Student Works

10-28-2019

Automated Dynamic Detection of Self-Hiding Behavior in Android Apps

Luke Baird
Embry-Riddle Aeronautical University, bairdl1@my.erau.edu

Seth Rodgers
University of Texas at Arlington, seth.rodgers@mavs.uta.edu

Scholarly Commons Citation

Baird, L., & Rodgers, S. (2019). Automated Dynamic Detection of Self-Hiding Behavior in Android Apps. , (). Retrieved from https://commons.erau.edu/student-works/150

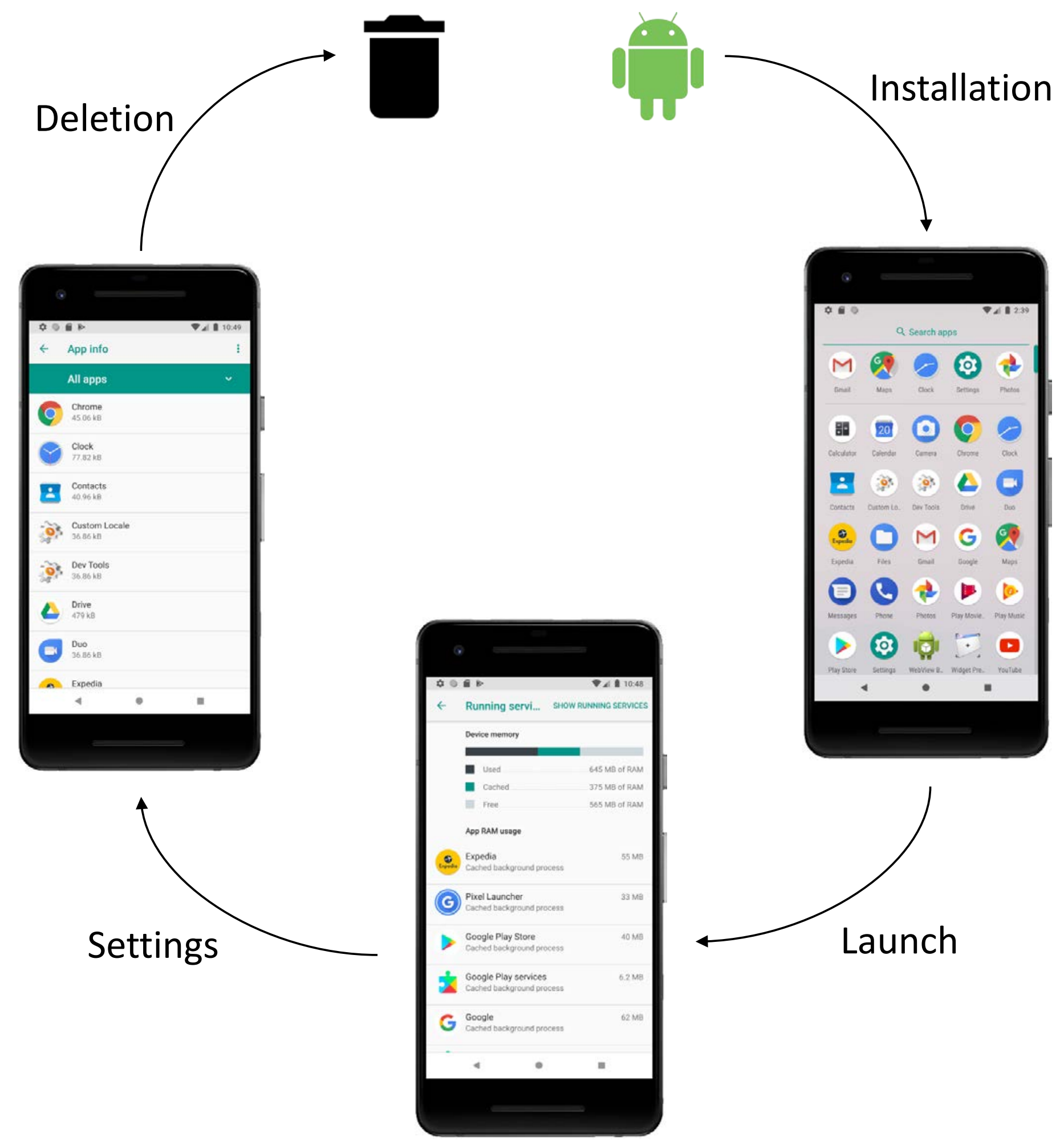
NETCPS REU
October 28, 2019

Automated Dynamic Detection of Self-Hiding Behavior in Android Apps

