Frozen RAM is not a Fast Food: Cold Boot Attacks Change the Data Leakage Landscape

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

As always, it’s a pleasure to collaborate with my current and present graduate students in bringing you thoughtful articles. Jürgen Pabel graduated from the MSIA program in June 2004 in the first graduating class; he is an experienced network engineer and security consultant in Köln (Cologne), Germany and has become a valued friend and colleague.

Recently Jürgen and I collaborated on this column and the next; Jürgen wrote the first draft and then I provided additional material, edits and references. In what follows, “I” refers to Jürgen.

* * *

Until 2008, the consensus has been that there would be no practical way to remove a RAM chip from a computer system without losing all contained data.

However, in July 2008, J. Alex Halderman< http://www.cs.princeton.edu/~jhalderm > and a research team including Dr Edward W. Felten< http://www.cs.princeton.edu/~felten > at the Center for Information Technology< http://citp.princeton.edu/ > at Princeton University< http://www.princeton.edu/main/ > published a paper< http://citp.princeton.edu/pub/coldboot.pdf > about something quite amazing: most random-access memory (RAM) chips maintain their data for several seconds without any power, thus allowing a channel for data leakage from any computer to which an attacker has physical access. The group has established an excellent Web site full of information about this “cold boot attack”< http://citp.princeton.edu/memory/ >; the site includes a five-minute video lecture about the attack, some frequently asked questions< http://citp.princeton.edu/memory/faq >, an guide to the experimental methods< http://citp.princeton.edu/memory/exp >, some source code< http://citp.princeton.edu/memory/code >, and a collection of additional videos and photographs< http://citp.princeton.edu/memory/media >.

The time over which the data are remembered depends largely on the make of the RAM chips. However, cooling RAM chips down to -50°C (-58°F) prior to power loss causes a significant prolongation of the data retention time, usually to several minutes. Therefore, it is now feasible to extract all data stored in live memory from a powered-on computer system by removing the cooled RAM chips and placing them into another computer system for analysis. Under certain circumstances, it is not even necessary to physically move the RAM chips to another computer system: if the system is configured to allow booting from external media (e.g., CD/DVD, USB flash drive or those ancient floppy disks that some readers remember) then it may be possible to simply reset the system and to boot into a software-analysis environment such as. This approach would usually work because the basic input output system (BIOS) on most computers is configured to skip over RAM integrity checks for performance reasons; the checks would otherwise write a test pattern to all memory cells and read them back to verify the functional integrity of the hardware chips in RAM.

It might seem odd for an adversary to specifically target data in RAM if they have physical access to the target computer system – they could just easily access any data by reading it from
the disk drive. However, if the target system is protected by a full disk encryption solution then the data on the disk drive are practically inaccessible unless the adversary extracts the disk’s cryptographic key from RAM.

Cold boot attacks represent a new vulnerability. The most significant aspect of this vulnerability is that no effective countermeasure exists; Halderman et al. write, “Though we discuss several strategies for partially mitigating these risks, we know of no simple remedy that would eliminate them.” Thus, other actions must be implemented in order to address the associated risk. In theory, it would be a trivial and effective solution to always power off the computer system any time it is about to be potentially exposed to unauthorized physical access. However, practical implications render this approach unfeasible: nobody is going to power down their workstation every time they leave the room or even the building – and most servers are up as much as possible. Another solution would be to switch from software-implemented full disk encryption to hardware-implemented products such as the self-encrypting hard drives manufactured by Fujitsu, Hitachi, and Seagate<http://news.cnet.com/8301-1009_3-10097371-83.html>; however, the higher acquisition and migration costs are likely to delay universal implementation, especially with the worldwide economy in a slump (although Forrester Research predicts continued growth in security expenditures<http://www.darkreading.com/security/management/showArticle.jhtml?articleID=212700661>).

One obvious question has not yet been addressed: just how much of a risk does this attack pose? Well, there’s no quantitative answer. However, a generic and non-representative answer can be derived by considering the preconditions and circumstances. First, an adversary must be able to obtain physical access to a powered on and running computer system. Second, the screen must be locked at the time of loss or theft – if the screen is unlocked then an adversary usually has access to all data and functions immediately. And last, the adversary must be somewhat technically versed in order to carry out the attack. Therefore, it might be a fair assumption that most opportunistic thieves are not a relevant threat as they are usually only driven by the monetary value of the hardware and might not possess the necessary technical skills to execute a cold boot attack. On the other hand, targeted attacks are usually carried out by well-versed and well-funded adversaries. Whether these adversaries might resort to an attack that also employs a cold boot attack on a target computer system is entirely dependent on the specific circumstances – it’s always about the weakest link from the adversary’s point of view. Though we discuss several strategies for partially mitigating these risks, we know of no simple remedy that would eliminate them.

Nevertheless, cold boot attacks are essentially an unmanageable risk – and that’s about as bad as it gets. However, I am currently researching a concept that should effectively protect cryptographic keys against cold boot attacks. More on that in the second part of this article.

* * *


M. E. Kabay, PhD, CISSP-ISSMP <mailto:mekabay@gmail.com> specializes in security and operations management consulting services. CV online.<http://www.mekabay.com/cv/>
Permission is hereby granted to *Network World* to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.