



Reality Check

Princeton Attack on Software Encryption

Researchers at Princeton have published results of their attack on software encryption, in a report titled “Lest We Remember: Cold Boot Attacks on Encryption Keys.”

The Princeton research focused on a well-known property of DRAM (dynamic RAM) called remanence, which can leave a cryptographic key stored in desktop or laptop computer memory (and the related encrypted data) vulnerable to attack.

Remanence means that DRAM retains stored data for a short period after powering down the computer. Cooling the DRAM after turning the computer off can extend the remanence period to several minutes or longer, giving attackers enough time to access the DRAM and extract the key.

The researchers, using computers with three different software-based encryption programs, described and tested three types of attacks:

- Re-boot, launch custom kernel, gain access to memory
- Cut power, restore power, launch custom kernel
- Cut power, transfer DRAM to another computer

Even though the attacks are impractical under most circumstances, the Princeton researchers noted that security best practices, including powering down or hibernating unattended computers to drain the DRAM memory, will thwart such an attack.

Measures such as screen-locking and suspension alone will not prevent DRAM attacks since, with each, the computer remains powered up. Current software solutions do not erase keys from memory while the computer is powered up.

The paper demonstrates not only how to identify, extract and reconstruct encryption keys from key shards found in memory, but how to use error correction techniques to recover corrupted (faded) keys.

DRAM attacks to hardware-based full disk encryption (FDE) drives, the technology that powers the Seagate® Momentus® 5400 FDE.2 drives for laptop computers, are not possible, because the cryptographic key never leaves the hard drive. The key is not stored in DRAM, but in the ASIC chip that implements the encryption algorithm, which is built into the drive.

To Learn More

- The report titled “Lest We Remember: Cold Boot Attacks on Encryption Keys” can be found here: <http://citp.princeton.edu.nyud.net/pub/coldboot.pdf>.

Princeton Attack on Software Encryption



No probe points or external interfaces are provided to the key stored in disk drives. Moreover, any attempt to extract the tightly integrated memory from the drive package and move it to another system cuts off the power, locking the drive and erasing the encryption key from the drive's memory.

Full Disk Encryption Q&A

Note: *Software encryption* means that the encryption is implemented in software running on the computer. *Hardware full disk encryption (FDE)* means that the encryption is implemented in the processor hardware on the hard drive.

Q: What types of encryption are vulnerable to the key theft highlighted in the Princeton paper?

A: Most software encryption packages are vulnerable to this theft. In the vulnerable software encryption packages, the encryption key is kept in memory while the system is booted and running, allowing the operating system to encrypt data as it is written to disk. Since the key is preserved in memory during power on, it is possible to steal the key by locating that copy and saving it for use later. Software encryption programs can conceal the key by dismantling it and storing the pieces in various locations in memory, though this defense can degrade performance and explains why most software encryption programs keep the key intact in one location. Another way to defend against the freezing DRAM attack is to keep the encryption key in special CPU registers or a locked section of the CPU cache—a feature of few software encryption programs.

Q: My key is 128 to 256 bits in 1 GB (or more) of memory. Isn't this like looking for a needle in a haystack?

A: Usually the hacker must exploit some weakness in the operating system to access the system memory. By freezing the DRAM, the hacker can gain access to the system memory without having to circumvent the operating system or other protections designed to secure computer memory from unauthorized users. The process is as simple as freezing the DRAM, shutting down the computer, moving the DRAM to another

computer and searching for encryption keys as described above. Once the program finds an encryption key, it copies the key elsewhere for later use. Locating the key is much easier because the operating system is not loaded and therefore unable to protect the computer's memory from nefarious searches.

Q: Why would someone want to steal my key? Wouldn't it be easier to just steal my data?

A: It depends on what the thief wants. In order for the frozen DRAM exploit to work, your computer must be up and running with software encryption working, so the thief could just steal your data by copying it from your computer to an external storage device, such as an external hard drive. The thief gets a copy of whatever you have on your computer at that time. By stealing the key, the thief can return at any time, power up your computer, install the encryption key and get your data.

Q: Can I change my encryption key to keep a thief from getting my data?

A: You must change your encryption key and rewrite all of the data that was encrypted under the previous encryption key. If someone has stolen your encryption key and you change to a new key, the data written under the previous key is vulnerable. In order to make the data secure, you must re-encrypt all of your data with the new encryption key.

Q: If I power off my computer, am I vulnerable to data theft?

A: No, provided you wait a few minutes after power down, until the memory loses its contents. If your data is encrypted and your system is powered off, your data is safe from theft. You must leave your computer in the hibernate mode or power it off completely to secure your data. In addition, it is important not to leave your computer unattended for a half hour or so (depending on the type of memory it uses), because data loaded to RAM does not disappear instantly.

Princeton Attack on Software Encryption



Q: If I power off my computer, am I vulnerable to key theft?

