Listing of Threat Agents - By Category

Human Interaction

- **Stolen Device User:** A user who obtained unauthorized access to the device aiming to get the memory-related sensitive information belonging to the owner of the device.
- **Owner of the Device:** A user who unwillingly has installed a malicious phone application that gains access to the device application memory.
- **Common Wi-Fi Network User:** This agent is aimed at any adversary intentionally or unintentionally sniffing the Wi-Fi network used by a victim. This agent stumbles upon all the data transmitted by the victim device and may reuse it to launch further attacks.
- **Malicious Developer:** A human user who has the intent of writing an application that not only provides a commonly known function like gaming/calculator/utility in the foreground but steals as much information from your device as possible in real time and transmits it to the malicious user. This agent can also be looked at an angle from which he or she codes an app to perform DOS by using up all the device resources.
- **Organization Internal Employees:** Any user who is part of the organization (may be a programmer/admin/ user/ etc.). Anyone who has privileges to perform an action on the application.
- **App Store Approvers/Reviewers:** Any app store which fails to review potentially dangerous code or malicious application that executes on a user's device and performs suspicious/malicious activities

Automated Programs

- **Malware on the device**: Any program/mobile application that performs suspicious activity. It can be an application that is copying real-time data from the user's device and transmitting it to any server. This type of program executes parallel to all the processes running in the background and stays alive, performing malicious activity all the time, e.g. Olympics App, which stole text messages and browsing history:[2]http://venturebeat.com/2012/08/06/olympics-android-app/

- **Scripts executing at the browser with HTML5**: Any script code written in a language similar to JavaScript having capability of accessing the device-level content falls under this type of agent section. A script executing at the browser reading and transmitting browser memory data/complete device level data.
- **Malicious SMS**: An incoming SMS redirected to trigger any kind of suspicious activity on the mobile device. There are multiple services that keep running in the background. Each of these services has listeners which might be active to listen for the content of an incoming SMS. An SMS message may be a sort of trigger for the service to perform some suspicious activity.
- **Malicious App:** Failure to detect malicious or vulnerable code and the likelihood of a compromise or attack against the app store itself, potentially turning legitimate code into hostile things including updates and new downloaded apps.