# Unhackable computer under development with DARPA grant

December 21 2017, by Nicole Casal Moore

By turning computer circuits into unsolvable puzzles, a University of Michigan team aims to create an unhackable computer with a new $3.6 million grant from the Defense Advanced Research Projects Agency.

Todd Austin, U-M professor of computer science and engineering, leads the project, called MORPHEUS. Its cybersecurity approach is dramatically different from today's, which relies on software—specifically software patches to vulnerabilities that have already been identified. It's been called the "patch and pray" model, and it's not ideal.

This spring, DARPA announced a $50 million program in search of cybersecurity solutions that would be baked into hardware.

"Instead of relying on software Band-Aids to hardware-based security issues, we are aiming to remove those hardware vulnerabilities in ways that will disarm a large proportion of today's software attacks," said Linton Salmon, manager of DARPA's System Security Integrated Through Hardware and Firmware program.

The U-M grant is one of nine that DARPA has recently funded through SSITH.

MORPHEUS outlines a new way to design hardware so that information is rapidly and randomly moved and destroyed. The technology works to elude attackers from the critical information they need to construct a

successful attack. It could protect both hardware and software.

"We are making the computer an unsolvable puzzle," Austin said. "It's like if you're solving a Rubik's Cube and every time you blink, I rearrange it."

In this way, MORPHEUS could protect against future threats that have yet to be identified, a dreaded vulnerability that the security industry called a "zero day exploit."

"What's incredibly exciting about the project is that it will fix tomorrow's vulnerabilities," Austin said. "I've never known any security system that could be future proof."

Austin said his approach could have protected against the Heartbleed bug discovered in 2014. Heartbleed allowed attackers to read the passwords and other critical information on machines.

"Typically, the location of this data never changes, so once attackers solve the puzzle of where the bug is and where to find the data, it's 'game over,'" Austin said.

Under MORPHEUS, the location of the bug would constantly change and the location of the passwords would change, he said. And even if an attacker were quick enough to locate the data, secondary defenses in the form of encryption and domain enforcement would throw up additional roadblocks. The bug would still be there, but it wouldn't matter. The attacker won't have the time or the resources to exploit it.

"These protections don't exist today because they are too expensive to implement in software, but with DARPA's support we can take the offensive against attackers with new defenses in hardware and implement then with virtually no impact to software," Austin said.

More than 40 percent of the "software doors" that hackers have available to them today would be closed if researchers could eliminate seven classes of hardware weaknesses, according to DARPA. The hardware weakness classes have been identified by a crowd-source listing of security vulnerabilities called the Common Weakness Enumeration. The classes are: permissions and privileges, buffer errors, resource management, information leakage, numeric errors, crypto errors, and code injection.

DARPA is aiming to render these attacks impossible within five years. If developed, MORPHEUS could do it now, Austin said.

While the complexity required might sound expensive, Austin said he's confident his team can make it possible at low cost.

Also on the project team are: Valeria Bertacco, an Arthur F. Thurnau Professor and professor of computer science and engineering at U-M; Mohit Tiwari, an assistant professor of electrical and computer engineering at the University of Texas; and Sharad Malik, the George Van Ness Lothrop Professor of Engineering and a professor of electrical engineering at Princeton University.

Provided by University of Michigan