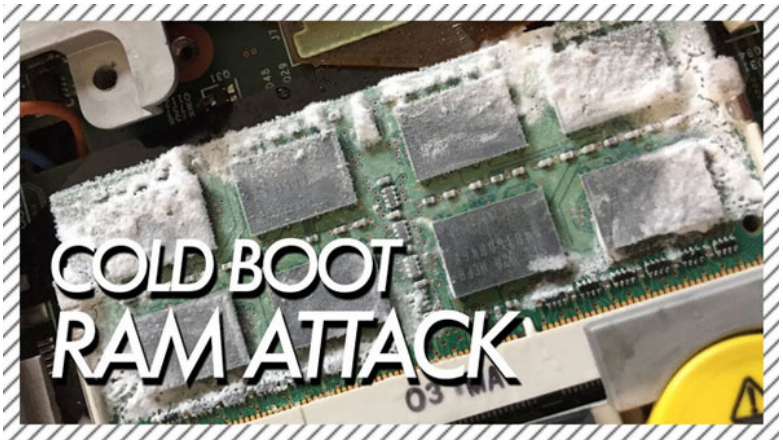
Bad guys can steal data by freezing RAM sticks with liquid nitrogen

With the cold boot attack technique, one can separate data from a RAM bar after it is turned off.

RAM (Random Acesss Memory) is a temporary data storage of the device. The information stored on RAM will completely disappear if the device suddenly loses power.

However, with the cold boot attack technique, one can separate data from a RAM stick after it is turned off. This technique is an illegal hacking activity, used in forensic science, data recovery.

The cold boot attack technique is applied on DRAM. When a power failure, this type of RAM will not lose data immediately but will discharge slowly over time.

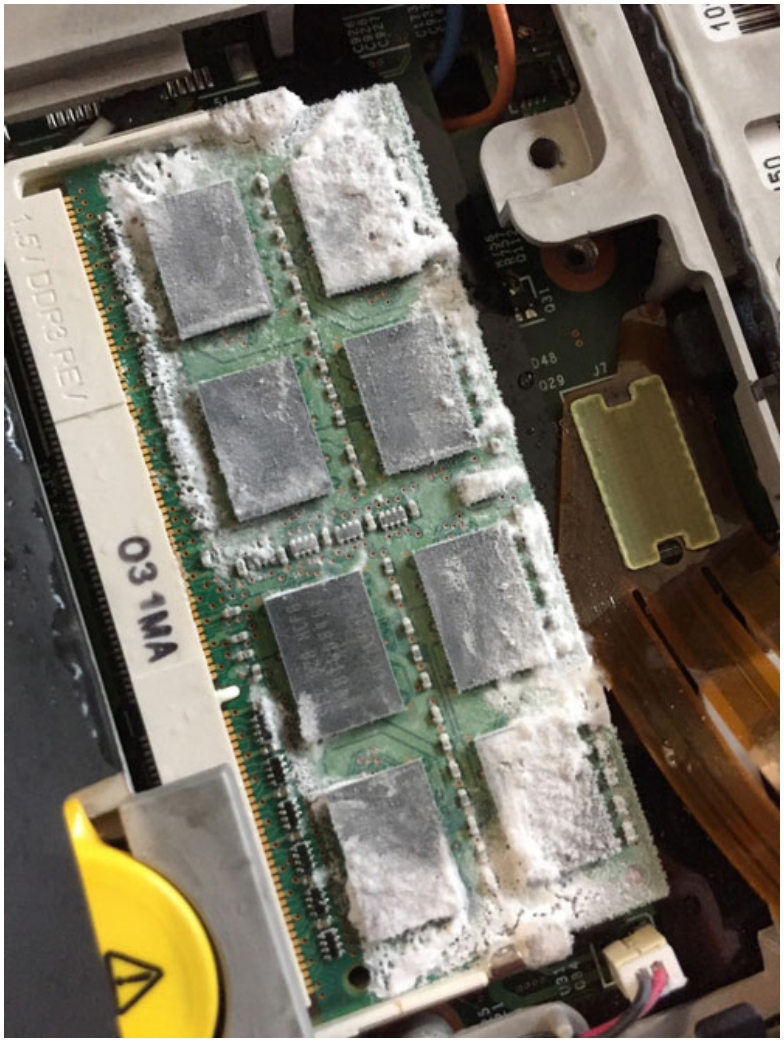


This method is called Cold Boot RAM Attack.

