ADVERTISEMENT

ELECTION SECURITY

DARPA Is Building a $10 Million, Open Source, Secure Voting System

The system will be fully open source and designed with newly developed secure hardware to make the system not only impervious to certain kinds of hacking, but also allow voters to verify that their votes were recorded accurately.

By Kim Zetter | Mar 14 2019, 9:02am

Image: Shutterstock

SHARE TWEET

For years security professionals and election integrity activists have been pushing voting machine vendors to build more secure and verifiable election systems, so voters and

Now they might finally get this thanks to a new $10 million contract the Defense Department's Defense Advanced Research Projects Agency (DARPA) has launched to design and build a secure voting system that it hopes will be impervious to hacking.

ADVERTISEMENT

The first-of-its-kind system will be designed by an Oregon-based firm called Galois, a longtime government contractor with experience in designing secure and verifiable systems. The system will use fully open source voting software, instead of the closed, proprietary software currently used in the vast majority of voting machines, which no one outside of voting machine testing labs can examine. More importantly, it will be built on secure open source hardware, made from special secure designs and techniques developed over the last year as part of a special program at DARPA. The voting system will also be designed to create fully verifiable and transparent results so that voters don't have to blindly trust that the machines and election officials delivered correct results.

But DARPA and Galois won't be asking people to blindly trust that their voting systems are secure—as voting machine vendors currently do. Instead they'll be publishing source code for the software online and bring prototypes of the systems to the Def Con Voting Village this summer and next, so that hackers and researchers will be able to freely examine the systems themselves and conduct penetration tests to gauge their security. They'll also be working with a number of university teams over the next year to have them examine the systems in formal test environments.

"Def Con is great, but [hackers there] will not give us as much technical details as we want [about problems they find in the systems]," Linton Salmon, program manager in DARPA's Microsystems Technology Office who is overseeing the project, said in a phone call. "Universities will give us more information. But we won't have as many people or as high visibility when we do it with universities."

ADVERTISEMENT

The systems Galois designs won't be available for sale. But the prototypes it creates will be available for existing voting machine vendors or others to freely adopt and customize without costly licensing fees or the millions of dollars it would take to research and develop a secure system from scratch.

"We will not have a voting system that we can deploy. That's not what we do," said Salmon. "We will show a methodology that could be used by others to build a voting system that is completely secure."

Joe Kiniry is the principal scientist at Galois who is leading the project at his company. Kiniry has been involved in efforts to secure elections for years as part of a separate company he runs called Free & Fair. He's consulted with foreign governments about their election systems, and his company has been working with states in the US to design robust post-election audits. But the idea to create a secure voting system didn't come from Kiniry; it came from DARPA.

"DARPA was searching for a sexy demonstration for the [secure hardware] program. What could you put on secure hardware that people would care about and understand?" Kiniry said.

They needed a project that would be unclassified so DARPA could talk about it publicly.

"We wanted something where there could be a lot of people who could look at this in an open way and critique it and find problems," said Salmon.

election security and integrity.

“If we were to build a fake radar system, it could demonstrate secure hardware, but it wouldn’t be useful to anybody. [DARPA] love the fact that we’re building a demonstrator that might actually be useful to the world,” Kiniry said.

Kiniy said Galois will design two basic voting machine types. The first will be a ballot-marking device that uses a touch-screen for voters to make their selections. That system won’t tabulate votes. Instead it will print out a paper ballot marked with the voter’s choices, so voters can review them before depositing them into an optical-scan machine that tabulates the votes. Galois will bring this system to Def Con this year.

Many current ballot-marking systems on the market today have been criticized by security professionals because they print bar codes on the ballot that the scanner can read instead of the human-readable portion voters review. Someone could subvert the bar code to say one thing, while the human-readable portion says something else. Kiniry said they’re aiming to design their system without barcodes.

The optical-scan system will print a receipt with a cryptographic representation of the voter’s choices. After the election, the cryptographic values for all ballots will be published on a web site, where voters can verify that their ballot and votes are among them.

“That receipt does not permit you to prove anything about how you voted, but does permit you to prove that the system accurately captured your intent and your vote is in the final tally,” Kiniry said.

