A flaw in the memory chip of Android devices is allowing hackers to root Android devices. The flaw, known as Rowhammer, is a hardware vulnerability that does not require user permission or exploit any software vulnerability. It lets hackers exploit the vulnerability through a malicious app and allows them to change content of memory, which otherwise they are unable to access. The user may not have Android app security awareness and install a malicious app that does not require any permissions.

Ever since the publicity of Rowhammer, attacks on Android devices have not yielded consistent results. Out of 15 attacks on Google Nexus 5 handsets, 12 attacks were successful; whereas only one of the two attacks on Samsung Galaxy S5 were successful. Test attacks on other devices such as Galaxy S4 and S6, Moto G models and LG G4 also showed inconsistent results.

An exploit known as Drammer (short form of Deterministic Rowhammer), can root Android devices with the help of a completely unauthorized app. This technique proves that hardware attacks without relying on software vulnerabilities are possible and feasible, and allow attackers to take control of your phone or mobile device even with Android app security in place.

Professor of systems security at Vrije Universiteit Amsterdam, Herbert Bos, along with his team that discovered the exploit, will practically demonstrate it at a security conference in Vienna, Austria. According to him, the demonstration will show that administrator privileges can be acquired from an unprivileged app without looking for a software bug. Although Google tried fixing the problem, it couldn’t be done as the vulnerability lies in the hardware and cannot be exactly fixed with improved Android app security.

Bos and his team have developed “Hammertime”, a Rowhammer simulator, which is available on Github. The researchers have also thought upon the possibility of the attack to work on ARM-based microprocessors since the required “bit-flips” that make the Drammer successful might be slow on an ARM-based memory controller.