Theoretically, the discharge time of a DRAM bar is inversely proportional to the temperature. This means the colder the RAM is, the longer it will discharge.

At room temperature, DRAM takes only a few milliseconds to discharge. But if the temperature is below -50 degrees Celsius, this time can last up to tens of seconds. This amount of time is enough for engineers to remove the DRAM stick from the motherboard and place it on another computer. The data on it will be read through a type of software that can store this data on the hard drive.

One of the cooling methods people often use on microprocessors is liquid nitrogen.



When cooling a DRAM bar, bad guys can easily steal data.

This technique can also be used to attack mobile devices. Usually mobile phones do not have a reset button, so in order to catch the reset system to enable cold start, we have to disconnect the phone battery. The phone then connects to the user's computer via USB and is flashed by an operating system that can "dump" data from RAM, and then store it on memory.

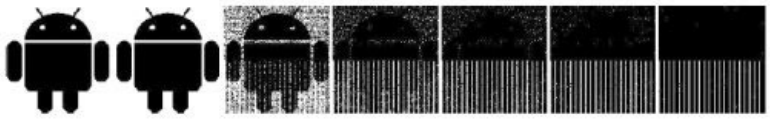


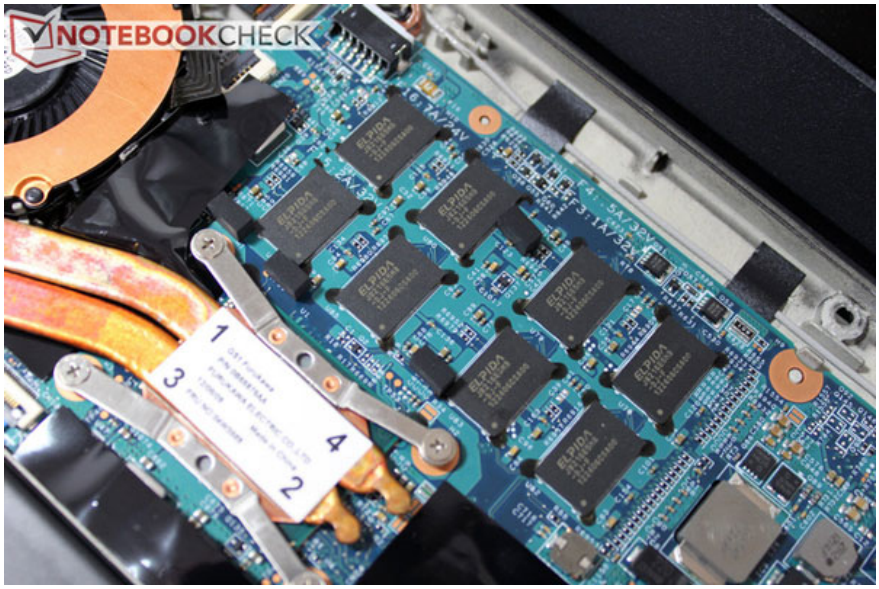
Fig. 4. A Droid-bitmap in RAM of a Galaxy Nexus device after 0, ε, 0.5s, 1s, 2s, 4s, and 6s without power. The cold boot attacks have been deployed at room temperature.

An image is stored on RAM timelines after 0, 0.5, 1, 2 and 4 seconds.

So to deal with cold boot attack technique, what methods do we have?

1. Buy computers with soldered RAM sticks to the motherboard. This gives the attacker an opportunity to remove them from the machine.

2. Encrypt the entire memory, but this requires changes from the operating system, software and hardware.
3. "SEOM", or Secure Erasure Of Memory - forces the BIOS to clear all memory when the computer is not being used.



1. 10 operating systems for security research preferred by hackers
2. Viettel, VinaPhone, VNPT, Mobifone, FPT . block websites containing videos and 18+ images on computers and phones?

You finished reading the article "**Bad guys can steal data by freezing RAM sticks with liquid nitrogen**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

© 2019 TipsMake.com