P0 – B216

Topic: IMEI

There are over 5 billion mobile phones worldwide[1]. To identify every individual phone on the network, the phones have a unique number – an IMEI or International Mobile Equipment Identity. The IMEI number stays with the phone, even if you insert another SIM-card into it. This is very beneficial in the fight against phone theft. If a phone is stolen, the owner can report the phone stolen through its IMEI. If the thief tries to use the phone on a network anywhere in the world, the phone will be denied access, and it is useless as a phone.[2]

The phones IMEI are normally hidden for others the operators of the GSM module. If someone can get your IMEI, they can make a phone with the same IMEI number, and imitate you. They can also track your position, by your cell mast.

Stolen IMEI's is normally used in terrorism and organized crime. They can steal your identity, and if the police try to find you by your IMEI, they will find the owner of the stolen IMEI.

Apps on android phones can read the phone's IMEI number[3]. With the IMEI number in wrong hands, they can abuse it, and it can have huge consequences for the owner.

Our state of problem is therefore:

"Why can apps on Android-phones get the IMEI, and what consequences can it have?"

---

[1] http://www.bbc.co.uk/news/10569081
[2] http://borger.itst.dk/lov-og-ret/adgang-til-internet-og-telefonlinjer/mobiltelefonen-er-stjalet-hvad-gor-du/din-mobiltelefon-eller-sim-kort-er-stjalet-hvad-gor-du
[3] http://developer.android.com/reference/android/telephony/TelephonyManager.html#getDeviceId%28%29