**Drammer – A Threat to Millions of Android Devices**

Information security researchers at University of Amsterdam have recently discovered a security vulnerabilitiy in the design of memory chip used in Android devices. This hardware vulnerability, known as Rowhammer, lets hackers aim for a certain memory chip and allows them to gain control of the complete system. When combined with already prevailing attack vectors such as Stagefright or BAndroid, Drammer can be a serious threat to Android app security by targeting millions of Android device users.

Rowhammer bug is not new. Security researchers had previously discovered a similar flaw in Linux-running systems which could be exploited in a similar fashion. This time android devices are affected. Google has given an award of $4000 to the security researchers for identifying this flaw. However, it is not easy to get rid of this bug and it will take a while before Android app security can be improved with the removal of this bug from Android devices.

**How does the attack work?**

The Drammer attack, just like its name suggests, targets or “hammers” a row of transistors in the DDR DRAM memory chip installed in a mobile android device. Attack is carried out through a malicious app that the user has unknowingly installed in the system. The attacker first embeds the code in the malicious app and once it is executed, the app continually accesses a certain row of transistors. This repetition becomes a cause of electric disturbance in the nearby rows, which in turn leaks electricity, thus resulting in a bit flip. With a successful bit flip, i.e. the interchanging of data bits in random locations, the hacker gains the ability to values of stored data on the chip and finally gain access to the attacked device.

Drammer is the first ever Android root exploit that does not rely on software vulnerability. Researchers are now trying to improve Android app security by developing apps that can detect the rowhammer bug in android devices.