



Facts from CE-Infosys regarding the Princeton Research Report on Hard Disk Encryption

Executive Summary

This paper is in response to the recently published Princeton report in which the authors outlined one method to retrieve encryption keys in the RAM from a stolen machine, hence breaking most software encryption products. This attack has been known to CE-Infosys for a long time, and we have continuously advocated that software encryption is only entry level. Governments and other organisations with highly sensitive data should use hardware encryption according to CE-Infosys' recommendations.

The wide-reaching nature of this attack means that other encryption products based on PC architectures, in particular network encryption products can also be compromised. These network encryption products implement a VPN and are widely deployed in many organisations today.

To mitigate the risk of this attack, we've suggested configuring the BIOS of machines to only boot from the primary hard disk. Also, we've recommended that only software encryption products that properly encrypt the RAM during hibernation be used. However, to fully solve this problem, governments and organisations with highly

sensitive data must use hardware encryption products that are properly designed.

CE-Infosys has a range of these products, namely the CompuSec Mobile and CompuSec HSM for notebooks and PCs respectively, as well as the MicroCryptors, PowerCryptors and GigaCryptors for network encryption. For even higher security, the ANIS range of network encryption products feature sensors that are able to detect and defeat all known attacks today, including the attack described in Princeton's research paper.

Introduction

We refer to the research paper, "Lest we remember: Cold Boot Attacks on Encryption Keys" from Princeton University, retrieved from <http://citp.princeton.edu/memory>.

In this article, we will elaborate upon the attack, and we will augment Princeton's research with our knowledge and experience in the security market. We also recommend some actions that security administrators can take, so as to mitigate the risk posed by this attack. Lastly, we will present the solution to this problem.

Further Description of Attack

In this research paper, the authors claim to have found an attack for hard disk encryption software such that the encryption keys used can be stolen by dumping the contents of the RAM in the machine. This is correct and can be formalised in a more general way. As long as you use a processor to encrypt data, the encryption algorithm and the keys must be directly accessible by this processor. This means storing it in the random access memory (RAM) attached to the processor. In today's systems, these are usually DDR-2 modules that are easily detachable. As soon as you find a way of copying the contents of the RAM, you have the keys and the encryption algorithm as well. This includes all the encryption keys that were in the RAM, including your VPN keys, keys used to protect passwords and others.

The attack used in the Princeton research is based on the fact that the DDR memory of a computer takes some time to lose its electrical charge even after power is removed. The time taken is longer when the molecular movement in the RAM is slowed, such as when the memory chips are cooled to a low temperature. Experts know this as the "Freon Attack".

The Princeton researchers then used this opportunity when the memory contents are not totally discharged to make a full copy of the data still stored in it. This can be done in 2 ways, first by booting the computer from an external media, such as a memory stick or a bootable hard disk, and run a simple memory copy routine. Booting from a temporarily attached boot server will also work if the computer is configured to boot from a network. This method is fast, easy and you need only access to the computer a short time after the authorised user has switched the machine off. We will describe a counter-measure for this attack further in this article.

The second way to copy the data requires physical access to the hardware. You will need to remove the memory modules from the original computer and insert them into another computer that uses the same type of memory module. After opening the cover, the attacker can spray the modules with a cooling liquid to slow the discharge of the RAM contents, before physically moving the RAM modules to another computer. Today's systems are designed to provide easy access to memory for ease of expansion or service, which makes it effortless to physically access the RAM modules.

With this knowledge, the Princeton researchers successfully found the encryption key from recently powered-off machines, and managed to access the machines' encrypted hard disks, thereby rendering the encryption on these machines useless.

Extension of Attacks

In both cases, you will need undetected physical access to the computer to perform the described attack. There are other methods of receiving a copy of your memory contents. One example is the well known memory dump that is created after a blue screen crash of the operating system. Another method to get a copy of the memory contents is through the hibernation file on the hard disk. In some encryption products, this hibernation file is stored in plain text, and can be easily retrieved from the hard disk. The keys can then be found easily from the copy.

