Abstract

Smart phones form essential part of our daily lives and remain almost always with us or in our close vicinity. They act as an interface for very crucial and personal information like images, videos, voice calls, video calls, downloaded media, text messages, call logs, banking transaction details, passwords etc., thus housing very large amount of private information which can provide deep insight into the personality of the concerned person and thus can be of pivotal importance for Secret service and law enforcement agencies. We have proposed a new Surveillance scheme utilizing the existing Cellular Infrastructure to monitor and extract the information from the blacklisted smart phone devices i.e. devices of terrorists, corrupt politicians, hard core Criminals, drug dealers etc. We will review several attacks over the Smart phones via Communication channels in order to provide the insight for using the Cellular Infrastructure for the purpose of Surveillance and extraction of information from the Blacklisted Smart phone devices and for conducting those very attacks. Surveillance and extraction of information via Cellular infrastructure would be capable of providing both live feedbacks (like ongoing conference(in the vicinity of Smart phone device), ongoing voice/video call, present...
location etc.) as well as the information contained in the Smart Phone device’s memory (including Downloaded media, Images, video Call logs, e-mails, passwords, credit card numbers etc.).

References


www.spiegel.de/international/world/how-the-nsa-spies-on-smartphones-including-the-blackberry-a-921161.html


**Index Terms**

Computer Science  Information Sciences

**Keywords**

Blacklisted smart phones, Spying of smart phones, Attacks over Communication Channels, Surveillance.