A: Yes, you are vulnerable to at least two types of attacks, if you are using a software encryption package that keeps its encryption keys in memory. First, it will take several seconds or even minutes for the contents of your memory to decay, so a hacker that accesses the computer soon after it has powered down can tap the computer's memory to find the encryption keys. Second, a hacker could write a program that scans your computer's memory anytime your system is booted and encryption is running. This program could run quietly in the background, locating and capturing any encryption keys left in memory. Hardware FDE keeps your encryption keys out of computer memory at all times, protecting the keys against this type of theft.

Q: Does the type of encryption matter in this theft?

A: No. Encryption relies on what is termed "symmetric key cryptography" by security experts—the same key is used to encrypt and decrypt the data. For symmetric key cryptography, the key must be as random as possible, regardless of the type of encryption used.

Q: What can I do to prevent this theft?

A: Never leave your computer running where it can be easily accessed by a potential hacker or thief, and be sure to wait a few minutes before leaving your computer to allow the contents of your DRAM to gradually disappear. *If a thief or attacker cannot get physical possession of your computer, he or she cannot freeze your DRAM or get to your data.* If this is not possible, never leave your computer unattended in standby mode. Instead, always use the hibernate mode anytime you are not present. In the standby mode, your computer keeps the operating system and encryption keys in memory so that the system can restart as quickly as possible (whenever you open the lid). In hibernate mode, all contents of memory are written to disk and the system is powered down. After a few minutes, the computer's memory is empty, so freezing the DRAM will be useless. The disadvantage of this mode is that it takes longer for the system to load

(~10 seconds longer for the newest laptops) and the user password must be entered each time the computer lid is opened.

Q: Is it possible to remove my encryption key from memory when my computer is in standby mode?

A: Yes. Your software encryption could erase the encryption key each time you go into standby mode (i.e., shutting the lid on your laptop), but this will require that you re-enter your password each time you open the lid on your laptop, since the key will be lost. Please note that your software must explicitly erase the encryption key. Requiring a password each time you open the lid is not enough.

Q: How does hardware FDE help?

A: Hardware FDE, such as that provided by the Seagate Momentus 5400 FDE.2 drive, never leaves the encryption key in the laptop's memory. Since the encryption key is never in memory, a hacker can never find it by scanning memory, and the laptop user's data is much less vulnerable. Of course, even the Momentus 5400 FDE.2 drive offers little protection if a user leaves the laptop unattended in standby mode. All a thief needs to do is to lift the laptop lid, and (assuming that some type of password protection upon resuming from standby has not been set up) copy all of the data to an external storage device.

Q: Is hardware FDE vulnerable to the DRAM freezing attack?

A: No. The drive memory and components on the Momentus 5400 FDE.2 drive are mounted in a way that would require a hacker to remove the drive's PCBA (printed circuit board assembly) and flip it over in order to gain access—a process that would cut off power to the drive, locking it and removing the encryption keys from drive memory. In addition, the Momentus 5400 FDE.2 drive keeps encryption keys in drive memory for as short a time as possible and overwrites the key with zeros after each use. Because keys can be contained in drive memory, Seagate carefully secures the drive using hardware and software mechanisms to prevent access to the drive memory by all but authorized users.

Princeton Attack on Software Encryption



Q: What about passwords? Is it possible to find passwords in memory?

A: Yes. Anytime a program prompts for a password, it is stored temporarily in your computer's memory. If the program does not erase the password, it may linger for several seconds to many hours, depending on how much memory is needed by the programs you are running. During this time, it is possible to search the computer's memory and locate any un-zeroed passwords. All types of encryption are vulnerable to password theft. Two ways to avoid password theft: make sure the software you use to support encryption erases passwords immediately after use, and shut down or hibernate your computer anytime you are not able to protect it against physical access or theft.

AMERICAS Seagate Technology LLC 920 Disc Drive, Scotts Valley, California 95066, United States, 831-438-6550
ASIA/PACIFIC Seagate Technology International Ltd. 7000 Ang Mo Kio Avenue 5, Singapore 569877, 65-6485-3888
EUROPE, MIDDLE EAST AND AFRICA Seagate Technology SAS 130-136, rue de Silly, 92773, Boulogne-Billancourt Cedex, France 33 1-4186 10 00

Copyright © 2008 Seagate Technology LLC. All rights reserved. Printed in USA. Seagate, Seagate Technology and the Wave logo are registered trademarks of Seagate Technology LLC in the United States and/or other countries. Momentum is either a trademark or registered trademark of Seagate Technology LLC or one of its affiliated companies in the United States and/or other countries. All other trademarks or registered trademarks are the property of their respective owners. When referring to hard drive capacity, one gigabyte, or GB, equals one billion bytes and one terabyte, or TB, equals one trillion bytes. Your computer's operating system may use a different standard of measurement and report a lower capacity. In addition, some of the listed capacity is used for formatting and other functions, and thus will not be available for data storage. Though encryption methods used in Seagate products provide a certain level of security, no method of encryption is completely secure. Exercise caution in selecting and securing your password and protecting the physical security of your product. Seagate reserves the right to change, without notice, product offerings or specifications. Publication Number: RC514.1-0702US, February 2008