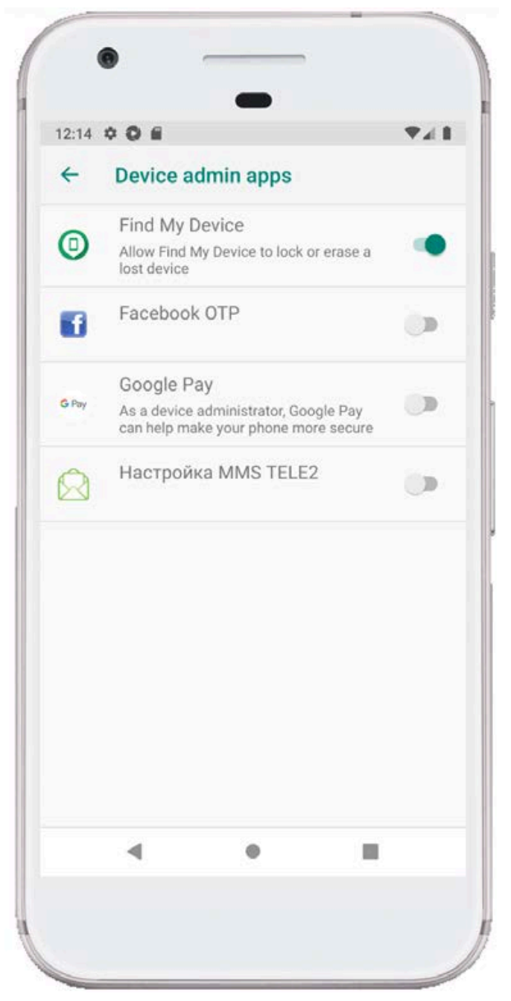
Luke Baird | Seth Rodgers | Faculty Mentor: Dr. Zhiyong Shan

Android App Lifecycle

- Covers an app's existence existence on an Android phone from its installation to its deletion
- An Android app should appear in three places on a device:
  - Home app list
  - Running app list
  - Installed app list
- An app that is hiding from any of these lists exhibits a self-hiding behavior that adversely affects a normal user experience with the app
- Research developed three dynamic analysis tools to detect self-hiding behavior in each of these lists.

