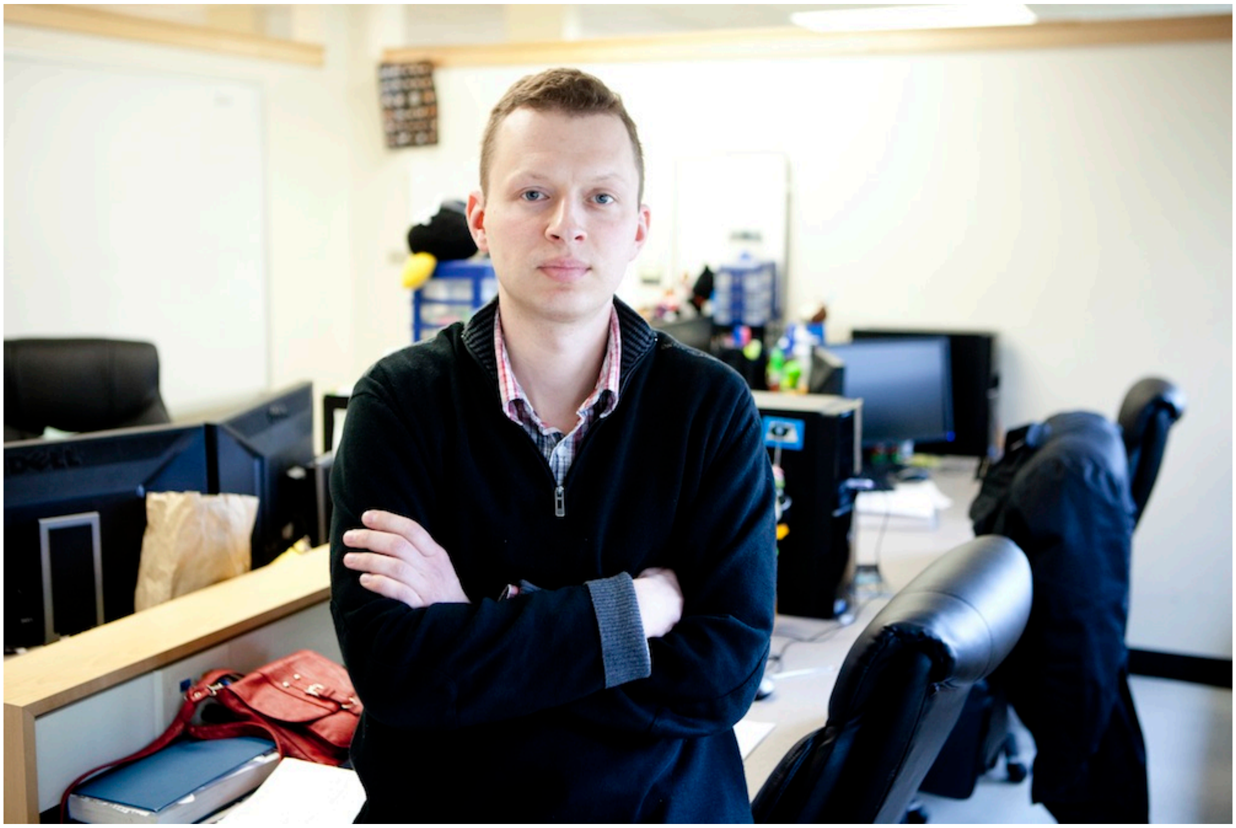
Researchers want to use hardware to fight computer viruses

November 7 2016



Dmitry Ponomarev, professor of computer science at Binghamton University, State University of New York, is the principal investigator of a project titled 'Practical Hardware-Assisted Always-On Malware Detection.' Credit: Jonathan Cohen/Binghamton University

Fighting computer viruses isn't just for software anymore. Binghamton

University researchers will use a grant from the National Science Foundation to study how hardware can help protect computers too.

"The impact will potentially be felt in all computing domains, from mobile to clouds," said Dmitry Ponomarev, professor of computer science at Binghamton University, State University of New York. Ponomarev is the principal investigator of a project titled "Practical Hardware-Assisted Always-On Malware Detection."

More than 317 million pieces of new malware—computer viruses, spyware, and other malicious programs—were created in 2014 alone, according to work done by Internet security teams at Symantec and Verizon. Malware is growing in complexity, with crimes such as digital extortion (a hacker steals files or locks a computer and demands a ransom for decryption keys) becoming large avenues of cyber attack.

"This project holds the promise of significantly impacting an area of critical national need to help secure systems against the expanding threats of malware," said Ponomarev. "[It is] a new approach to improve the effectiveness of malware detection and to allow systems to be protected continuously without requiring the large resource investment needed by software monitors."

Countering threats has traditionally been left solely to software programs , but Binghamton researchers want to modify a computer's central processing unit (CPU) chip—essentially, the machine's brain—by adding logic to check for anomalies while running a program like Microsoft Word. If an anomaly is spotted, the hardware will alert more robust software programs to check out the problem. The hardware won't be right about suspicious activity 100 percent of the time, but since the hardware is acting as a lookout at a post that has never been monitored before, it will improve the overall effectiveness and efficiency of malware detection.

"The modified microprocessor will have the ability to detect malware as programs execute by analyzing the execution statistics over a window of execution," said Ponomarev. "Since the hardware detector is not 100-percent accurate, the alarm will trigger the execution of a heavy-weight software detector to carefully inspect suspicious programs. The software detector will make the final decision. The hardware guides the operation of the software; without the hardware the software will be too slow to work on all programs all the time."

The modified CPU will use low complexity machine learning—the ability to learn without being explicitly programmed—to classify malware from normal programs, which is Yu's primary area of expertise.

"The detector is, essentially, like a canary in a coal mine to warn software programs when there is a problem," said Ponomarev. "The hardware detector is fast, but is less flexible and comprehensive. The hardware detector's role is to find suspicious behavior and better direct the efforts of the software."

Much of the work—including exploration of the trade-offs of design complexity, detection accuracy, performance and power consumption—will be done in collaboration with former Binghamton professor Nael Abu-Ghazaleh, who moved on to the University of California-Riverside in 2014.

Lei Yu, associate professor of computer science at Binghamton University, is a co-principal investigator of the grant.

Grant funding will support graduate students that will work on the project both in Binghamton and California, conference travel and the investigation itself. The three-year grant is for $275,000.

Provided by Binghamton University

Citation: Researchers want to use hardware to fight computer viruses (2016, November 7) retrieved 9 April 2024 from https://phys.org/news/2016-11-hardware-viruses.html