These attacks are not new and for that reason CE-Infosys has been advocating that software encryption only provides an entry level protection. In all our discussions with governments and organisations, we have impressed upon them the importance of using hardware encryption for highly sensitive data. In our opinion, there is no known software encryption system available to prevent any of these attacks. The keys have to be kept in the memory, so that the system is able to transparently decrypt data when accessed from the hard disk. As such, these keys are at a risk of

being stolen when such an attack is applied. For this reason, all software encryption products are vulnerable to these kinds of attack.

Mitigating the Risk

To mitigate the risk of such an attack, we recommend administrators configure the BIOS to only boot from the primary hard disk. This will reduce the risk of the attacker using a bootable external media to run software to dump the memory. In addition, the BIOS should be password protected to prevent any unauthorised changes to the BIOS configuration. Although this method does not totally eliminate the risk of this attack, it makes it more difficult for this attack to be carried out.

Security administrators can also ensure that the software encryption products they are using support hibernation correctly. This means that when the machine is hibernated, the contents of the RAM must be encrypted first, before being stored into the hard disks.

Some encryption products on the market allow the organisation to install their software on multiple machines using disk imaging, which cause these machines to use the same hard disk encryption key. This flawed method is absolutely unacceptable and poses high risks as this attack has revealed. Administrators must make ensure that your encryption product vendor uses a completely different and independent key for each and every computer being encrypted.

CE-Infosys has informed the computer manufactures of a counter-measure that can be implemented in the system BIOS of their machines. With this modification, the attacks mentioned by the Princeton researchers can work only if the memory modules are physically removed from the computer. It is now up to these notebook manufacturers to implement these counter-measures.

Other Forms of Encryption Products Are Also Vulnerable

A little known fact is that such an attack is not only possible on PCs or notebooks with hard disk encryption software, but also on some existing network encryption products currently available in the market. These products implement a virtual private network (VPN) between company locations in different parts of the world. Most of these products use a CPU to perform the encryption, and during this operation, store the encryption keys on the RAM in the machine, just like a normal PC or notebook. As such, these keys can be read from the RAM easily with the described attack from Princeton. With this key available, large amounts of data sent through the VPN everyday between different offices is at risk.

Solution

The only solution to this problem is to use hardware encryption products for all forms of encryption in the organisation. These products must perform the encryption and the key management in hardware, such that the key is never in the RAM of the system. Encryption in hardware means to have a dedicated encryption chip. This is essentially different from having a separate CPU to perform the encryption. In addition, these products must feature strong user authentication to prevent any unauthorised use of a stolen encryption product.

The possibility of such kinds of attacks was the reason why CE-Infosys developed a range of hardware encryption products targeted at governments and organisations with sensitive data. These hardware encryption products are designed so that the encryption keys are only used inside an encryption chip. Unlike the RAM, this encryption chip is not readable even with physical access, therefore the encryption keys used in this chip is always secure and kept secret. 2-factor pre-boot authentication is required before the key can be activated in the encryption chip. Only after such a successful authentication the encrypted hard disk can be accessed and the computer used.

For PCs and notebooks, the products with this architecture are the CompuSec HSM and the CompuSec Mobile. These products use an encryption chip, managed by a separate processor. A smartcard or a USB token is required, together with a password, before the user can gain access to the machine. The products in CE-Infosys' network encryption range, MicroCryptor, PowerCryptor and GigaCryptor, all feature this same architecture. The encryption of the packets is performed in the encryption chip, and a separate processor manages other aspects of the product.

In the high end network encryption products featuring the ANIS capability, an array of sensors is built into the product. These sensors detect physical access to the products, such as opening the casing, movement of the product while in operation and sudden temperature changes. These sensors make these ANIS products resistant against all known attacks, including the recently disclosed ones.

Conclusion

Software encryption provides only an entry level protection for the confidentiality of data in the machines, and can be defeated by a determined attacker. One example is described in the Princeton research paper. The attack described can also be applied to other encryption products as well, thus, it is imperative for governments and organisations to use hardware encryption for the encryption of their data.