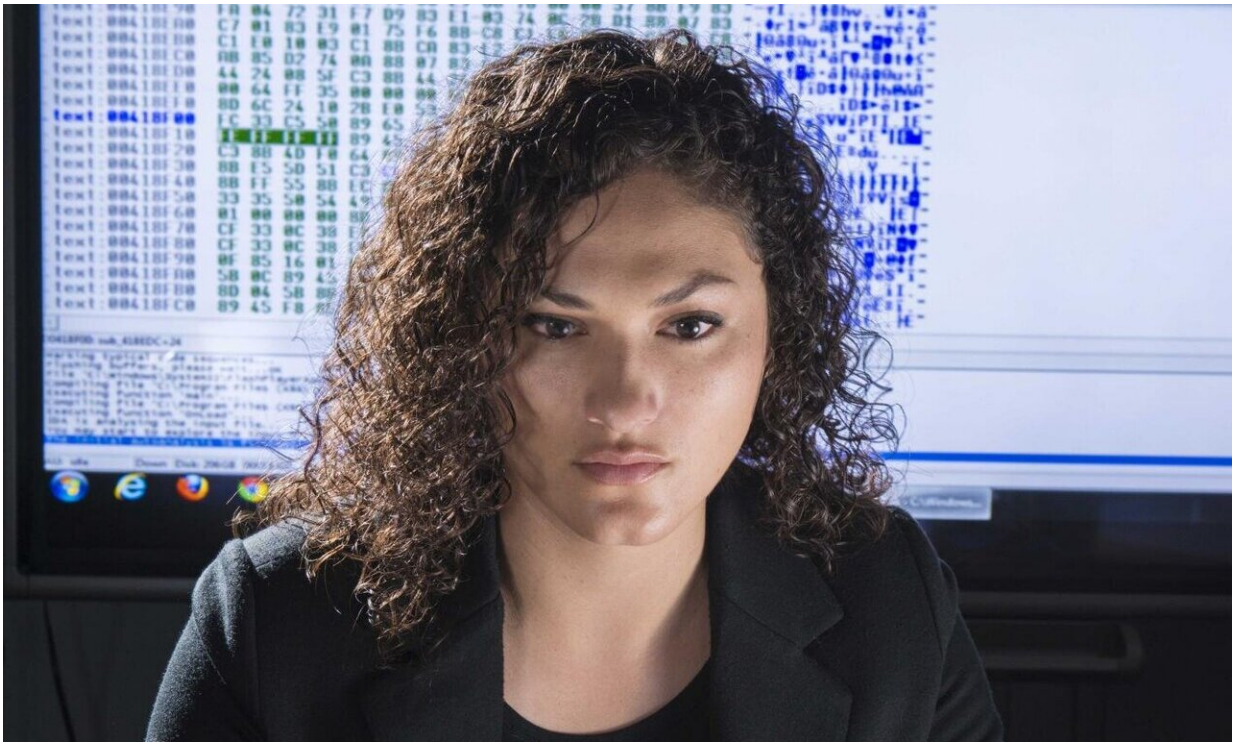
Expanding access to cyber research tools

June 26 2020



Cyber researcher Armida Carbajal tracks cyberthreats at Sandia National Laboratories, which has created free cyber research tools for academic and research institutions. Credit: Sandia National Laboratories

Faculty and students at Purdue University now have access to cybersecurity research software developed at Sandia National Laboratories. This marks the first time Sandia has collaborated with an academic community to make its cyber software widely available.

Sandia has previously invited academic collaborators to use cyber research software at the labs or by connecting to its systems remotely. This is the first academic partnership in which Sandia has made the software available throughout an institution for teaching or research regardless of affiliation with the labs.

The software, called minimega, will help advance cybersecurity research to discover security threats in a variety of systems and develop new safeguards. It also will increase research opportunities at the Center for Education and Research in Information Assurance and Security, based at the university in West Lafayette, Indiana. It was installed on a server that supports the center's new Scalable Open Laboratory for Cyber Experimentation, or SOL4CE, which was unveiled in February.

"Minimega is an open-source emulation platform that allows users to set up a simulated, virtual network to safely explore and reason about computer networks and distributed systems. This could include looking at cybersecurity, resilience, what-if scenarios and red-teaming assessments. Resources like this are relatively few and far between," said Sandia computer scientist Vince Urias. A red team identifies vulnerabilities for the purpose of fixing them.

A virtual testing ground like minimega is an important early step in research because it can quickly generate data on variations of experimental security protocols or simulate enterprises that are difficult to reproduce in the real world, especially large or specialized systems. Researchers use the simulated data to home in on approaches that show the most promise for use in the real world and to identify unintended effects on a system.

The program is part of Sandia's suite of cybertools, called Emulytics—a portmanteau of emulation and analytics.

Expanding the program

"We hope more universities will follow," said Han Lin, who oversees Sandia's cyber educational outreach programs. "Cyberthreats are always changing, so it's important that researchers have easy access to tools to test new countermeasures."

"This is just a first step—we have plans in the works to release more of our Emulytics software stack to the experimental cyber research community, working closely with our academic partners" said Zach Benz, who formerly managed Sandia's Emulytics development.

In addition to installing the software, Sandia staff developed training and "hosted outreach and support for installation and configuration, as well as led workshops with faculty to help them get up and running," Urias said.

"We want to ensure universities have tools to quantify how good a system is—actual metrics that tell you a system is safe, rather than thinking it's safe," said Kamlesh "Ken" Patel, manager of Purdue partnerships at Sandia.

Sandia National Laboratories is a multimission laboratory operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration. Sandia Labs has major research and development responsibilities in nuclear deterrence, global security, defense, energy technologies and economic competitiveness, with main facilities in Albuquerque, New Mexico, and Livermore, California.

Provided by Sandia National Laboratories