Sandia cyber-testing contributes to DHS Transition to Practice

September 10 2014

Sandia National Laboratories' Daniel Soh, right, offers an overview of the continuous variable quantum key distribution lab for the Department of Homeland Security's Mike Pozmantier, center in white shirt. Pozmantier visited Sandia recently to observe cybersecurity projects. Credit: Dino Vournas, Sandia National Laboratories

Through the Department of Homeland Security's Transition to Practice (TTP) program, cybersecurity technologies developed at Sandia National Laboratories—and at other federal labs—now stand a better chance of

finding their way into the real world.

The innovative TTP program, spearheaded by the department's Science and Technology Directorate (S&T), helps move federally funded cybersecurity technologies into broader use. Getting research discoveries and new technologies over the so-called "valley of death"—the gap between early, promising research on one side and technology that's in use on the other—is a dire need in the national lab community.

"Moving technologies from the laboratory into actual practice is difficult," said Steve Hurd, a cybersecurity researcher who helps lead Sandia's TTP efforts. He said one major reason is that technologies that seem to work in the lab might need fine-tuning or further upgrades in the field.

"So TTP is an inventive attempt to help all the labs improve in this area," Hurd continued. "It's paying dividends already by opening doors that will get new innovative cyber defense technologies from Sandia and other laboratories into the hands of industry, academia and other research institutions that can really use them."

TTP's methodology is straightforward. Department of Homeland Security's Mike Pozmantier, the program manager for TTP in the S&T Cyber Security Division, conducts events across the country each year that feature cyber technologies developed at Department of Energy (DOE) and Department of Defense (DoD) laboratories and selected for evaluation by DHS. The events are targeted to specific sectors and audiences, including those in the federal government and the high-tech, energy, financial and critical infrastructure sectors.

The goal is to generate interest, initiate conversations and build relationships and business partnerships that get important cyber technologies, including some developed at Sandia, into practice. That

could be accomplished through pilot programs with industry, licensing or spinning off of technologies into startup companies through venture capital funding.

To support this process, selected technologies go through testing and evaluation to assess whether they're ready for a practical pilot test or commercialization. Technology providers also get help readying their technologies for market.

Sandia has key testing and evaluation role

In addition to considering Sandia-developed cyber technologies for transition, DHS uses Sandia's cybersecurity expertise to test and evaluate TTP technologies developed by other DOE and DoD labs.

"Our main goal is to help make the technologies easier and more cost-effective for end users to adopt, ultimately leading to more effective protection of digital systems," said Hurd. "We try to discover the areas in the technology that need improvement, then provide specific feedback to the developers."

Sandia tests in realistic environments, using a wide range of tools, including dynamic testing of executable files in software and the adversarial-based red-teaming, something that Sandia has excelled at for years. "Red teaming" refers to assessments that help customers acquire an independent, objective view of their technologies' weaknesses from the perspectives of a wide variety of potential adversaries.

Sandia is employing two unique capabilities as part of the TTP test and evaluation effort, said project manager Susanna Gordon.

"Our Forensics Analysis Repository for Malware, or FARM, provides a large number of analyzed malware samples that we are using to test

technologies intended for enhanced malware analysis," said Gordon. For technologies intended to run on enterprise-scale networks, Sandia's researchers are conducting tests using the labs' Emulytics platforms, which can efficiently emulate and analyze representative enterprise-scale networks, greatly reducing the cost of running at-scale testing.

The test and evaluation team also examines implementation costs and looks for new problems or risks associated with each technology it evaluates.

"Maybe the product successfully addresses some problem. But, to use an analogy, Sandia knows from experience that adding new computer security is not like building another fence," Gordon said. "What is intended to add additional security to a computer can actually be counterproductive and break the existing security system. Those things have to be considered very carefully."

Long-lasting value

In TTP's kickoff year, three cyber technologies were selected from Oak Ridge National Laboratory, two from Pacific Northwest National Laboratory, and one each from Sandia, Lawrence Livermore and Los Alamos labs. When TTP expanded its reach to DoD labs in its second year, two Sandia technologies, SecuritySeal and WeaselBoard, were selected. Now, in its third year, the TTP program again selected two Sandia technologies, the Sandia Cyber Omni Tracker and Network Randomization Tool for Integrated Computer Solutions.

Sandia's CodeSeal, a year-one TTP-selected technology, is a program that protects critical software from malware and a variety of security gaps. CodeSeal is gaining industry interest from Vir2us, a Bay Area computer security company, and may soon see real-world use scenario at the DOE GridSTAR Center in Philadelphia. The plan, says Sandia

business development specialist Craig Smith, is to bring CodeSeal to GridSTAR—embedded into Vir2us's security suite program, Citadel—to execute on the grid, an activity expected to lead to useful validation data for CodeSeal.

"With successful validation of CodeSeal, we see the opportunity to integrate CodeSeal into Citadel, enhancing Vir2us's already-impressive lineup of security systems," said Smith.

"As a Federally Funded Research and Development Center, one of our main objectives is to partner with DHS to improve the nation's cybersecurity posture in whatever capacity we can best serve," Hurd said. "We know that any good cyber technology will benefit the entire community, no matter which lab has developed it, and we are pleased to draw on Sandia's broad and deep cybersecurity expertise to develop new technologies and also to make those of the entire community stronger."

Provided by Sandia National Laboratories