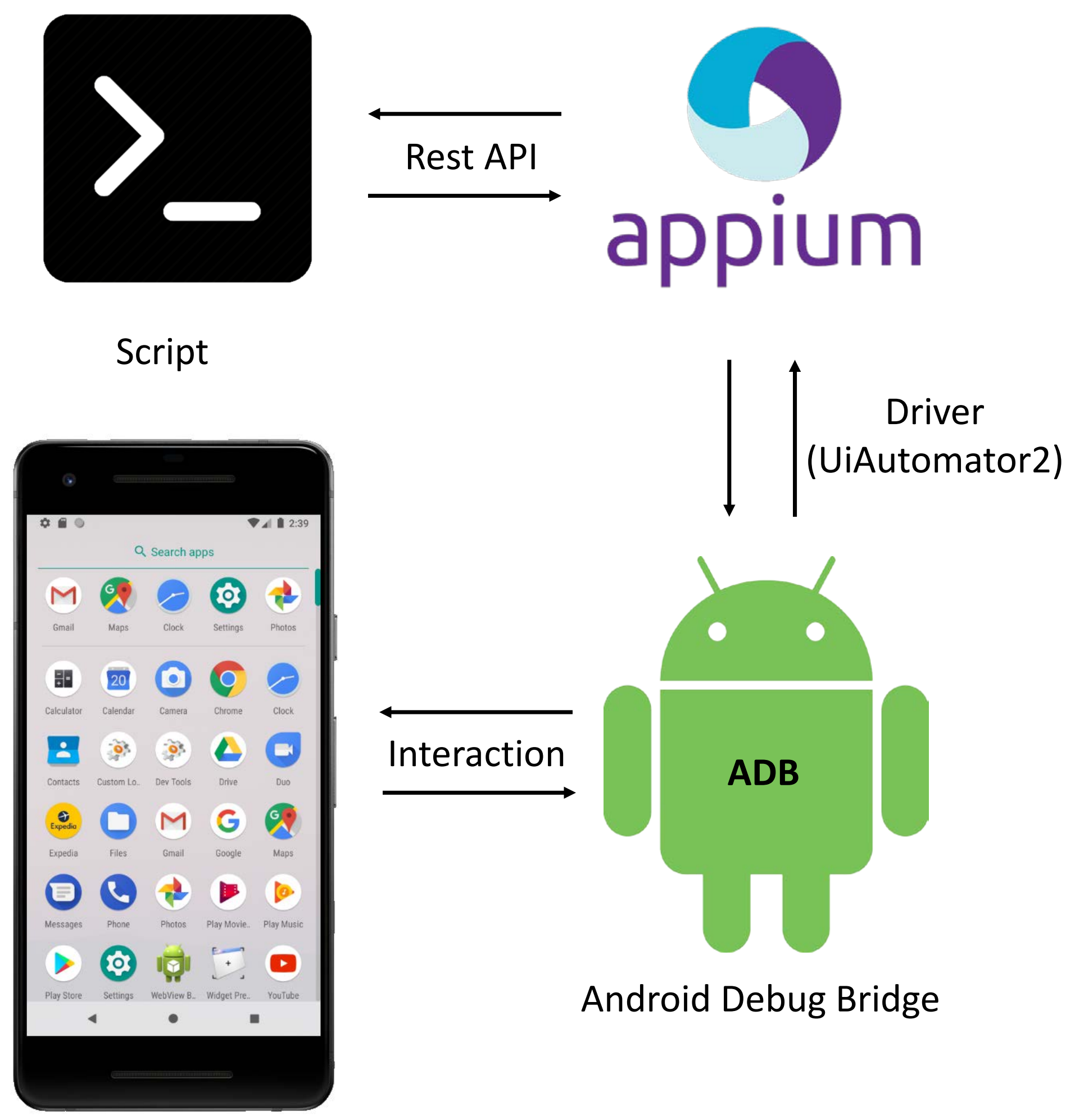


Device Admin Apps



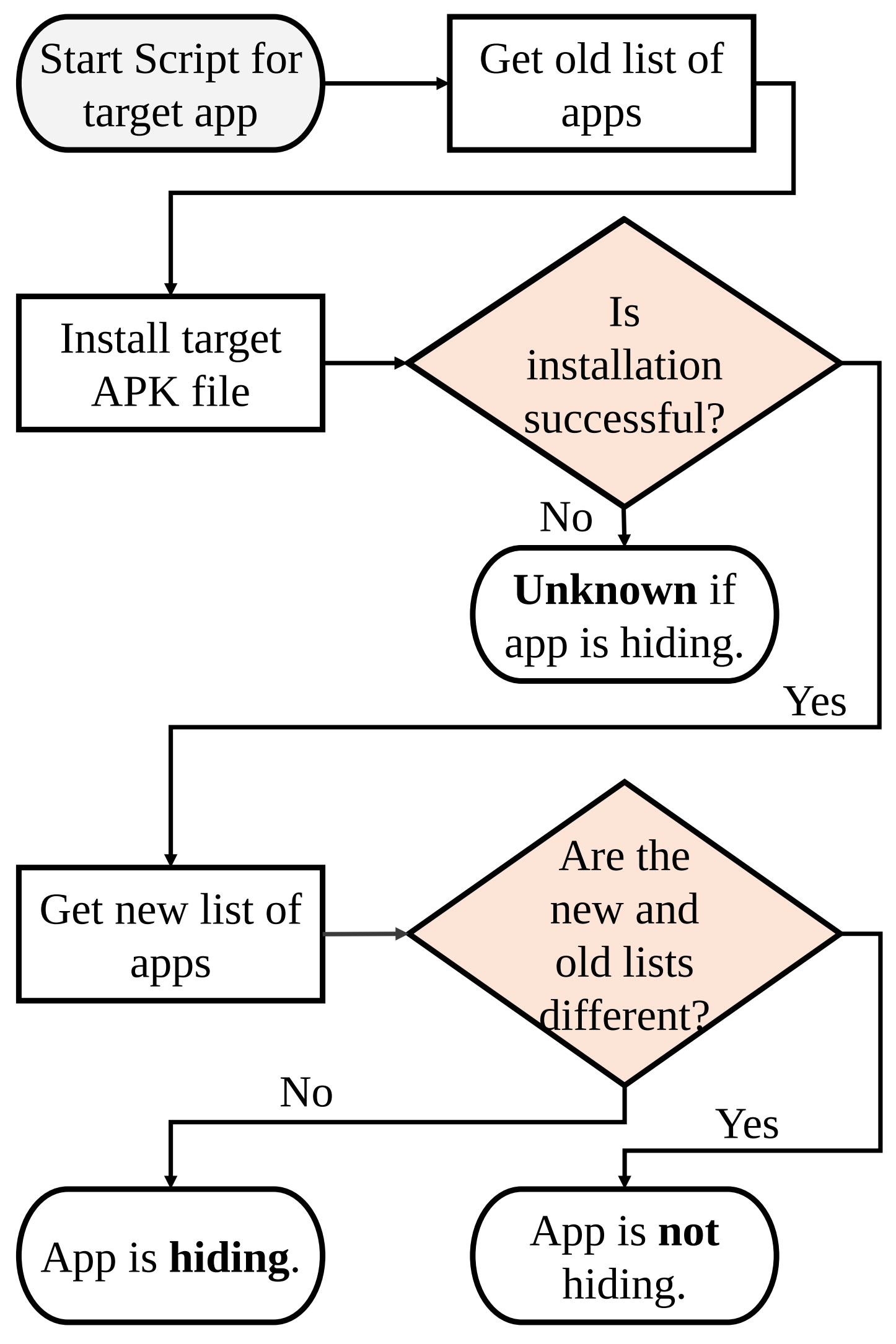
- Android devices use a permission-based system to determine which apps have the ability to execute different tasks and access certain information
- Device Admin permission allows apps to run tasks such as factory resetting a device

