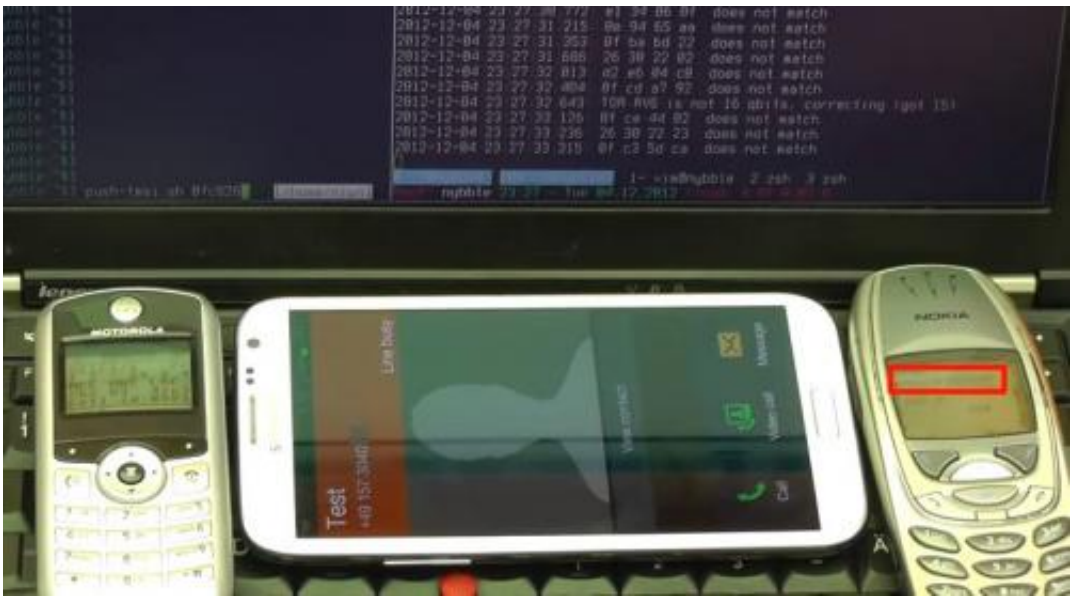
Firmware tweak can block subscriber calls, says Berlin group

August 28 2013, by Nancy Owano



A telecommunications security research group at the Technical University of Berlin earlier this month told an audience at the 22nd USENIX Security Symposium that they were able to hack phones by modifying embedded software. They could block calls and texts intended for nearby people connected to the same cellular network. They pulled this off by modifying embedded software on the mobile phone's baseband processor, controlling communications with a network's transmission towers. Just one phone could have the impact of blocking

service to people served by base stations within a certain coverage area. The hack involves modifying the baseband processor on some phones and tricking older 2G GSM networks into not delivering calls and messages intended for subscribers nearby.

The hacked firmware – OsmocomBB – can block calls and messages because it can quickly respond to them before the phones that are intended to get the communications can do so.

But wait, did they say GSM (Global System for Mobile communications)? Isn't that the older type of network, so who cares? The fact that the group's method worked on the second-generation (2G) GSM networks is important. These are the most common type of cell networks worldwide; about 4 billion people use GSM networks for calls even though carriers promote 3G and 4G. The group's work with 2G was explained further at USENIX by Kévin Redon, a Berlin-based researcher. Radon said that GSM is still relevant, can be found everywhere; in fact, in some countries there is only GSM, he stated.

Redon and researchers Nico Golde and Jean-Pierre Siefert provided the presentation, "Let Me Answer That For You: Exploiting Broadcast Information in Cellular Networks."

They implemented their approach and they tested it out to find that they were able to carry out their attacks on a number of German cell phone operators, vulnerable to the trio's attack.

According to their work, "We demonstrate that for at least GSM, it is feasible to hijack the transmission of mobile terminated services such as calls, perform targeted denial of service attacks against single subscribers and as well against large geographical regions within a metropolitan area."

They also noted that the attack can be accomplished just by using inexpensive consumer devices that are available on the market. According to *MIT Technology Review*, the group used open-source baseband code to write replacements.

More information: www.usenix.org/conference/usen … on-cellular-networks
www.technologyreview.com/news/ … other-peoples-calls/
threatpost.com/phone-hack-coul … some-mobile-networks