DEFENSE SYSTEMS

CONNECTED WARRIOR
AI & ANALYTICS
CLOUD
CYBER
IT INFRASTRUCTURE
UNMANNED SYSTEMS
RESOURCES
NEWSLETTER
EVENTS
ADVERTISE

CYBERSECURITY

G+ Share Share Tweet

Stronger security via a different chip?

BY ERIC TEGLER • DEC 18, 2017

As the military and government fervently push to aggregate and organize systems and data in ever more centralized ways, one corner of the cybersecurity community is taking a contrary approach to defending information and architecture -- by securing distributed hardware.

Cambridge, Mass.-based Draper, a non-profit engineering and research firm that specializes in embedded systems security, has developed a chip known as the Inherently Secure Processor (ISP).

It's an alternative to the software-centric approach to cybersecurity, which emphasizes defense against specific exploits. Instead, the ISP is designed to protect against classes of attacks. A wide variety of attacks now cross cyber boundaries guarded by software, disrupting or altering the functionality of interconnected physical systems and devices. Avionics are a good example. In 2016, the Air Force identified avionics in 50 weapons

Defense Systems Update

Sign up for our newsletter.

Email Address

Select primary job function/rank
Click to Select One

Select military branch/agency/business type
Click to Select One

I agree to this site's Privacy Policy.

SUBMIT

Featured Articles

- Stronger security via a different chip?
- Army awards contract for Virtual Patient Simulator System
- After exposing DISA data to Russia, contractor agrees to new

systems -- from satellites to the F-35 -- with cyber-vulnerabilities.

“We have DOD clients that have very hard requirements and it’s very difficult for them to meet those with software,” said Draper Cyber Technologies Program Manager Chris Lockett. “Adding software to secure a system, adds complexity and often makes the problem worse.”

“The current CPU architecture hasn’t changed since 1947,” he added. “A processor processes data and instructions as fast as it can. What we’re doing is applying policies to the data instructions in-line to the CPU processing with a minimal performance hit.”

The ISP integrates with commercial processors and enables the hardware to identify and block bad data and instructions (how hackers compromise systems) and remediate the attack at cyber-relevant speeds. It is not simply a gatekeeper, cordoning off processing or memory from unwanted instructions. Rather than shut down or significantly limit a device/system, it works to maintain functionality and resiliency.

“How you handle what you detect is as important as the fact that you can detect it,” Lockett affirmed.

Draper is initially targeting the ISP at embedded devices. In addition to DOD applications, the company sees the ISP as highly relevant to the power grid. The technology and philosophy emerged from DARPA’s 2010 Clean-Slate Re-design of Adaptive, Secure Hosts (CRASH) program, as well as previous NSA and chip maker efforts seeking to diminish the vulnerability of systems for which cybersecurity was not a design-phase consideration.

The ISP’s memory protection, control flow integrity, data providence and re-write/execute polices address over 95 percent of cyber vulnerabilities, according to Draper. The ISP policies can either be fixed or updated by isolated, protected firmware separated from the host processor. Clients may forgo updating the chip in the interest of even greater security.

security controls

- Lessons learned from training Army combat units in cyber ops
- GAO: Security clearance problems far from fixed

Most Popular Articles

- Beam-switching tech successfully tested on Predator drone
- DARPA seeks 'smart plants' to protect soldiers
- Marines seek new enterprise mobility management solution
- DOD should rethink its approach to IoT
- Trump taps former NASA administrator to head DOD tech research

“A lot of the current cybersecurity solutions effectively add holes and vulnerabilities,” Lockett observed. “Teams here at Draper use [add-on] hardened software to actually break into systems.”

Lockett’s sentiment was echoed by Rodney Joffe, senior fellow at IT authentication/security firm Neustar. “No matter what you do in software, it doesn’t matter if the hardware is not already secured," he said. "With software, you’re actually expanding the attack surface. What Draper is doing is a no-brainer. They’re building on the right thing. It absolutely has to be done.”

Joffe added that a hardware-centric security emphasis has been followed by the Chinese in particular, underlining its criticality. Draper is addressing the commercial security side as well, spinning out a new firm called Dover Microsystems to market the ISP to chip makers.

A holistic approach to cybersecurity that begins with securing hardware is rapidly gaining acceptance within government, Lockett affirmed. “We have government agencies who say ‘Thank goodness. We’ve spent money on very good security software. The ISP will help protect the networking software that’s running on our embedded devices.”

In tackling security at the CPU, Draper’s ISP offers a chance to decentralize risk and bake protection in from the start, an approach the cybersecurity community will surely hear more about.

About the Author

Eric Tegler is a freelance writer specializing in technology and defense issues.

8251 Greensboro Drive, Suite 510, McLean, VA 22102 703-876-5100