Appium Architecture



- The Appium framework is an automated testing bench for apps.
- Appium is a REST API server that connects a script to a driver.
- The driver connects Appium to the Android Debug Bridge (ADB) for Android devices.
- Interactions with a device are simulated and received through ADB, returning via Appium to the script.

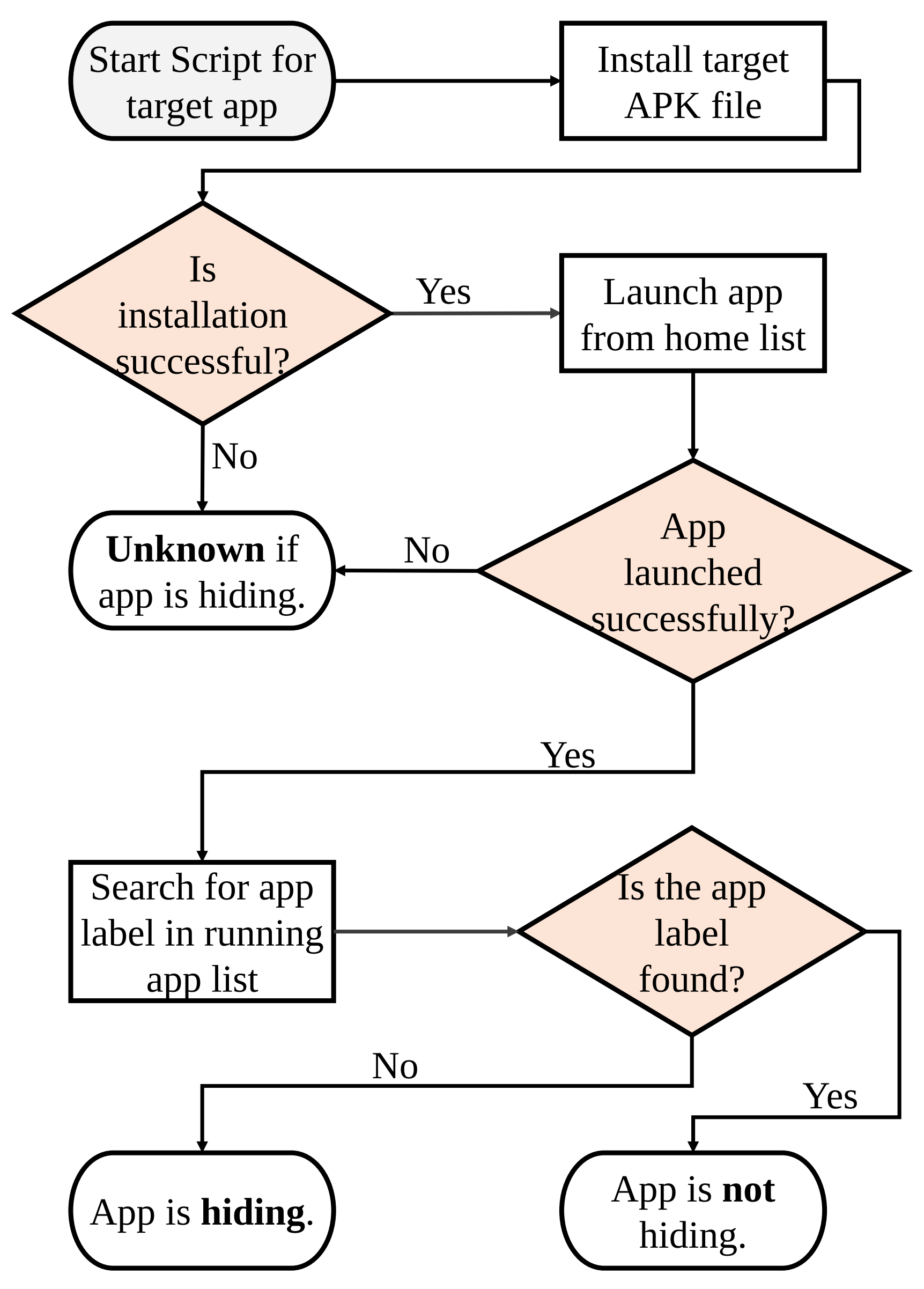
Home / Installed Application Lists


Start Script for target app
Get old list of apps
Install target APK file
Is installation successful?
No
Unknown if app is hiding.
Yes
Get new list of apps
Are the new and old lists different?
No
Yes
App is hiding.
App is not hiding.

- Home and Installed self-hiding behavior detection tool algorithm flowchart
- Old and new lists are pulled with Appium
- Compares lists before and after an app is installed

Running Application List

- Launches an app from the home app list using Appium
- Searches for an app in the running app list
- If an app is hiding in the home app list, the test fails
- Does not compare old and new lists
- Is more error-prone than home and installed list tests as it is reliant on the ability to parse a meaningful label from an app.
- Malware can dump its payload when it is loaded. Because this tool runs its test app, this can cause an emulator's performance to suffer


Start Script for target app
Install target APK file
Is installation successful?
Yes
Launch app from home list
No
Unknown if app is hiding.
No
App launched successfully?
Yes
Search for app label in running app list
Is the app label found?
No
Yes
App is hiding.
App is not hiding.

