Calling Android: Researchers see if Rowhammer-based exploits still possible

July 4 2018, by Nancy Owano

Credit: CC0 Public Domain

Android risks fade... and remorph. A variant of Rowhammer has turned up according to a discovery by researchers from institutions including Vrije Universiteit Amsterdam.

"The attack allows malicious applications to break out of their sandbox

and access the entire operating system, giving an adversary complete control of the targeted device," said *Threatpost*.

Seriously? It is not exaggerating, as the team itself posted this in a blog.

"While apps are typically not permitted to read data from other apps, a malicious program can craft a rampage exploit to get administrative control and get hold of secrets stored in the device. This might include your passwords stored in a password manager or browser, your personal photos, emails, instant messages and even business-critical documents."

The researchers call the new variant RAMpage. The title is inspired by its nature, as the vulnerability involves ramming memory pages to obtain arbitrary read and write access.

The exploit resonates with the Rowhammer type of attack. Long and short, with Rowthammer, data stored in memory chips gets manipulated. Rowhammer itself is not an exploit, said *Android Central*, but is a "term used to describe a hardware issue that affects computer RAM. It's not technically an exploit and happens because of the laws of physics."

Tom Spring in *Threatpost* said the researchers initially identified the flaw in DRAM memory in laptops and PCs in 2015.

A quick Wikipedia nabbed definition: "Row hammer (also written as rowhammer) is an unintended side effect in dynamic random-access memory (DRAM) that causes memory cells to leak their charges and interact electrically between themselves, possibly leaking the contents of nearby memory rows that were not addressed in the original memory access."

The naming of the exploit suggested how the exploit works, in that one hammers at a row of memory cells for an electromagnetic interference

for adjacent rows, causing them to lose data and change normal operation.

In hammering the rows thousands of times a second, said Dan Goodin in *Ars Technica*, "the technique causes the bits to flip, meaning 0s are changed to 1s and vice versa."

Google in the past had indeed acted on this. Google made changes to Android's ION memory manager, said Goodin, "which restricted access to physical contiguous kernel memory." (ION, said *Android Central*, "is a universal generic memory management system that Google added to the Android kernel.")

Were the patches marking the end of that headache? Goodin turned to an email from Prof. Victor van der Veen, Vrije Universiteit Amsterdam. Why not. The professor helped devise both Drammer (before the latest) and RAMpage exploits. He said abusers could play with the allocator.

Tom Spring in *Threatpost* walked readers through how RAMpage works. "It targets an Android's universal generic memory management system called ION introduced by Google in 2011 as part of Android 4.0. It's part of a subsystem used to manage and allocate memory. An attack consists of a write and refresh request on the device's RAM until it flips a bit in an adjacent row. This opens the door to the device compromise."

All in all, mobile devices based on Android shipped with LPDDR2, LPDDR3, or LPDDR4 memory are potentially affected by the RAMpage , said Van der Veen and his colleagues, in a blog post.

The new RAMPpage exploit is the focus of the team's research paper, where they described their defense. The researchers said they're working with Google to find ways to reduce the performance costs GuardION has on real-world apps, according to *Ars Technica*.

Their team is made up of eight academics from four universities and two private companies, said Spring.

Universities include Vrije Universiteit Amsterdam, Amrita University India, UC Santa Barbara and the French graduate school Eurecom. The blog noted "an international collaboration of system security researchers."

Meanwhile, reported *Android Central*, Google reached out to *Android Central* with a statement: "We have worked closely with the team from Vrije Universiteit, and though this vulnerability isn't a practical concern for the overwhelming majority of users, we appreciate any effort to protect them and advance the field of security research. While we recognize the theoretical proof of concept from the researchers, we are not aware of any exploit against Android devices."