Lest we remember: cold-boot attacks on encryption keys

Although while computers are powered on, the OS can defend against hackers coming in and taking things, however when the computer is off the memory’s info is still vulnerable. Although most types of memory differ, at room temperature the rate of decay on memory is pretty fast, and the decay rate at very cold temperatures is fairly slow, so one way to hack and get info from memory is to make it very cold and move it to another computer to get data from it. In the article many different methods of attacks were described to get data from machines such as:

* PXE Network Boot – Intel CPU’s have PXE on them which allow for network booting, so the writers wrote an attack which would run inside the PXE and dump all the memory to a laptop connected via Ethernet crossover.
* USB drives – Save the memory into the usb after from it via SYSLINUX
* EFI Boot – Recent computers including intel-based mac computers implement EFI. If you implement a memory dumper as an EFI netboot application, we can just dump memory that way.
* IPods – Memory dumpers have been installed on IPods to dump memory in a concealed manner.

Simple reboots can allow for us to dump memory as long as we perform a cold reboot. If none of the techniques described pose successful then we can transfer the DRAM modules by inverting a can of air duster and spraying it onto the memory and transfer to an external device with permissive properties.