Replicant developers find and close Samsung Galaxy backdoor

by [Paul K](https://www.fsf.org/author/paulk) — Published on Mar 12, 2014 04:50 PM

**While working on Replicant, a fully free/libre version of Android, we discovered that the proprietary program running on the applications processor in charge of handling the communication protocol with the modem actually implements a backdoor that lets the modem perform remote file I/O operations on the file system.**

*This is a guest post by*[*Replicant*](http://replicant.us/)*developer Paul Kocialkowski. The Free Software Foundation supports Replicant through its Working Together for Free Software fund.*[*Your donations to Replicant*](https://crm.fsf.org/civicrm/contribute/transact?reset=1&id=19)*support this important work.*

Today's phones come with two separate processors: one is a general-purpose applications processor that runs the main operating system, e.g. Android; the other, known as the modem, baseband, or radio, is in charge of communications with the mobile telephony network. This processor always runs a proprietary operating system, and these systems are known to have backdoors that make it possible to remotely convert the modem into a remote spying device. The spying can involve activating the device's microphone, but it could also use the precise GPS location of the device and access the camera, as well as the user data stored on the phone. Moreover, modems are connected most of the time to the operator's network, making the backdoors nearly always accessible.

It is possible to build a device that isolates the modem from the rest of the phone, so it can't mess with the main processor or access other components such as the camera or the GPS. Very few devices offer such guarantees. In most devices, for all we know, the modem may have total control over the applications processor and the system, but that's nothing new.

While working on [Replicant](http://replicant.us/), a fully free/libre version of Android, we discovered that the proprietary program running on the applications processor in charge of handling the communication protocol with the modem actually implements a backdoor that lets the modem perform remote file I/O operations on the file system. This program is shipped with the Samsung Galaxy devices and makes it possible for the modem to read, write, and delete files on the phone's storage. On several phone models, this program runs with sufficient rights to access and modify the user's personal data. A technical description of the issue, as well as the list of known affected devices is [available at the Replicant wiki](http://redmine.replicant.us/projects/replicant/wiki/SamsungGalaxyBackdoor).

Provided that the modem runs proprietary software and can be remotely controlled, that backdoor provides remote access to the phone's data, even in the case where the modem is isolated and cannot access the storage directly. This is yet another example of what unacceptable behavior proprietary software permits! Our free replacement for that non-free program does not implement this backdoor. If the modem asks to read or write files, Replicant does not cooperate with it.

Replicant does not cooperate with backdoors, but if the modem can take control of the main processor and rewrite the software in the latter, there is no way for a main processor system such as Replicant to stop it. But at least we know we have closed one specific backdoor.

*The FSF encourages all current Samsung Galaxy owners to appeal publicly to*[*SamsungMobile*](http://mobile.twitter.com/SamsungMobile)*for an explanation (they can also be*[*emailed*](http://www.samsung.com/us/support/email/product/)*). Samsung should release this program as free software, without the backdoor, so that Replicant doesn't have to continue defusing the traps they have apparently left for their users.*