Malware Analysis on Mobile Devices

Fachgebiet: Informatik
Betreuer: Dr. Ulrich Fiedler
Experte: Dr. Torsten Braun

Malware is reported to increasingly spread on smartphones and may thus spy on the user's location, compromise personal information, such as contact lists or passwords, and more. On WiFi, malicious activities can be monitored rather easily. As a consequence, malware may switch to using cellular networks. In this thesis project, we have set up and configured a GSM/GPRS base station and conducted a sample malware analysis with two apps.

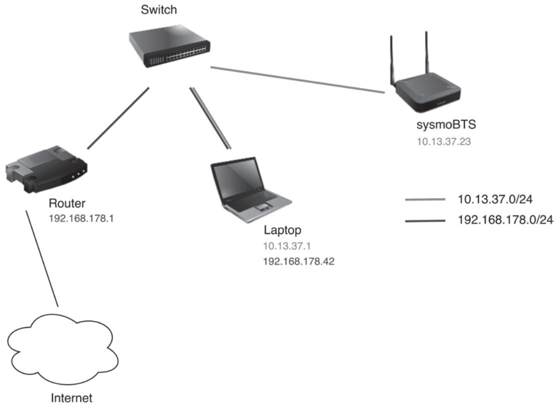
During the last years, several observers reported an exponentially increasing spread of malware on mobile devices. In their third annual mobile threats report, the company Juniper Networks found that nearly one fifth of the malware detected was spyware – the kind of malware, which secretly captures and transfers user data to attackers.

The impact is significant. Smartphones have become daily companions to many of us and they are aware of our position, contacts, messages and even more private information. Given the fact that they are permanently connected to the Internet, attackers can spy for personal information of the phone holder or undertake industrial espionage.

My set-up to monitor GPRS IP traffic on a sysmoBTS with Wireshark.

One approach to detect malicious activities is the analysis of Internet traffic from the phone under examination. This kind of analysis over WiFi networks is simple; mainly because WiFi operates on a free frequency band and thus is available to anyone. Even though cellular networks are as wide spread as WiFi networks, the situation is totally different for GSM (2G), UMTS (3G) and LTE (4G). The main difference is, that the cellular network technologies work on a licensed radio spectrum. Accordingly, running such networks is more difficult and often too expensive for non-operators.

Since a few years, there are open source projects which facilitate research with GSM. In this thesis project, we have set up and configured a low–cost sysmoBTS GSM/GPRS base station with free software and conducted a sample malware analysis with two apps. We have found (i) that a popular free game from Google Play Store transmits unencrypted information on location to at least five ad providers and (ii) that a commercial spy service not only collects information on a dedicated server but also transmits it in plain text.



Schematic view on the set-up.

Denis Simonet
+41 76 509 84 82
denis.simonet@bluewin.ch