ADVERTISEMENT

Members of the public will also be able to use the cryptographic values to independently tally the votes to verify the election results so that tabulating the votes isn't a closed process solely in the hands of election officials.

“Any organization [interested in verifying the election results] that hires a moderately smart software engineer [can] write their own tabulator,” Kiniry said. “We fully expect that Common Cause, League of Women Voters and the [political parties] will all have their own tabulators and verifiers.”

The second system Galois plans to build is an optical-scan system that reads paper ballots marked by voters by hand. They’ll bring that system to Def Con next year.

*

The voting system project grew out of a larger DARPA program focused on developing secure hardware. That program, called System Security Integrated Through Hardware and Firmware or SSITH, was launched in 2017 and is aimed at developing secure hardware, and design tools to build that hardware, so that hardware would be impervious to most of the software attacks prevalent today.

Currently most security is focused on software protections for operating systems, browsers, and other programs.

> “This is only the beginning. This is a problem that is so big that one DARPA program isn’t going to solve even 20 percent of the problem.”

already, he said, "but they don't go far enough and … require too much power and performance….We want to fix this in hardware, and then no matter what [vulnerabilities] you have in software, [attackers] would not be able to [exploit] them."

ADVERTISEMENT

The basic problem, he said, is that most hardware is gullible and has no way of distinguishing between acceptable and unacceptable behavior. If an attacker's exploit tells the machine to do something malicious, the hardware complies without making judgments about whether it should do this.

"I'm trying to change that and make hardware part of the solution to security rather than a bystander," said Salmon. "This is only the beginning. This is a problem that is so big that one DARPA program isn't going to solve even 20 percent of the problem."

In a voting system, this means the hardware would prevent, for example, someone entering a voting booth and slipping a malicious memory card into the system and tricking the system into recording 20 votes for one vote cast, as researchers have shown could be done with some voting systems.

"Our goal is to make this so that the hardware is blocked against all of these various types of attack from the external world. If this is successful, and if the software put on top is equally successful, then it means people can't hack in and … alter votes. It would also mean that the person who votes would get some verification that they did vote and all of that would be done in a manner that hackers couldn't change," Salmon said.

Galois, which is part of the SSITH project, plans to build its voting system on top of the secure hardware designed by these teams, and will create a prototype for each CPU design.

ADVERTISEMENT

Ad

“It’s normal, open source voting system software, which just happens to be running on top of those secure CPUs,” said Kiniry. “Our contention is… that a normal voting system running on COTS [commercial off-the-shelf hardware] will be hacked. A normal voting system running on the secure hardware will probably not be hacked.”

Not only are teams developing secure CPUs but to best take advantage of what a secure CPU offers, they’re developing new versions of open source C-compilers so they can recompile the entire software stack on a system—the operating system, the kernel, all the libraries and all the user software that’s written in C.

“So it really is a powerful software play and hardware play,” Kiniry said.

The program isn’t about re-architecting new CPUs, but proving that existing hardware can be modified to be made secure, thereby avoiding the need to re-design hardware from scratch.

