Danger on ice: Android info thaws in cold boot attack

18 February 2013, by Nancy Owano

(Phys.org)—Can low temperatures yield access to information in the phone's memory? Researchers found that a "FROST" attack can unlock an Android's phone data. Their research findings discuss how hackers can freeze their way into a phone's sensitive data. Researchers at Erlangen University in Germany showed how their cold boot attack method was able to read information from a Samsung Galaxy Nexus running the latest version of Android.

They said the hack can be achieved even if the phone is protected by a PIN and with its storage disk encrypted. They said they chose the Galaxy Nexus from Samsung because it was the first device with Android 4.0 and consequently it was the first Android-based smartphone with encryption support. Also, since it is an "official" Google phone, they added, it carries an official Android version from Google unmodified by the phone manufacturer. They said that Google releases are most amenable for in-depth security analysis.

In their paper, they wrote, "We present FROST, a tool set that supports the forensic recovery of scrambled telephones. To this end we perform cold boot attacks against Android smartphones and retrieve disk encryption keys from RAM. We show that cold boot attacks against Android phones are generally possible for the first time, and we perform our attacks practically against Galaxy Nexus devices from Samsung."

Authors Tilo Mueller and Michael Spreitzenbarth of the Friedrich-Alexander University of Erlangen-Nuremberg discovered that Android's boot sequence enabled them to perform cold boot attacks, and they observed how valuable information can be retrieved from RAM. According to the researchers, such cold boot attacks can allow the retrieval of sensitive information such as contact lists, visited web sites, and photos, directly from RAM, even though the bootloader is locked. By chilling the Galaxy Nexus, the researchers could bypass security settings and read from the phone's memory. The recovery tool FROST stands for Forensic Recovery of Scrambled Telephones.

In chilling the phone to freezing temperatures, the information lingered on in memory for five or six seconds, which was long enough to pull data out with a computer.

Mueller and Spreitzenbarth found they could read data that included images, e-mails and web browsing history.

Their research is not a first in explorations into cold-boot attacks, which were in evidence as early as 2008, shown on PCs. Their research, however, focused on mobile devices.

The authors referred to data remanence, where the computer RAM holds residual information briefly even after the computer is shut down. Mueller observed that in cooling the phone the contents are lost in five or six seconds, enough time to reboot

the phone and access the memory. Rebooting a phone more often may leave less sensitive data in its memory.

On the flip side, their research is not only a warning for Android users but may be helpful for forensic experts who attempt to recover data from a seized phone.

More information:
www1.informatik.uni-erlangen.de/frost
www1.cs.fau.de/filepool/projects/frost/frost.pdf

APA citation: Danger on ice: Android info thaws in cold boot attack (2013, February 18) retrieved 22 October 2019 from https://phys.org/news/2013-02-danger-ice-android-info-cold.html