

February 1, 2023



Intel and UC San Diego Join DARPA Program to Prevent Exploitation of Computing Systems

Intel and the University of California, San Diego have been selected for the DARPA Hardening Development Toolchains Against Emergent Execution Engines program.

SANTA CLARA, Calif.--(BUSINESS WIRE)-- **What's New:** Intel and the University of California, San Diego (UC San Diego) announced today that they have been selected to join the [Hardening Development Toolchains Against Emergent Execution Engines](#) (HARDEN) program team for the Defense Advanced Research Projects Agency (DARPA). Adversaries have crafted increasingly complex cyberattacks in reaction to decades of platform hardening efforts and increasing IT security measures that reduce vulnerabilities. Attempts to mitigate these threats have fallen short, creating an increased risk of intrusion into current and legacy code.

"The growing complexity of computer systems leads to more avenues for executing exploits. Through the DARPA HARDEN program, we will deepen research with UC San Diego to achieve a practical method to harden legacy and future systems against cyberattacks across the government computing landscape and beyond."

– Michael LeMay, Intel Labs senior staff research scientist and Intel's principal investigator for the DARPA HARDEN program

How It Works: To address threats of cyberattack, DARPA selected several teams to work on solutions to mitigate and prevent vulnerabilities in integrated computing systems. The four-year joint effort will focus on creating tools rooted in cryptography and formal security theories. As part of this effort, DARPA will utilize Intel's [Cryptographic Capability Computing \(C3\)](#) system, the first stateless memory safety mechanism that effectively replaces inefficient metadata with efficient cryptography.

At UC San Diego, the effort will be led by professors Deian Stefan and Dean Tullsen from the Department of Computer Science and Engineering.

Why It Matters: Since at least the mid-1960s, computer scientists have sought "capability-based access control" for its thorough security. Capabilities enlighten processors to fine-grained divisions between data objects in memory, which enables addressing memory safety issues that have persistently accounted for most software vulnerabilities across the industry. These can provide an entry point for adversaries to launch "emergent execution" attacks, which manipulate complex interacting system behaviors (sometimes called "weird machine" behaviors) to compromise data and system operation.

HARDEN will help create practical tools to prevent the exploitation of integrated computing systems by disrupting the patterns of robust, reliable exploits used by attackers and

depriving the attackers of emergent execution engines.

The Details: Intel has a long history of developing capability-based access control mechanisms, such as in the iAPX 432 and i960MX processors from the 1980s. The C3 system published at the MICRO 2021 conference overcomes substantial limitations of prior capability-based access control mechanisms, like their heavy reliance on metadata (data about data) that is expensive to store and process, and their incompatibility with legacy code. C3 effectively replaces inefficient metadata with efficient cryptography by encrypting individual pointers and data objects in a way that can be widely deployed, even to legacy x86 software.

The HARDEN program will enable Intel and UC San Diego to further investigate and demonstrate C3's potential to improve security for legacy and future systems on DARPA-hard challenge programs. This will further the goal of understanding how attackers turn parts of modern computing systems against the whole, so this can be prevented in the future.

What's Next: The HARDEN program will run for 48 months and is organized into three phases: Phases 1 and 2 will each be 18 months, followed by a 12-month Phase 3. Intel is proud to be a part of this pioneering work with UC San Diego and DARPA, helping keep the U.S. government's systems secure.

About Intel

Intel (Nasdaq: INTC) is an industry leader, creating world-changing technology that enables global progress and enriches lives. Inspired by Moore's Law, we continuously work to advance the design and manufacturing of semiconductors to help address our customers' greatest challenges. By embedding intelligence in the cloud, network, edge and every kind of computing device, we unleash the potential of data to transform business and society for the better. To learn more about Intel's innovations, go to newsroom.intel.com and intel.com.

© Intel Corporation. Intel, the Intel logo and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as the property of others.

View source version on businesswire.com:

<https://www.businesswire.com/news/home/20230201005315/en/>

Laura Stadler

1-619-346-1170

laura.stadler@intel.com

Source: Intel Corporation