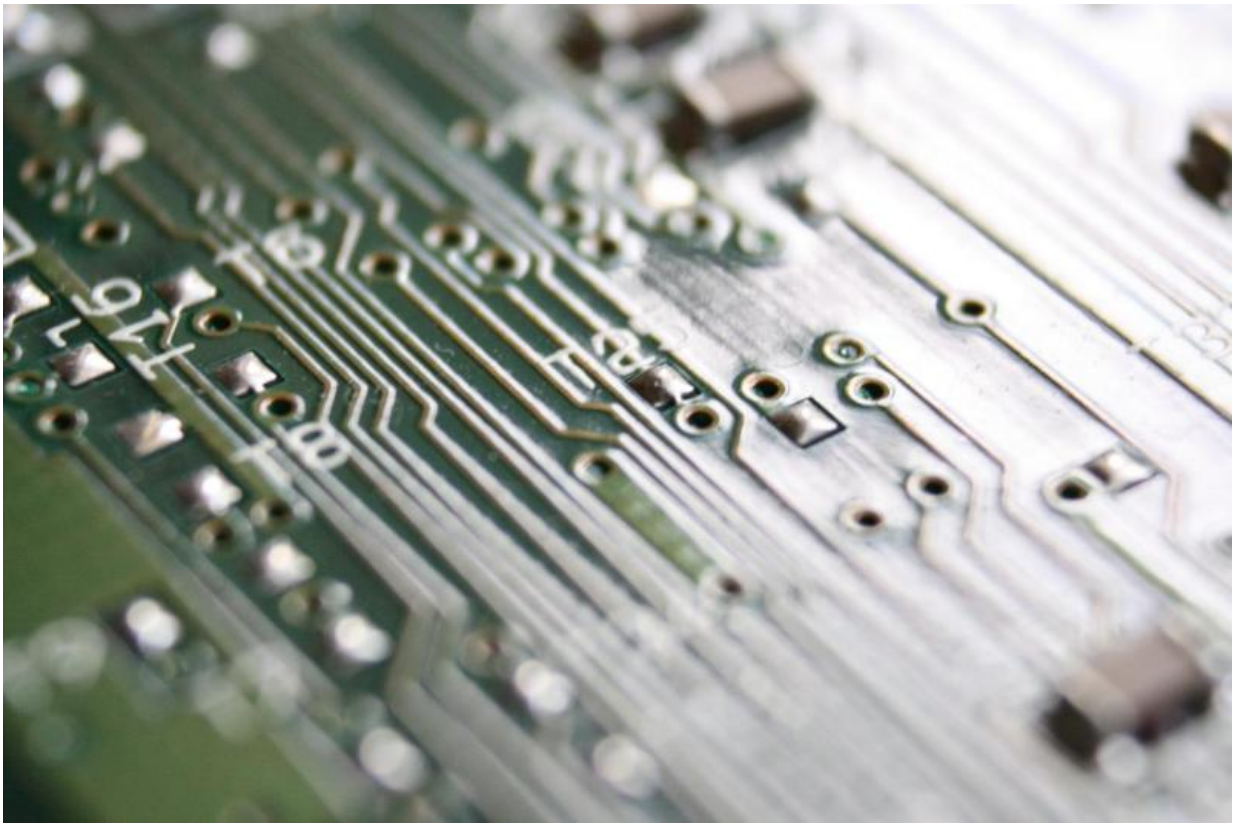
New chip stops attacks before they start

May 2 2019



Credit: Public Domain

A new computer processor architecture developed at the University of Michigan could usher in a future where computers proactively defend against threats, rendering the current electronic security model of bugs and patches obsolete.

Called MORPHEUS, the chip blocks potential attacks by encrypting and randomly reshuffling key bits of its own code and data 20 times per second—infinitely faster than a human hacker can work and thousands of times faster than even the fastest electronic hacking techniques.

"Today's approach of eliminating security bugs one by one is a losing game," said Todd Austin, U-M professor of computer science and engineering and a developer of the system. "People are constantly writing code, and as long as there is new code, there will be new bugs and security vulnerabilities.

"With MORPHEUS, even if a hacker finds a bug, the information needed to exploit it vanishes 50 milliseconds later. It's perhaps the closest thing to a future-proof secure system."

Austin and his colleagues have demonstrated a DARPA-funded prototype processor that successfully defended against every known variant of control-flow attack, one of hackers' most dangerous and widely used techniques.

The technology could be used in a variety of applications, from laptops and PCs to Internet of Things devices, where simple and reliable security will be increasingly critical.

"We've all seen how damaging an attack can be when it hits a computer that's sitting on your desk," he said. "But attacks on the computer in your car, in your smart lock or even in your body could place users at even greater risk."

Austin said that instead of using software to patch known code vulnerabilities, MORPHEUS bakes security into its hardware. It makes vulnerabilities virtually impossible to pin down and exploit by constantly randomizing critical program assets in a process called "churn."

"Imagine trying to solve a Rubik's Cube that rearranges itself every time you blink," Austin said. "That's what hackers are up against with MORPHEUS. It makes the computer an unsolvable puzzle."

Yet MORPHEUS is transparent to software developers and end users. This is because it focuses on randomizing bits of data known as "undefined semantics." Undefined semantics are nooks and crannies of the computing architecture—for example the location, format and content of program code is an undefined semantic.

Undefined semantics are part of a processor's most basic machinery, and legitimate programmers don't generally interact with them. But hackers can reverse-engineer them to uncover vulnerabilities and launch an attack.

The chip's churn rate can be adjusted up or down to strike the right balance between maximizing security and minimizing resource consumption. Austin said a churn rate of once every 50 milliseconds was chosen for the demonstration processor because it's several thousand times faster than even the fastest electronic hacking techniques, but only slows performance by about 1%. The architecture also includes an attack detector that looks for pending threats and increases the churn rate if it senses that an attack is imminent.

Austin and colleagues presented the chip and research paper last month at the ACM International Conference on Architectural Support for Programming Languages and Operating Systems.

The demonstration chip is a RISC-V processor—a common, open-source chip design often used for research. Austin is working to commercialize the technology through Agita Labs, a startup company founded by Austin and U-M computer science and engineering professor Valeria Bertacco, also an author on the paper.

More information: "Morpheus: A Vulnerability-Tolerant Secure Architecture Based on Ensembles of Moving Target Defenses with Churn
," dl.acm.org/citation.cfm?doid=3297858.3304037

Provided by University of Michigan