### Copy of identity (Rasmus)

On the GSM network, an identity is based on two numbers: The IMEI number, which is bound a specific phone. This number can usually be found by pressing “\*#06” on the phone – but it is also located under the battery, and it also appears on the bill when purchasing the phone. In case a cellphone is stolen, you can contact your network provider, and have that exact phone blocked on all networks.

The other number is the IMSI number – this number is tied to the SIM-card, which again is tied to the individual user of that SIM-card. Both the IMEI and the IMEI number are used to identify the phone, when it connects to a signal transmitter. In Android it is very easy for an app to get both the IMEI and IMSI number. The app simply has to call the TelephonyManager[[1]](#footnote-1) library, and then use the getDeviceId()[[2]](#footnote-2) function to get the IMEI number, and the getSubscriberId()[[3]](#footnote-3) function to get the IMSI number. In theory the app could then silently transmit these numbers to a remote server, and a criminal would be able to alter these on to another phone.

It is in fact illegal to alter the IMEI number – this is because the only apparent reason to alter the IMEI number is if the phone was stolen and blacklisted. But organized criminals like terrorist may be interested in obtaining IMEI- and corresponding IMSI numbers to hide their identity and to make it harder for the authorities to trace them.

There have already been a number of reported Trojan horses on the Android platform, which obtained the IMEI and IMSI numbers and established encrypted data connections to remote servers and transmitted the infected phones IMEI and IMSI numbers. At least three of the known Trojans for Android were spread using fake Chinese clones of the Android Market. In these markets popular apps where repackaged in order to contain the Trojan. This is may be the easiest method to obtain IMEI and IMSI numbers. Another, more sophisticated method to obtain this sensitive data is to build a GSM transmitter – this can be built with regular electronic equipment, which can be found in most electronic stores[[4]](#footnote-4). A cellphone will in theory connect to the signal transmitter with best connectivity, thus getting the best signal. A custom built transmitter will then be able to decode the encrypted phone signal, and extract the IMEI and IMSI numbers.

To prevent these attacks, one would simply disallow roaming, thus unabeling the phone to connect to other service providers, and unknown network transmitters. One would also have to have an updated anti-virus application to prevent infections on the phone.

1. http://developer.android.com/reference/android/telephony/TelephonyManager.html [↑](#footnote-ref-1)
2. http://developer.android.com/reference/android/telephony/TelephonyManager.html#getDeviceId() [↑](#footnote-ref-2)
3. http://developer.android.com/reference/android/telephony/TelephonyManager.html#getSubscriberId() [↑](#footnote-ref-3)
4. Do You Trust Your Phone - Aniello Castiglione, Roberto De Prisco, and Alfredo De Santis, Dipartimento di Informatica ed Applicazioni “R. M. Capocelli”, Universit`a di Salerno, Via Ponte don Melillo, I-84084 Fisciano (SA), Italy [↑](#footnote-ref-4)