DATA ANALYSIS OF ANDROID MALWARE

https://www.cnet.com/android-update/

Rafael Estrada
Department of Mathematics
New Mexico Tech

Mentor: Dr. Golden G. Richard III
Postdoctoral Researcher: Aisha Ali-Gombe

July 26th 2017
CCT REU 2017

ANDROID MALWARE

- What is it?
  - “Malicious software”, that attacks cellular devices, more specifically the Android OS.
- What can this mobile malware do?
  - Capable of sending SMS/MMS messages, memory deletion (SD card), contacts possession, and privacy leakage.
- Infection mechanism?
  - Malware in Play store.
  - Repackaged apps in alternate app market.

METHODS

- Static Analysis
  - Aims to find weaknesses in code that will cause problems
  - Runs before actual code execution (debugging)
  - Displays where code may have errors/flaws (unused variables, dead code, infinite loops)
- Tools
  - FlowDroid & Androguard
    - Examine apk files (Android Package Kit).

ANDROGUARD

- Mines data such as activities, **permissions**, and methods.
- Powerful tool for:
  - Reverse engineering
  - Decompiling apk files
  - Reading Android xml files within the apk

http://blog.k3170makan.com/2014/11/automated-dex-decompilation-using.html

PERMISSIONS

- Listed in the Manifest file
  - Benign or dangerous
- Android 6.0 (API level 23 and on)
  - User grants permissions at runtime
    - Increased user control (i.e. permission removal)
- Android 5.1 (API level 22 and before)
  - User grants permission at install time

EXAMPLES

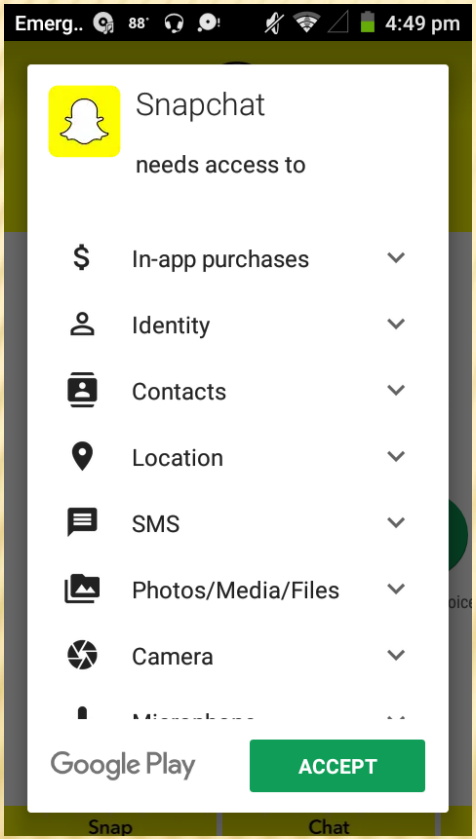


Figure 1: Android 5.1 Permission at install time

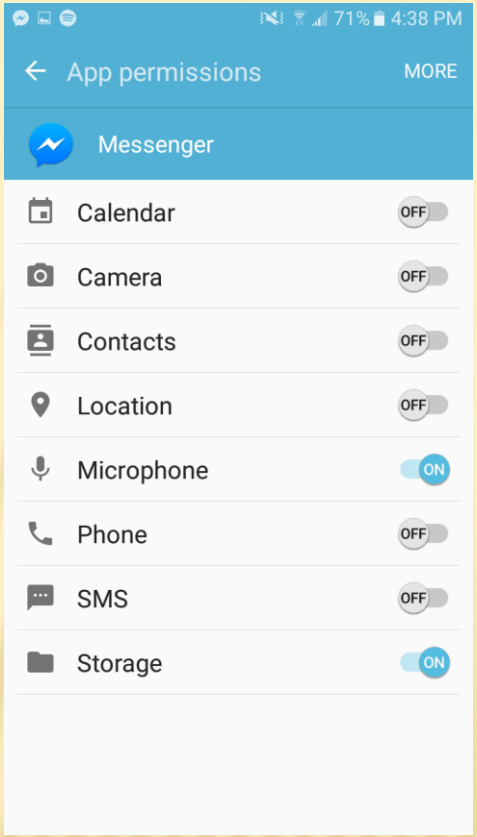


Figure 2: Android 6.0.1 Settings Screen

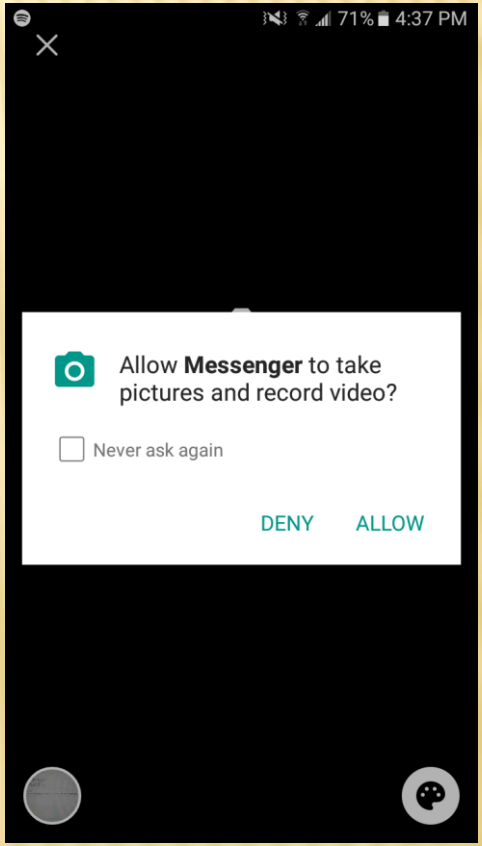


Figure 3: Android 6.0.1 App asking for permission

ANDROGUARD (CONTINUED)

