User Privacy Threats through the analysis of Mobile Device's Side-Channels

When

Monday 09 May 2016

Time

From 5:30 PM

Location

Aula Alfa - Department of Informatics, Sapienza University
Nowadays, users handle with their mobile devices a huge amount of sensitive information. People continuously carry these devices with them and use them for daily communication activities and social network interactions. Unfortunately, mobile devices can be maliciously exploited to violate the privacy of people. A possible way to infer private insights about users of mobile devices is to exploit leaked information that such devices through side-channels, such as electric energy traces and network traffic. On one hand, the information that could be inferred from a side-channels are often not in clear (e.g., the payload of a message) and as accurate as the ones obtained by a malware.

On the other hand, the existence of side-channels is due to the way in which the operative system normally works and the user interact with the device. In addition to that side-channels have a desirable strength for an attacker who want to remain undetected: side-channel attacks are passive, thus they are hard (if not impossible) to be detected. In this research project, we focus on extract user private information from side-channels produced by mobile devices. In order to gain such knowledge we use pattern recognition and machine learning techniques. Currently, the side-channels we are taking into account are two: network traffic and electric energy traces.

In network traffic analysis of mobile devices, we consider an adversary, who does not interact actively with the mobile device, but he is able to eavesdrop the network traffic of the device from the network side (e.g., controlling a Wi-Fi access point). The fact that the network traffic is often encrypted makes the attack even more challenging. Our work prove that it is possible to leverage traffic analysis in order to identify user activity and apps installed on mobile devices.
Such insights are becoming a very attractive data gathering technique for adversaries, network administrators, investigators and marketing agencies.

In electric energy consumption analysis, we consider an adversary that is able to measure with a power monitor the amount of energy supplied to a mobile device. In fact, we observed that the usage of mobile device resources (e.g., CPU, network capabilities) directly impact on the amount of energy retrieved from the supplier, i.e., usb port for smartphones, wall-socket for laptops. Leveraging energy traces, we aim to extract the same insights as for network traffic analysis on smartphones. In addition to that, we aim to recognize a specific laptop user among a group and detect intruders (i.e., user not belonging to the group).

Relatore: Dr. Riccardo Spolaor

He earned Master’s degree in Computer Science in 2014, at University of Padua, Italy, with thesis about smartphone privacy attack inferring user actions via traffic analysis. In November 2014, He started Ph.D. in Brain, Mind and Computer Science at the same university under the supervision of Prof. Mauro Conti.

His main research interests are Privacy and Security issues on smartphones. In particular, He applies Machine Learning techniques to infer user information and build countermeasures. Most of the research that He carried out up to now is about the application of Machine Learning classifier on Android network traffic.