First Assignment

Omer Michael

Dor Baram

Name of the paper: "When the Guard failed the Droid: A case study of Android malware" link: https://arxiv.org/abs/2003.14123

The feature set that the paper(code) uses:

In the code:

1. perm: SET_DEBUG_APP
2. READ_PHONE_STATE
3. RECORD_AUDIO
4. INTERNET
5. PROCESS_OUTGOING_CALLS
6. ACCESS_FINE_LOCATION
7. RECEIVE_BOOT_COMPLETED
8. ACCESS_COARSE_LOCATION
9. RECEIVE_SMS
10. WRITE_SMS
11. SEND_SMS
12. UNINSTALL_SHORTCUT
13. INSTALL_SHORTCUT
14. SET_PREFERRED_APPLICATIONS

The feature set that the paper uses:

1. An application must not have the SET_DEBUG_APP permission label.
2. An application must not have PHONE_STATE, RECORD_AUDIO, and INTERNET permission labels.
3. An application must not have PROCESS_OUTGOING_CALL, RECORD _AUDIO, and INTERNET permission labels.
4. An application must not have ACCESS_FINE_LOCATION, INTERNET, and RECEIVE_BOOT_COMPLETE permission labels.
5. An application must not have ACCESS_COARSE_LOCATION, INTERNET, and RECEIVE_BOOT_COMPLETE permission labels.
6. An application must not have RECEIVE_SMS and WRITE_SMS permission labels.
7. An application must not have SEND_SMS and WRITE_SMS permission labels.
8. An application must not have INSTALL_SHORTCUT and UNINSTALL_ SHORTCUT permission labels.
9. An application must not have the SET_PREFERRED_APPLICATION permission label and receive Intents for the CALL action string

The type of classifier that you analyze (static/dynamic/behavioral). **static**.

GitHub Link(Fork): https://github.com/DorBaram/When-the-guard-failed-the-droid