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

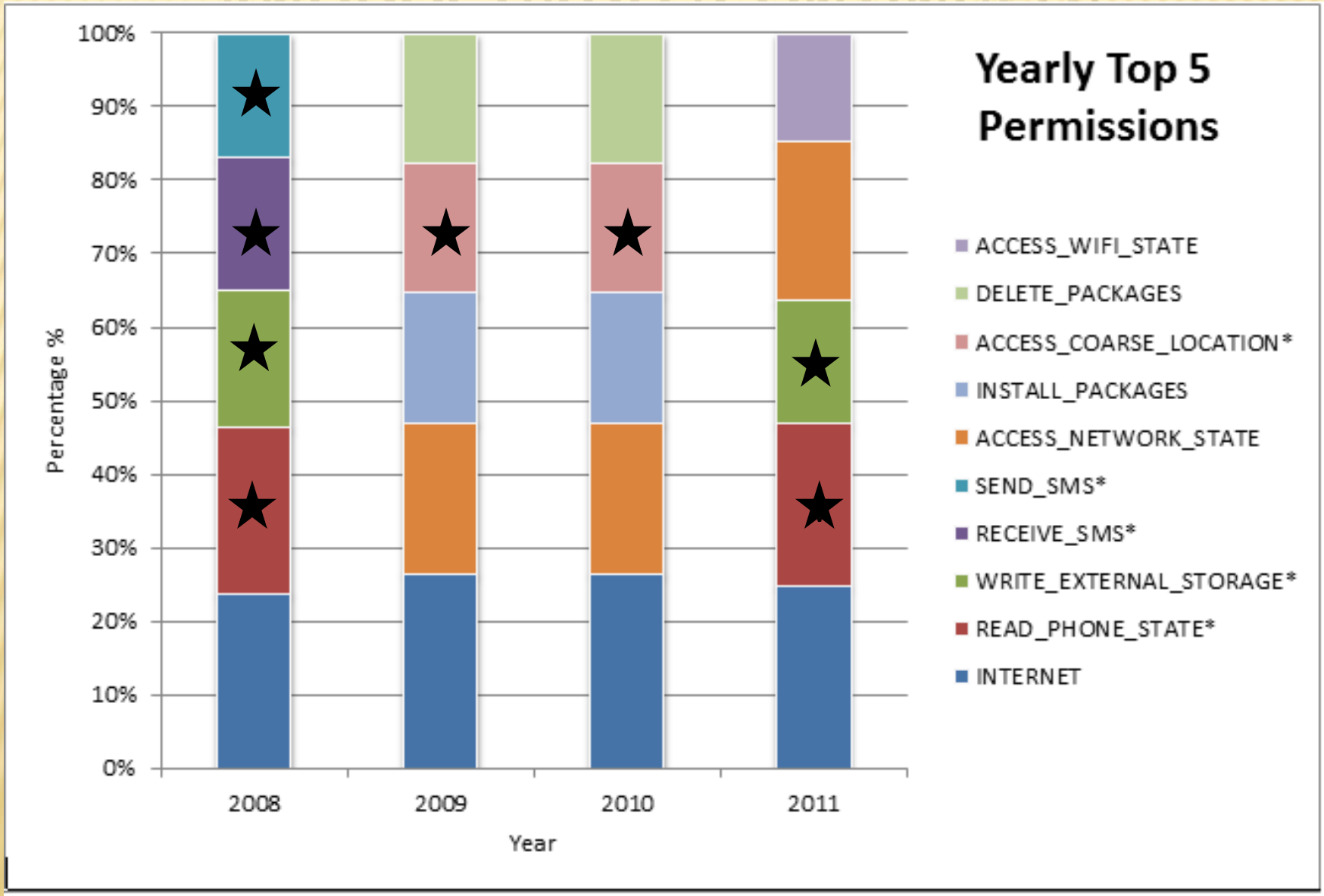
- Normal Permissions are automatically granted
- Dangerous Permissions need user approval

Dangerous Permissions

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

https://inthecheesefactory.com/uploads/source/blog/mpermission/permgroup.png

ANDROGUARD (CONTINUED)



OVERALL

- Permissions display what Android applications are able to access
  - Benign or threatening?
  - Ambiguity exists as to what the application will undertake
- Other features for other tools
  - Sinks & Sources
  - Methods
  - Data Flow Analysis

QUESTIONS?