Researchers describe technique to bypass ASLR schemes

October 21 2016, by Nancy Owano

Credit: Wikipedia

(Tech Xplore)—Technology watching sites were abuzz this week with news about a CPU flaw regarding Intel Haswell powered devices. Researchers participating in the IEEE/ACM International Symposium on Microarchitecture in Taiwan said they developed a bypass for Intel's Address Space Layout Randomization (ASLR) technology on Haswell processors.

On Tuesday, the bypass was discussed at the IEEE/ACM International Symposium on Microarchitecture in Taipei.

The news is all about a side channel in Haswell CPUs which makes possible a bypass from ASLR protection. If left unfixed, said *Ars Technica*'s Dan Goodin, malware attacks could be more potent.

Intel is aware of the situation. *Hot Hardware* on Thursday said Intel was investigating the matter. According to Goodin in *Ars Technica* an Intel spokesman said he was investigating the research paper.

Yes, there is a paper to all this. The three researchers are Dmitry Evtyushkin and Dmitry Ponomarev, both from State University of New York at Binghamton, and Nael Abu-Ghazaleh, University of California, Riverside. Their research paper is "Jump Over ASLR: Attacking Branch Predictors to Bypass ASLR." The paper describes how the bypass was done, weakening defense.

So what did they exactly jump over? And what is ASLR? *Hot Hardware*'s Paul Lilly defined ASLR. He said it is "a built-in defense against a common form of attack that attempts to install malware by exploiting vulnerabilities in an OS or program. When you fire up a program, part of it is loaded into system memory. What ASLR does is randomize the location of various bits of code so that malware can't predict where to find it."

Nael Abu-Ghazaleh, a computer scientist at the University of California at Riverside and one the researchers who developed the bypass, told *Ars Technica*:

"ASLR is an important defense deployed by all commercial Operating Systems. It is often the only line of defense that prevents an attacker from exploiting any of a wide range of attacks (those that rely on knowing the memory layout of the victim)."

The researchers, in exploiting a flaw in the branch predictor part of a Haswell CPU, could load a small application that identifies the memory addresses where specific parts of code are loaded.

The researchers noted in their paper that ASLR was a widely adopted security mechanism, in kernel and application levels. It is intended to protect systems from code reuse attacks. The authors' side channels, though, allowed the recovery of the memory layout of both the kernel and user-level applications.

"We demonstrated a successful attack on a system with Haswell CPU and a recent version of Linux kernel," they said. They also described possible software and hardware countermeasures to mitigate this.

Haswell is the codename for the processor microarchitecture; it is the successor to Ivy Bridge microarchitecture.