Security chip that does encryption in PCs hacked

February 8 2010, By JORDAN ROBERTSON , AP Technology Writer

In this Tuesday, Feb. 2, 2010 photo, Chris Tarnovsky poses for photos after speaking at the Black Hat Briefings in Arlington, Va. Tarnovsky figured out a way to break chips that carry a "Trusted Platform Module," or TPM, designation. Such chips are billed as the industry's most secure and are estimated to be in as many as 100 million personal computers and servers, according to market research firm IDC. (AP Photo/Jacquelyn Martin)

(AP) -- Deep inside millions of computers is a digital Fort Knox, a special chip with the locks to highly guarded secrets, including classified government reports and confidential business plans. Now a former U.S. Army computer-security specialist has devised a way to break those locks.

The attack can force heavily secured computers to spill documents that likely were presumed to be safe. This discovery shows one way that spies and other richly financed attackers can acquire military and trade secrets, and comes as worries about state-sponsored computer espionage intensify, underscored by recent hacking attacks on Google Inc.

The new attack discovered by Christopher Tarnovsky is difficult to pull off, partly because it requires physical access to a computer. But laptops and smart phones get lost and stolen all the time. And the data that the most dangerous computer criminals would seek likely would be worth the expense of an elaborate espionage operation.

Jeff Moss, founder of the Black Hat security conference and a member of the U.S. Department of Homeland Security's advisory council, called Tarnovsky's finding "amazing."

"It's sort of doing the impossible," Moss said. "This is a lock on Pandora's box. And now that he's pried open the lock, it's like, ooh, where does it lead you?"

Tarnovsky figured out a way to break chips that carry a "Trusted Platform Module," or TPM, designation by essentially spying on them like a phone conversation. Such chips are billed as the industry's most secure and are estimated to be in as many as 100 million personal computers and servers, according to market research firm IDC.

When activated, the chips provide an additional layer of security by encrypting, or scrambling, data to prevent outsiders from viewing information on the machines. An extra password or identification such as a fingerprint is needed when the machine is turned on.

Many computers sold to businesses and consumers have such chips, though users might not turn them on. Users are typically given the choice to turn on a TPM chip when they first use a computer with it. If they ignore the offer, it's easy to forget the feature exists. However, computers needing the most security typically have TPM chips activated.

"You've trusted this chip to hold your secrets, but your secrets aren't that safe," said Tarnovsky, 38, who runs the Flylogic security consultancy in Vista, Calif., and demonstrated his hack last week at the Black Hat security conference in Arlington, Va.

The chip Tarnovsky hacked is a flagship model from Infineon Technologies AG, the top maker of TPM chips. And Tarnovsky says the technique would work on the entire family of Infineon chips based on the same design. That includes non-TPM chips used in satellite TV equipment, Microsoft Corp.'s Xbox 360 game console and smart phones.

That means his attack could be used to pirate satellite TV signals or make Xbox peripherals, such as handheld controllers, without paying Microsoft a licensing fee, Tarnovsky said. Microsoft confirmed its Xbox 360 uses Infineon chips, but would only say that "unauthorized accessories that circumvent security protocols are not certified to meet our safety and compliance standards."

The technique can also be used to tap text messages and e-mail belonging to the user of a lost or stolen phone. Tarnovsky said he can't be sure, however, whether his attack would work on TPM chips made by companies other than Infineon.

Infineon said it knew this type of attack was possible when it was testing its chips. But the company said independent tests determined that the hack would require such a high skill level that there was a limited chance of it affecting many users.

"The risk is manageable, and you are just attacking one computer," said

Joerg Borchert, vice president of Infineon's chip card and security division. "Yes, this can be very valuable. It depends on the information that is stored. But that's not our task to manage. This gives a certain strength, and it's better than an unprotected computer without encryption."

The Trusted Computing Group, which sets standards on TPM chips, called the attack "exceedingly difficult to replicate in a real-world environment." It added that the group has "never claimed that a physical attack - given enough time, specialized equipment, know-how and money - was impossible. No form of security can ever be held to that standard."

It stood by TPM chips as the most cost-effective way to secure a PC.

It's possible for computer users to scramble data in other ways, beyond what the TPM chip does. Tarnovsky's attack would do nothing to unlock those methods. But many computer owners don't bother, figuring the TPM security already protects them.

Tarnovsky needed six months to figure out his attack, which requires skill in modifying the tiny parts of the chip without destroying it.

Using off-the-shelf chemicals, Tarnovsky soaked chips in acid to dissolve their hard outer shells. Then he applied rust remover to help take off layers of mesh wiring, to expose the chips' cores. From there, he had to find the right communication channels to tap into using a very small needle.

The needle allowed him to set up a wiretap and eavesdrop on all the programming instructions as they are sent back and forth between the chip and the computer's memory. Those instructions hold the secrets to the computer's encryption, and he didn't find them encrypted because he was physically inside the chip.

Even once he had done all that, he said he still had to crack the "huge problem" of figuring out how to avoid traps programmed into the chip's software as an extra layer of defense.

"This chip is mean, man - it's like a ticking time bomb if you don't do something right," Tarnovsky said.

Joe Grand, a hardware hacker and president of product- and security-research firm Grand Idea Studio Inc., saw Tarnovsky's presentation and said it represented a huge advancement that chip companies should take seriously, because it shows that presumptions about security ought to be reconsidered.

"His work is the next generation of hardware hacking," Grand said.

©2010 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed.

Citation: Security chip that does encryption in PCs hacked (2010, February 8) retrieved 1 February 2023 from https://phys.org/news/2010-02-chip-encryption-pcs-hacked.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.