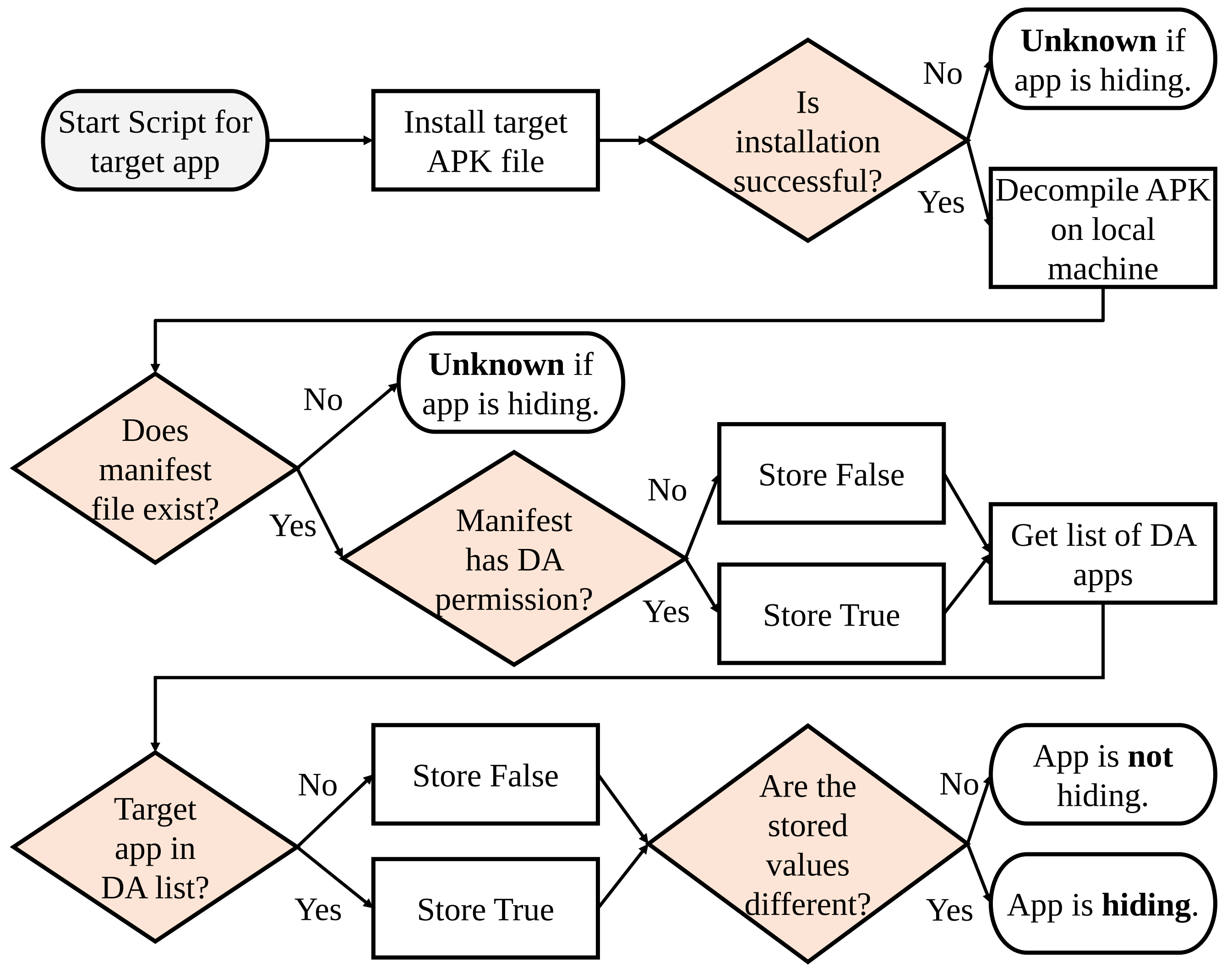
System Environment

- The home, installed, and running application list tools were tested on Windows 10.0.18362.239. The target emulator was a Pixel 2 AVD running Android Oreo 8.1.
- The device admin list tool was tested on MacOS 10.14.3. The target emulator was a Nexus 6P AVD running Android Pie 9.0.

References

1. Z. Shan, I. Neamtiu, and R. Samuel, "Self-hiding behavior in android apps: detection and characterization," in 2018 IEEE/ACM 40th International Conference on Software Engineering (ICSE). IEEE, 2018, pp. 728–739.

Device Admin List


Start Script for target app
Install target APK file
Is installation successful?
No
Unknown if app is hiding.
Yes
Decompile APK on local machine
Does manifest file exist?
No
Unknown if app is hiding.
Yes
Manifest has DA permission?
No
Store False
Yes
Store True
Get list of DA apps
Target app in DA list?
No
Store False
Yes
Store True
Are the stored values different?
No
App is not hiding.
Yes
App is hiding.

- Device Admin self-hiding behavior detection tool algorithm flowchart
- Static analysis is used with the tool apktool to decompile the APKs.
- Dynamic analysis is completed with Appium to inspect the Device Admin list

Results

Test	# analyzed	# hiding	# not hiding	False Positives	False Negatives	Precision	Recall	F-Measure	Errors
Home	77	12	62	2	0	97.47%	100%	98.72%	3
Installed	77	0	76	0	0	100%	N/A	100%	1
Running	63	3	40	0	0	100%	100%	100%	20
Device Admin	72	6	64	N/A	N/A	N/A	N/A	N/A	2

- Results show the number of self-hiding behaviors detected by our tools
- The home, installed, and running application list tools have low false positive and false negative rates
- With an average time of less than 3 minutes per app on all three tools with proper time analysis, we conclude that these tools are efficient.

Efficiency

App	Total Time (all units in seconds)	Average time per app	Median time per App	Maximum time per App	Minimum time per app
Home	8569	85.9	84	139	30
Installed	14712	149.3	156	188	76
Running	10982	111	96	1373	5

Acknowledgements

- Thank you to Embry-Riddle Aeronautical University Undergraduate Research Institute for providing travel funding.
- Thank you to Dr. Vinod Namboodiri, NETCPS REU Coordinator at Wichita State University this summer 2019 for his guidance and support.