage of known static analyzing tools. FlowDroid and Androguard were the tools used for this research; each tool was used to extract important features from the apk files.

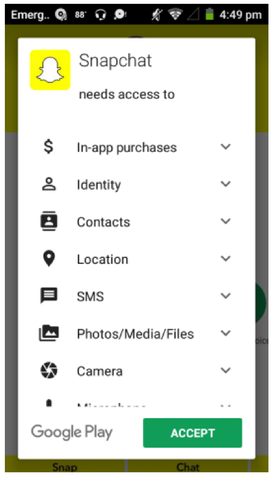
Permission Group	Permissions
android.permission-group.CALENDAR	• android.permission.READ_CALENDAR • android.permission.WRITE_CALENDAR
android.permission-group.CAMERA	• android.permission.CAMERA
android.permission-group.CONTACTS	• android.permission.READ_CONTACTS • android.permission.WRITE_CONTACTS • android.permission.GET_ACCOUNTS
android.permission-group.LOCATION	• android.permission.ACCESS_FINE_LOCATION • android.permission.ACCESS_COARSE_LOCATION
android.permission-group.MICROPHONE	• android.permission.RECORD_AUDIO
android.permission-group.PHONE	• android.permission.READ_PHONE_STATE • android.permission.CALL_PHONE • android.permission.READ_CALL_LOG • android.permission.WRITE_CALL_LOG • com.android.voicemail.permission.ADD_VOICEMAIL • android.permission.USE_SIP • android.permission.PROCESS_OUTGOING_CALLS
android.permission-group.SENSORS	• android.permission.BODY_SENSORS
android.permission-group.SMS	• android.permission.SEND_SMS • android.permission.RECEIVE_SMS • android.permission.READ_SMS • android.permission.RECEIVE_WAP_PUSH • android.permission.RECEIVE_MMS • android.permission.READ_CELL_BROADCASTS
android.permission-group.STORAGE	• android.permission.READ_EXTERNAL_STORAGE • android.permission.WRITE_EXTERNAL_STORAGE

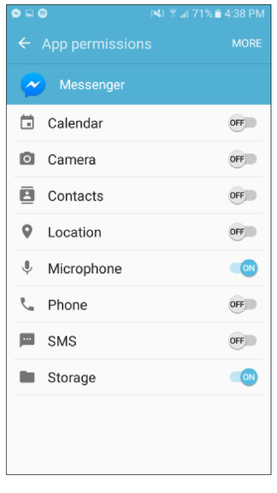
Analysis

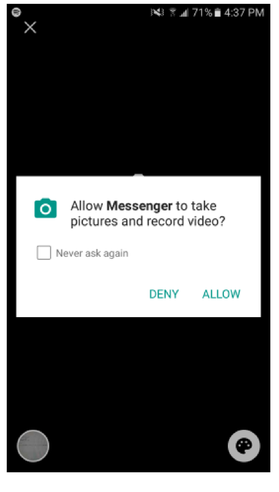
Androguard is a helpful tool in static analysis because one may mine data such as activities, **permissions**, and methods. This tool provides a strong foundation for reverse engineering, decompiling apk files, and providing a means to read Android xml files within the apk.



Of the 17,801 permissions analyzed:
6,710 – Normal Permissions (38%)
8,072 – Dangerous Permissions (45%)
3,019 – Other (17%)







Discussion

There exist copious methods and procedures on evaluating and analyzing mobile malware. One feature, permissions, is a key aspect. The permissions display what android applications are able to access. One can see the list (lower left corner) of dangerous permission groups. Whether permissions are benign or threatening, one must be aware of what application he/she is installing since ambiguity exists as to what the application will undertake.

References

Arzt, Steven (N/d) soot-infoflow. Retrieved June 18, 2017 from https://github.com/secure-software-engineering/soot-infoflow

Nuuneoi, (2015, August 26) Everything every Android Developer must know about new Android's Runtime Permission [Web log post]. Retrieved July 15, 2017 from https://inthecheesefactory.com/blog/things-you-need-to-know-about-android-m-permission-developer-edition/en

N/a, (N/d) Secure Software Engineering. Retrieved July 20, 2017 from https://blogs.uni-paderborn.de/sse/tools/flowdroid/

N/a (Open Source) androguard. Retrieved June 26, 2017 from https://github.com/androguard/androguard

Acknowledgements

This material is based upon work supported by the National Science Foundation under award OCI-1560410 with additional
support from the Center for Computation & Technology at Louisiana State University

LSU Center for Computation & Technology
Interdisciplinary | Innovative | Inventive

NSF

NEW MEXICO TECH
SCIENCE • ENGINEERING • RESEARCH UNIVERSITY