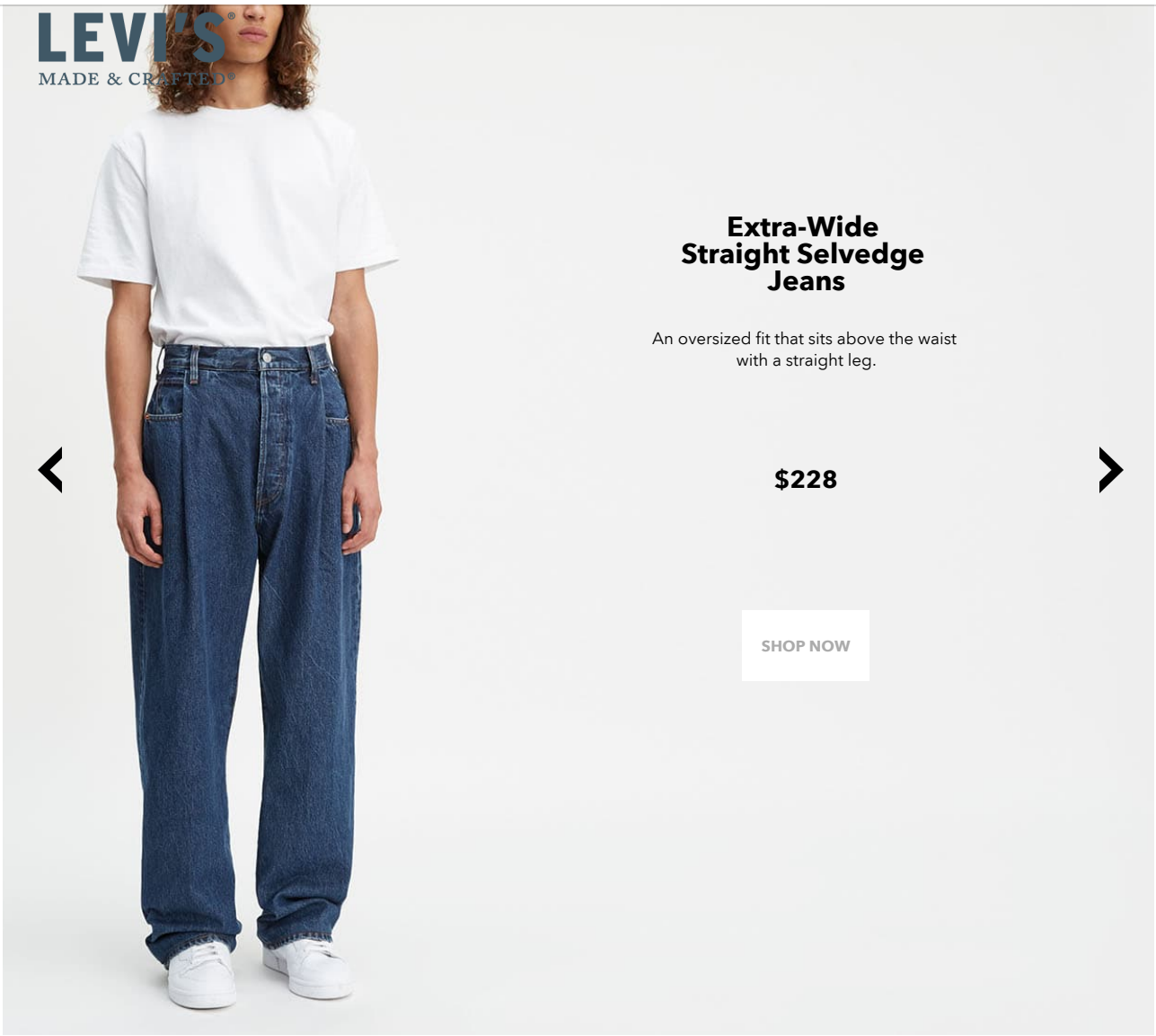
> “Galois and DARPA have just stepped up and filled a vacuum of leadership at the federal level to address the well-documented

But even so, the secure designs are expected to change how new CPUs are architected going forward.

Joe Fitzpatrick, a noted hardware security expert who trains professionals on hardware hacking and security, calls the DARPA secure hardware project a lofty goal that will be great if it succeeds.

“I can’t tell if they truly are architecting a new CPU that is truly resistant to all these [attacks]. But if they designed a new CPU that was able to understand and determine malicious or correct operations from the software, that’s not trivial. That would be pretty amazing,” said Fitzpatrick.

ADVERTISEMENT



Peiter “Mudge” Zatko, a former program manager at DARPA and noted security professional who has testified to Congress on security issues, said this and other DARPA

“We should [also] work towards building processors that have more security principles inherent in them,” he told Motherboard.

Susan Greenhalgh, policy director for the for the National Election Defense Coalition, an election integrity group, hopes the systems Galois and DARPA are building will finally change the status quo of insecure voting.

“The [current systems are] woefully equipped and too prosaic to drive the quantum changes needed to face the nation-state actors that are threatening our democracy,” she told Motherboard. “Galois and DARPA have just stepped up and filled a vacuum of leadership at the federal level to address the well-documented vulnerabilities in US voting machines that constitute a national security crisis.”

M

SHARE TWEET

TAGGED: DARPA, VOTING

Watch This Next