Researchers find weakness in common computer chip

October 25 2016

Dmitry Ponomarev is a professor of computer science at Binghamton's Thomas J. Watson School of Engineering and Applied Science. Credit: Jonathan Cohen/Binghamton University

Researchers from Binghamton University—State University of New

York and the University of California, Riverside have found a weakness in the Haswell central processing unit (CPU) components that makes common computer operating systems vulnerable to malicious attacks.

Computer hackers could take control of individual, company and government computers if a weak point in address space layout randomization (ASLR) software is exploited by manipulating a CPU's branch predictor, a piece of hardware designed to improve program performance.

Before anyone worries too much, researchers suggested several methods to mitigate the attacks they identified in the paper "Jump over ASLR: Attacking the Branch Predictor to Bypass ASLR," and companies have already started to work on the issues raised.

"In the current state of security, attackers have an arsenal of tricks and systems deploy comprehensive protections. ASLR is only a piece of this puzzle, and if the system does not have other vulnerabilities, it is very difficult to attack even if ASLR is broken," said Dmitry Ponomarev, professor of computer science at Binghamton's Thomas J. Watson School of Engineering and Applied Science. "Previous research demonstrated several ways to bypass ASLR, but our attack is just more efficient and direct. It does not change the fundamental state of the security arms race. Individual users should not worry about this attack, but rather make sure that operating systems are always updated to ensure that other exploitable vulnerabilities are not present."

Researchers demonstrated the weakness in commonly-used Linux operating systems using Intel processors. However, the team led by Binghamton PhD candidate Dmitry Evtyushkin, Ponomarev and former Binghamton Computer Science Professor Nael Abu-Ghazaleh think the vulnerability could also apply to other operating systems such as Windows and Android.

According to the work, the attack may also be practical on virtualization systems such as Kernel-based Virtual Machines (KVM), which are used in cloud computing systems.

The results were presented at the 49th Annual IEEE/ACM International Symposium on Microarchitecture (Micro-49) on Oct. 18 in Taipei, Taiwan.

"Ultimately, we found a vulnerability in a normal design feature that makes a new attack possible. It is unreasonable to expect Intel, or any company, to anticipate these kinds of sophisticated attacks while designing chips," Ponomarev said. "Hardware vendors are already doing a lot for security, and we should encourage them to continue to do so."

ASLR software automatically randomizes information in a computer's memory which protects a machine during crashes and defends against a wide range of malware. The team identified a way to disable and bypass ASLR by attacking the branch predictor hardware.

With the ASLR down, a hacker can then perform "buffer overflow" and "code reuse" attacks to gain administrator or "root" level privileges to steal sensitive data. However, another exploitable vulnerability in software is needed to perform a buffer overflow attack.

"While most cybersecurity research considers software vulnerabilities and defenses, our research focuses on the underlying hardware and computer architecture, which also play important roles in computer security, both in terms of introducing new vulnerabilities as well as supporting more secure software," said Abu-Ghazaleh, who is now in the University of California, Riverside's computer science and engineering and electrical and computer engineering departments, in a press release from the school.

Provided by Binghamton University