Shape-shifting computer chip thwarts an army of hackers

May 25 2021, by Todd Austin and Lauren Biernacki

The Morpheus secure processor works like a puzzle that keeps changing before hackers have a chance to solve it. Credit: Alan de la Cruz via Unsplash

We have developed and tested a secure new computer processor that thwarts hackers by randomly changing its underlying structure, thus making it virtually impossible to hack.

Last summer, 525 security researchers spent three months trying to hack our Morpheus processor as well as others. All attempts against Morpheus failed. This study was part of a program sponsored by the U.S. Defense Advanced Research Program Agency to design a secure processor that could protect vulnerable software. DARPA released the results on the program to the public for the first time in January 2021.

A processor is the piece of computer hardware that runs software programs. Since a processor underlies all software systems, a secure processor has the potential to protect any software running on it from attack. Our team at the University of Michigan first developed Morpheus, a secure processor that thwarts attacks by turning the computer into a puzzle, in 2019.

A processor has an architecture—x86 for most laptops and ARM for most phones—which is the set of instructions software needs to run on the processor. Processors also have a microarchitecture, or the "guts" that enable the execution of the instruction set, the speed of this execution and how much power it consumes.

Hackers need to be intimately familiar with the details of the microarchitecture to graft their malicious code, or malware, onto vulnerable systems. To stop attacks, Morpheus randomizes these implementation details to turn the system into a puzzle that hackers must solve before conducting security exploits. From one Morpheus machine to another, details like the commands the processor executes or the format of program data change in random ways. Because this happens at the microarchitecture level, software running on the processor is unaffected.

A skilled hacker could reverse-engineer a Morpheus machine in as little as a few hours, if given the chance. To counter this, Morpheus also changes the microarchitecture every few hundred milliseconds. Thus, not only do attackers have to reverse-engineer the microachitecture, but they have to do it very fast. With Morpheus, a hacker is confronted with a computer that has never been seen before and will never be seen again.

The Morpheus computer processor, inside the square beneath the fan on this circuit board, rapidly and continuously changes its underlying structure to thwart hackers. Credit: Todd Austin, CC BY-ND

To conduct a security exploit, hackers use vulnerabilities in software to get inside a device. Once inside, they graft their malware onto the device. Malware is designed to infect the host device to steal sensitive data or spy on users.

The typical approach to computer security is to fix individual software vulnerabilities to keep hackers out. For these patch-based techniques to succeed, programmers must write perfect software without any bugs. But ask any programmer, and the idea of creating a perfect program is laughable. Bugs are everywhere, and security bugs are the most difficult to find because they don't impair a program's normal operation.

Morpheus takes a distinct approach to security by augmenting the underlying processor to prevent attackers from grafting malware onto the device. With this approach, Morpheus protects any vulnerable software that runs on it.

For the longest time, processor designers considered security a problem for software programmers, since programmers made the software bugs that lead to security concerns. But recently computer designers have discovered that hardware can help protect software.

Academic efforts, such as Capability Hardware Enhanced RISC Instructions at the University of Cambridge, have demonstrated strong protection against memory bugs. Commercial efforts have begun as well, such as Intel's soon-to-be-released Control-flow Enforcement Technology.

Morpheus takes a notably different approach of ignoring the bugs and instead randomizes its internal implementation to thwart exploitation of bugs. Fortunately, these are complementary techniques, and combining them will likely make systems even more difficult to attack.

We are looking at how the fundamental design aspects of Morpheus can be applied to protect sensitive data on people's devices and in the cloud. In addition to randomizing the implementation details of a system, how can we randomize data in a way that maintains privacy while not being a burden to software programmers?

More information: Mark Gallagher et al, Morpheus, *Proceedings of the Twenty-Fourth International Conference on Architectural Support for Programming Languages and Operating Systems* (2019). DOI: 10.1145/3297858.3304037

This story is part of Science X Dialog*, where researchers can report findings from their published research articles.* Visit this page *for information about ScienceX Dialog and how to participate.*

Provided by The Conversation

Citation: Shape-shifting computer chip thwarts an army of hackers (2021, May 25) retrieved 27 April 2024 from https://sciencex.com/news/2021-05-shape-shifting-chip-thwarts-army-ofhackers.html