Active Simulating cold boot attacks in the gem5 simulator

Loïc France
LIRMM, Université de Montpellier, France

Abstract

Modern computers rely heavily on their memories to store confidential data, such as cryptographic keys. Maintaining a device secured relies heavily on keeping aggressors from accessing these data. As such, the long-term storage of confidential data is secured using cypher algorithms, which make the data unreadable without a key to decipher it. However, run-time data cannot be protected by these algorithms, as this data must be accessed directly by the registers to perform operations on it. For example, cypher keys must be stored in the run-time memory for the device to process cipher and decipher secured data.

As long as the aggressor does not penetrate the running system, unprotected data in the run-time memory are usually not threatened, as this data rapidly decays when the system shuts down. Modern computers use the DRAM technology for its run-time memory, which stores data using capacitors. Once unpowered, the capacitors lose their charge and the stored data in a few seconds.

However, it has been demonstrated that by cooling the memory, one can largely increase the time for the DRAM to lose its data [1]. Therefore, by cooling the memory before un-plugging it from the victim computer and plugging it to an aggressor device, one can recover the majority of the data stored in the memory. Alternatively, the system can be shut down and quickly booted on a bootable drive that can extract the data from the memory, without the need to extract the physical memory from the device [2].

Over the years, the security community has proposed multiple solutions to protect the data in the memory from this attack. For example, detecting sudden temperature changes to wipe the memory before

the memory is extracted, or exploit features of the boot mechanism to prevent accessing encryption keys after a reboot [3].

However, all these solutions only make the attack harder, they do not prevent it. Moreover, as emerging non-volatile memories will eventually replace the DRAM technology, the data will be stored in the memory long after they are powered off, making cold-boot attack even easier to execute [4].

In order to make the development of countermeasures easier, and to evaluate the vulnerability of systems against the cold-boot attack, we modified the architecture simulator gem5 to integrate the simulation of cold-boot attacks, enabling a system to be booted with a memory filled with the data from another simulation.

[1] Skorobogatov, Sergei. "Low temperature data remanence in static RAM," 2002.

[2] Halderman, J. Alex, et al. "Lest we remember: cold-boot attacks on encryption keys," 2009.

[3] McGregor, Patrick, et al. "Braving the cold: New methods for preventing cold boot attacks on encryption keys," 2008.

[4] Pan, Xiang, et al. "Nvcool: When non-volatile caches meet cold boot attacks," 2018.