Cyber workshop at Sandia Labs seeks potential responses to cyberattacks

October 26 2011

Among other dubious achievements, hackers have stolen identities, broken into bank accounts and breached computer systems of military contractors. They could conceivably interrupt water or electricity service to targeted populations. And worse.

To solve these problems, Sandia National Laboratories has plans to increase cybersecurity research over the coming year through a new Cyber Engineering Research Institute (CERI) that will more closely coordinate with industry and universities and have a presence on both Sandia campuses in New Mexico and California.

The push accompanied a recent packed, two-day meeting on cybersecurity at Sandia's Computer Science Research Center. At the meeting, Rob Leland, center director, told the attendees: "The paradox is that even as we rely increasingly on computers to run our utilities, banks and basic security measures, the possibility of an adversary seriously damaging the increasingly complex programs that run these concerns has increased."

The difficulties of defending against cyberattacks and what to do to change that situation, were major themes of the second University Partners Cyber Open House and Workshop led by Sandia researcher Ben Cook, manager of Cyber Research and Education.

"One of our overarching purposes for holding this workshop was to increase awareness of Sandia as a research and educational partner," said

Cook. "There are few places in the country where a student can come and work on real cybersecurity projects that have national impact."

Attendees included 30 professors from across the U.S., along with cybersecurity program directors from the Department of Homeland Security and the National Science Foundation (NSF).

The meeting divided overwhelming macro-security problems into more workable pieces.

A key to developing strong cyberdefenses is painting a realistic picture of the threats, said Ann Campbell, Sandia senior manager for cyber research. Firewalls and antivirus software are important but sophisticated adversaries are more devious. They may introduce malicious elements into the supply chain so they later can steal information, whether personal or relating to national security, or weaken an information system by degrading its performance or availability.

"The nation needs to find ways to share threat information without compromising sensitive information," Campbell said.

Another problem is stagnating student enrollment in cyber courses.

One way to solve that problem, and at the same time come up with radical security innovations, could be through the historically effective method of prize competitions, suggested Carl Landwehr, NSF's program director for Trusted Computing.

"Evidence shows that a well-framed public competition can trigger innovation," he said.

Landwehr highlighted the limited progress to date in building appropriate cyberdefenses for large-scale computer systems. "I've been

working on this problem for 40 years, and all I've seen are Bandaids," he said. Then he provided a list of historical examples — one dating back to a 15th century design competition for a cathedral dome in Florence, Italy — to show how public competitions have led to technological breakthroughs, as well as significant public involvement.

A cybersecurity design competition with a particular target, prize and completion date, he said, could not only lead to radical technical solutions, but also help reinvigorate the research community and attract students to a field facing chronic talent shortages.

One reason for tepid student interest is that society rewards those who come up with imaginative, money-making programs, not cybercops, participants pointed out.

Also, university professors may find teaching the dynamic ins and outs of immediate response to threat less appealing than extensive investigations within specialty areas that lead to peer-reviewed publications.

As professor Ravi Sandhu of the University of Texas-San Antonio put it, "Academic incentives may encourage inertia, and inertia will not solve this problem."

He said an effective cybersecurity curriculum might include computer science theory, principles and practice; security theory; STEM (Science, Technology, Engineering and Mathematics) instruction, principles and practice; and statistics, sociology, organizational theory, economics, game theory, laws, regulations, compliance, privacy, history, successes and failures.

"In a world of overwhelming complexity, with incomprehensible advances happening in every branch of computing every month, how do

we train a cadre of enough students with enough incentives to learn so much that they can actively contribute before their [computer] knowledge is dated?" he said.

Discussions of one possible prize competition — better security for "smart" electric meters — showed that conducting challenges for even simple systems would take thought.

Sandia researchers Dan Thomsen and Lyndon Pierson said one reason the workshop chose smart meters is that they are tangible examples of a tough problem with high exposure.

"The adversary has access to as many units as needed to 'reverse engineer' the security measures," said Pierson, "and, with access to the supply chain portion of the life cycle, can insert [malicious elements that can be] triggered [later] to cause a targeted denial of electrical service."

What to do?

The necessarily low per-unit cost of meters would limit contestants to inexpensive, possibly less-effective security solutions. And even a superior solution would be hampered in its overall effect by the large number of meters already installed.

Other technologies could serve as a contest focus, but it would be hard to predict which would create the greatest future benefit.

In other sessions, researchers from a range of disciplines — including experimental criminal psychology, computational social science and visual analytics — suggested that the Internet is best understood as a human system, not a technological one, and that social science theory and methods can make important contributions to a science of cybersecurity.

Sandia researcher Kevin Nauer introduced a cyber forensics network training environment, developed by Sandia and Los Alamos national laboratories with Department of Energy support. Its purpose is to build a stronger virtual community of cyber defenders through team-building competitive exercises.

Thomsen gave an overview of the new educational game "Space Sheep," which increases student understanding of basic principles for securing threatened systems. The game was developed by Thomsen and several of Sandia's Center for Cyber Defenders (CCD) students over the past year with Sandia support and should be available publicly soon in response to requests from several faculty at the workshop. The CCD is a hands-on internship program focused on cybersecurity research.

In addition, the CCD offers students exposure to external research ideas and opportunities. The program hosts visiting faculty scholars who share their research, interact with Sandians and present lectures.

More information: Cybersecurity Research: www.sandia.gov/mission/dsa/cyber.html

Provided by Sandia National Laboratories