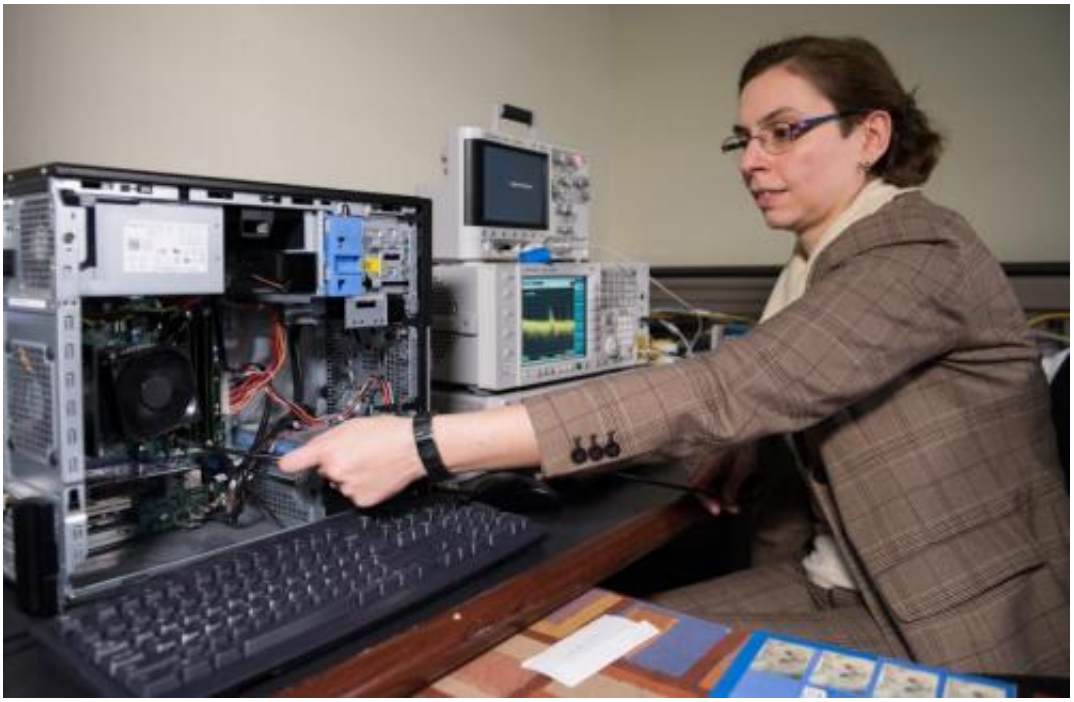
Team works to counter a new class of coffee shop hackers

January 8 2015



Georgia Tech researcher Alenka Zajic measures electromagnetic emissions from various components of a desktop computer. The researchers have studied emissions from desktop and laptop computers, as well as cellphones. Credit: Rob Felt

If you're sitting in a coffee shop, tapping away on your laptop, feeling safe from hackers because you didn't connect to the shop's wifi, think again. The bad guys may be able to see what you're doing just by analyzing the low-power electronic signals your laptop emits even when

it's not connected to the Internet.

And smartphones may be even more vulnerable to such spying.

Researchers at the Georgia Institute of Technology are investigating where these information "leaks" originate so they can help hardware and software designers develop strategies to plug them. By studying emissions from multiple computers, the researchers have developed a metric for measuring the strength of the leaks - known technically as "side-channel signal" - to help prioritize security efforts.

"People are focused on security for the Internet and on the wireless communication side, but we are concerned with what can be learned from your computer without it intentionally sending anything," said Alenka Zajic, an assistant professor in Georgia Tech's School of Electrical and Computer Engineering. "Even if you have the Internet connection disabled, you are still emanating information that somebody could use to attack your computer or smartphone."

Results of the research were presented December 15 at the 47th Annual IEEE/ACM International Symposium on Microarchitecture in Cambridge, U.K. The work is sponsored by the National Science Foundation and the Air Force Office of Scientific Research.

Side-channel emissions can be measured several feet away from an operating computer using a variety of spying methods. Electromagnetic emissions can be received using antennas hidden in a briefcase, for instance. Acoustic emissions - sounds produced by electronic components such as capacitors - can be picked up by microphones hidden beneath tables. Information on power fluctuations, which can help hackers determine what the computer is doing, can be measured by fake battery chargers plugged into power outlets adjacent to a laptop's power converter.

Some signals can be picked up by a simple AM/FM radio, while others require more sophisticated spectrum analyzers. And computer components such as voltage regulators produce emissions that can carry signals produced elsewhere in the laptop.

As a demonstration, Zajic typed a simulated password on one laptop that was not connected to the Internet. On the other side of a wall, a colleague using another disconnected laptop read the password as it was being typed by intercepting side-channel signals produced by the first laptop's keyboard software, which had been modified to make the characters easier to identify.

"There is nothing added in the code to raise suspicion," said Milos Prvulovic, an associate professor in the Georgia Tech School of Computer Science. "It looks like a correct, but not terribly efficient version of normal keyboard driver software. And in several applications, such as normal spell-checking, grammar-checking and display-updating, the existing software is sufficient for a successful attack."

Currently, there is no mention in the open literature of hackers using side-channel attacks, but the researchers believe it's only a matter of time before that happens. The potential risks of side-channel emissions have been reported over the years, but not at the level of detail being studied by the Georgia Tech researchers.

"Of course, it's possible that somebody is using it right now, but they are not sharing that information," Zajic noted.

To counter the threat, the researchers are determining where the leaks originate.

"We are trying to understand why these side channels exist and what can be done to fix these leaks," said Zajic. "We are measuring computers

and smartphones to identify the parts of the devices that leak the most. That information can guide efforts to redesign them, and on an architectural level, perhaps change the instructions in the software to change the device behavior."

Each computer operation has a different potential for leaking information. The processor draws different amounts of current depending on the operation, creating fluctuations that can be measured. Saving data to memory also requires a large amount of current, creating a "loud" operation.

"When you are executing instructions in the processor, you generate a different type of waveform than if you are doing things in memory," explained Zajic. "And there is interaction between the two."

To measure the vulnerability, Zajic, Prvulovic and graduate student Robert Callen developed a metric known as "signal available to attacker" (SAVAT), which is a measure of the strength of the signal emitted. They measured the level of SAVAT for 11 different instructions executed on three different laptops, and found the largest signals when the processors accessed off-chip memory.

"It is not really possible to eliminate all side-channel signal," said Prvulovic. "The trick is to make those signals weak, so potential attackers would have to be closer, use larger antennas and utilize time-consuming signal analyses. We have found that some operations are much 'louder' than others, so quieting them would make it more difficult for attackers."

The researchers are also now studying smartphones, whose compact design and large differential between idle and in-use power may make them more vulnerable. So far, they have only looked at Android devices.

Because the spying is passive and emits no signals itself, users of computers and smartphones wouldn't know they're being watched.

"If somebody is putting strange objects near your computer, you certainly should beware," said Zajic. "But from the user's perspective, there is not much they can do right now. Based on our research, we hope to develop something like virus scan software that will look for vulnerability in the code and tell developers what they should update to reduce this vulnerability."

More information: Robert Callan, Alenka Zajic and Milos Prvulovic, "A Practical Methodology for Measuring the Side-Channel Signal Available to the Attacker for Instruction-Level Events," (47th Annual IEEE/ACM International Symposium on Microarchitecture, 2014).

Provided by Georgia Institute of Technology