Attack on computer memory reveals vulnerability of widely-used security systems

February 21 2008

A combination of frost and refrigerant around the computer's memory chips. At this temperature, memory contents last for several minutes with almost no loss of information.

A team of academic, industry and independent researchers has demonstrated a new class of computer attacks that compromise the contents of "secure" memory systems, particularly in laptops.

The attacks overcome a broad set of security measures called "disk encryption," which are meant to secure information stored in a computer's permanent memory. The researchers cracked several widely used technologies, including Microsoft's BitLocker, Apple's FileVault and Linux's dm-crypt, and described the attacks in a paper and video published on the Web Feb. 21. (Video is available here:

www.youtube.com/watch?v=JDaicPIgn9U)

The team reports that these attacks are likely to be effective at cracking many other disk encryption systems because these technologies have architectural features in common.

“We’ve broken disk encryption products in exactly the case when they seem to be most important these days: laptops that contain sensitive corporate data or personal information about business customers,” said Alex Halderman, a Ph.D. candidate in Princeton’s computer science department. “Unlike many security problems, this isn’t a minor flaw; it is a fundamental limitation in the way these systems were designed.”

The attack is particularly effective against computers that are turned on but are locked, such as laptops that are in a “sleep” or hibernation mode. One effective countermeasure is to turn a computer off entirely, though in some cases even this does not provide protection.

Halderman’s Princeton collaborators included graduate students Nadia Heninger, William Clarkson, Joseph Calandrino, Ariel Feldman and Professor Edward Felten, the director of the Center for Information Technology Policy. The team also included Seth Schoen of the Electronic Frontier Foundation, William Paul of Wind River Systems and independent computer security researcher Jacob Appelbaum.

Felten said the findings demonstrate the risks associated with recent high-profile laptop thefts, including a Veterans Administration computer containing information on 26 million veterans and a University of California, Berkeley laptop that contained information on more than 98,000 graduate students and others. While it is widely believed that disk encryption would protect sensitive information in instances like these, the new research demonstrates that the information could easily be read even when data is encrypted.

“Disk encryption is often recommended as a magic bullet against the loss of private data on laptops,” Felten said. “Our results show that disk encryption provides less protection than previously thought. Even encrypted data can be vulnerable if an intruder gets access to the laptop.”

The new attacks exploit the fact that information stored in a computer’s temporary working memory, or RAM, does not disappear immediately when a computer is shut off or when the memory chip is taken from the machine, as is commonly thought. Under normal circumstances, the data gradually decays over a period of several seconds to a minute. The process can be slowed considerably using simple techniques to cool the chips to low temperatures.

Disk encryption technologies rely on the use of secret keys -- essentially large random numbers -- to encode and protect information. Computers need these keys to access files stored on their own hard disks or other storage systems. Once an authorized user has typed in a password, computers typically store the keys in the temporary RAM so that protected information can be accessed regularly. The keys are meant to disappear as soon as the RAM chips lose power.

The team wrote programs that gained access to essential encryption information automatically after cutting power to machines and rebooting them. The method worked when the attackers had physical access to the computer and when they accessed it remotely over a computer network. The attack even worked when the encryption key had already started to decay, because the researchers were able to reconstruct it from multiple derivative keys that were also stored in memory.

In one extremely powerful version of the attack, they were able to obtain the correct encryption data even when the memory chip was physically removed from one computer and placed in another machine. After obtaining the encryption key, they could then easily access all

information on the original machine.

“This method is extremely resistant to countermeasures that defensive programs on the original computer might try to take,” Halderman said.

The attacks demonstrate the vulnerability of machines when they are in an active state, including “sleep mode” or the “screen lock” mode that laptops enter when their covers are shut. Even though the machines require a password to unlock the screen, the encryption keys are already located in the RAM, which provides an opportunity for attackers with malicious intent.

None of the attacks required specialized equipment. “I think we're going to see attackers doing things that people have previously though impractical or impossible,” Appelbaum said.

The researchers were able to extend the life of the information in RAM by cooling it using readily available “canned air” keyboard dusting products. When turned upside down, these canisters spray very cold liquid. Discharging the cold liquid onto a memory chip, the researchers were able to lower the temperature of the memory to -50 degrees Celsius. This slowed the decay rates enough that an attacker who cut power for 10 minutes would still be able to recover 99.9 percent of the information in the RAM correctly.

“Hints of problems associated with computers retaining their temporary memory have appeared in the scientific literature, but this is the first systematic examination of the security implications,” said Schoen.

The researchers posted the paper describing their findings on the website of Princeton’s Center for Information Technology Policy. They submitted the paper for publication and it is currently undergoing review.

In the meantime, the researchers have contacted several manufacturers to make them aware of the vulnerability: Microsoft, which includes BitLocker in some versions of Windows Vista; Apple, which created FileVault; and the makers of dm-crypt and TrueCrypt, which are open-source products for Windows and Linux platforms.

“There’s not much they can do at this point,” Halderman said. “In the short term, they can warn their customers about the vulnerability and tell them to shut their computers down completely when traveling.”

In the longer term, Halderman said new technologies may need to be designed that do not require the storing of encryption keys in the RAM, given its inherent vulnerability. The researchers plan to continue investigating this and other defenses against this new security threat.

More information: citp.princeton.edu/memory/

Source: Princeton University