Secret Back Doors in Android

By *Roy Schestowitz*
Created *08/05/2014 - 2:37pm*
Submitted by Roy Schestowitz on Thursday 8th of May 2014 02:37:54 PM Filed under Just talk [1]

I am everything but a Google basher and I spent a lot of my life descending deep into research of Google foes, Google smear campaigns, lawsuits by proxy, and antitrust actions by proxy. I also advocate Android, but in recent years I have been increasingly concerned about the direction it is taking. I wish to share my latest concern. It relates to what the media characterises as "anti-theft" but is actually a facility to kill phones in a protest or convert them into hostile listening devices. Technology impacts human rights and those who control technology can be tempted to control humans.

Google habitually updates my tablet. It is a Nexus 7 tablet which Google invites itself to update remotely (shame on me for not installing Replicant, but this device does not support it yet). It is not a 3G tablet and it does not have two operation systems (unlike mobile phones) or even a carrier tracking its location all the time. It's a purely Android device with no network tying. It is network-agnostic. I only bought it because in order to replace my PDA (for over a decade) I wanted a device that is not a tracking device. Phones were out of the question.

Networks don't track the tablet. Google, however, is always out there, fully able to identify the connected user (latched onto a Gmail address because of Play), modifying the software without even the user's consent (the user is sometimes prompted to boot, without being able to opt out of the core update itself).

The update in itself is not a problem. What's problematic is its effect.

Following the latest Google update (which I was given no option to reject) I noticed that Google had added a remote kill switch as an opition. It was enabed by default. "Allow remote lock and erase" is what Google calls it and it is essentially working like a back door. Google and its partners in government are gaining a lot of power not over a smartphone but over a tablet.

The significance of this is that not only phones should be assumed to be remotely accessible for modification, including for example additional back doors. What's more, some devices that were sold without this functionality silently have it added. According to the corporate press, the FBI remotely turns Android devices into listening devices and it is getting simpler to see how.

NSA and PRISM destroy our computing. We definitely need to demand Free software, but we should go further by asking for audits, rejecting user-hostile 'features' like DRM, 'secure' boot, and kill switches. I gradually lose any remaining trust that I had in Google and even Free software such as Android.

Just talk