

How safe is your swipe?

EurekAlert

[1]

Used in a variety of products from credit cards to satellite televisions, secure chips are designed to keep encoded data safe. But hackers continue to develop methods to crack the chips' security codes and access the information within.

Thinking like hackers, Prof. Avishai Wool and his Ph.D. student Yossi Oren of Tel Aviv University's School of Electrical Engineering have developed an innovative way of extracting information from chip technology. By combining modern cryptology methods with constraint programming -- an area of computer science designed to solve a series of complex equations -- Prof. Wool and Oren were able to extract more information from secure chips. Their research, which could lead to important new advances in computer security, was recently presented at the 12th Workshop on Cryptographic Hardware and Embedded Systems (CHES) in Santa Barbara, CA.

Prof. Wool explains that cryptologists like himself try to stay one step ahead of attackers by thinking the way they do. "Companies need to know how secure their chip is, and how it can be cracked," he explains. "They need to know what they're up against."

Blocking out the "noise"

According to the researchers, the Achilles-heel of contemporary secure chips can be found in the chip's power supply. When a chip is in use, says Prof. Wool, it employs a miniscule amount of power. But the amount of this power, and how it fluctuates, depends on the kind of information the chip contains. By measuring the power fluctuations with an oscilloscope, a standard piece of lab equipment, and analyzing the data using appropriate algorithms, a potential hacker could decipher the information that the chip contains.

But extracting information in this way, through what the researchers call a "side channel," can be complex. When you do a power trace, says Prof. Wool, there is a lot of "noise" -- inaccuracies that result from the different activities the chip is doing at the time. He and Oren have now identified a method for blocking out the "noise" that has proved to be more effective than previous methods.

When applied to information gathered from a power source, a computer program like the one Prof. Wool and Oren have created can sort through this "noise" to deliver a more accurate analysis of a chip's secret contents. Their program is based in "constraint programming" -- the same computer programming approach used for complex scheduling programs like those used in the travel industry.

Knowing your enemy

How safe is your swipe?

Published on Electronic Component News (<http://www.ecnmag.com>)

No chip can be 100% secure, Prof. Wool admits. But he also stresses that it's important to explore the boundaries of how secure information can be extracted from these chips. An attacker could have access to a variety of computer technologies and equipment -- so researchers need to know the type of resources required to break a code, explains Prof. Wool. He has provided information to U.S. passport authorities on how to make the chips in passports more secure.

"We need to think like the attackers," he says, "in order to raise the bar against them."

[SOURCE](#) [2]

Source URL (retrieved on 04/02/2015 - 6:09am):

<http://www.ecnmag.com/news/2010/09/how-safe-your-swipe>

Links:

[1] <http://www.eurekalert.org/multimedia/pub/25778.php?from=169008>

[2] http://www.eurekalert.org/pub_releases/2010-09/afot-hsi092010.php