The New York Times | https://www.nytimes.com/2008/02/22/technology/22chip.html

Researchers Find Way to Steal Encrypted Data

Princeton-based researchers broke the encryption system by freezing memory chips, permitting them to read the software.
Center for Information Technology Policy, Princeton University

By John Markoff

Feb. 22, 2008

SAN FRANCISCO A group led by a Princeton University computer security researcher has developed a simple method to steal encrypted information stored on computer hard disks.

The technique, which could undermine security software protecting critical data on computers, is as easy as chilling a computer memory chip with a blast of frigid air from a can of dust remover. Encryption software is widely used by companies and government agencies, notably in portable computers that are especially susceptible to theft.

The development, which was described on the group’s Web site Thursday, could also have implications for the protection of encrypted personal data from prosecutors.

The move, which cannot be carried out remotely, exploits a little-known vulnerability of the dynamic random access, or DRAM, chip. Those chips temporarily hold data, including the keys to modern data-scrambling algorithms. When the computer’s electrical power is shut off, the data, including the keys, is supposed to disappear.

In a technical paper that was published Thursday on the Web site of Princeton’s Center for Information Technology Policy, the group demonstrated that standard memory chips actually retain their data for seconds or even minutes after power is cut off.

When the chips were chilled using an inexpensive can of air, the data was frozen in place, permitting the researchers to easily read the keys long strings of ones and zeros out of the chip’s memory.

“Cool the chips in liquid nitrogen (-196 °C) and they hold their state for hours at least, without any power,” Edward W. Felten, a Princeton computer scientist, wrote in a Web posting. “Just put the chips back into a machine and you can read out their contents.”

The researchers used special pattern-recognition software of their own to identify security keys among the millions or even billions of pieces of data on the memory chip.

“We think this is pretty serious to the extent people are relying on file protection,” Mr. Felten said.

The team, which included five graduate students led by Mr. Felten and three independent technical experts, said they did not know if such an attack capability would compromise government computer information because details of how classified computer data is protected are not publicly available.

Officials at the Department of Homeland Security, which paid for a portion of the research, did not return repeated calls for comment.

The researchers also said they had not explored disk encryption protection systems as now built into some commercial disk drives.

But they said they had proved that so-called Trusted Computing hardware, an industry standard approach that has been heralded as significantly increasing the security of modern personal computers, does not appear to stop the potential attacks.

A number of computer security experts said the research results were an indication that assertions of robust computer security should be regarded with caution.

“This is just another example of how things aren’t quite what they seem when people tell you things are secure,” said Peter Neumann, a security researcher at SRI International in Menlo Park, Calif.

The Princeton researchers wrote that they were able to compromise encrypted information stored using special utilities in the Windows, Macintosh and Linux operating systems.

Apple has had a FileVault disk encryption feature as an option in its OS X operating system since 2003. Microsoft added file encryption last year with BitLocker features in its Windows Vista operating system. The programs both use the federal government’s certified Advanced Encryption System algorithm to scramble data as it is read from and written to a computer hard disk. But both programs leave the keys in computer memory in an unencrypted form.

“The software world tends not to think about these issues,” said Matt Blaze, an associate professor of computer and information science at the University of Pennsylvania. “We tend to make assumptions about the hardware. When we find out that those assumptions are wrong, we’re in trouble.”

Both of the software publishers said they ship their operating systems with the file encryption turned off. It is then up to the customer to turn on the feature.

Executives of Microsoft said BitLocker has a range of protection options that they referred to as “good, better and best.”

Austin Wilson, director of Windows product management security at Microsoft, said the company recommended that BitLocker be used in some cases with additional hardware security. That might include either a special U.S.B. hardware key, or a secure identification card that generates an additional key string.

The Princeton researchers acknowledged that in these advanced modes, BitLocker encrypted data could not be accessed using the vulnerability they discovered.

An Apple spokeswoman said that the security of the FileVault system could also be enhanced by using a secure card to add to the strength of the key.

The researchers said they began exploring the utilities for vulnerabilities last fall after seeing a reference to the persistence of data in memory in a technical paper written by computer scientists at Stanford in 2005.

The Princeton group included Seth D. Schoen of the Electronic Frontier Foundation, William Paul of Wind River Systems and Jacob Appelbaum, an independent computer security researcher.

The issue of protecting information with disk encryption technology became prominent recently in a criminal case involving a Canadian citizen who late in 2006 was stopped by United States customs agents who said they had found child pornography on his computer.

When the agents tried to examine the machine later, they discovered that the data was protected by encryption. The suspect has refused to divulge his password. A federal agent testified in court that the only way to determine the password otherwise would be with a password guessing program, which could take years.

A federal magistrate ruled recently that forcing the suspect to disclose the password would be unconstitutional.