LAST YEAR, THE DEPARTMENT OF HOMELAND SECURITY (DHS) CAME IN FOR SOME BLISTERING CRITICISM FOR ITS LACK OF ATTENTION TO CYBER VULNERABILITIES. Cybersecurity czar Amit Yoran resigned after one year, saying publicly that he had done all he set out to do at DHS, but privately airing his frustration that he was unable to move cybersecurity forward within the department.

In recent months, however, the visibility of DHS cybersecurity efforts have picked up, and one project in particular is showing tremendous promise.

It’s called the Cyber Defense Technology Experimental Research (DETER) test bed, which is operated by the Information Sciences Institute (ISI) at the University of Southern California, with help from the University of California (UC) Berkeley. It’s the result of the Homeland Security Advanced Research Project Agency (HSARPA) teaming up with the National Science Foundation (NSF). The two agencies then turned to ISI in Marina Del Rey, Calif., where much of the Internet was truly born.

HSARPA and NSF provided ISI with about $10 million in funds under a three-year grant for the project. About one year of the grant is left. After that, DHS has committed to supporting DETER through at least fiscal 2010, continuing to make the cybersecurity test bed available for free use by qualified users.

“You can go back and look, and the government, particularly in the form of [the Defense Advanced Research Projects Agency], NSF, and [the National Security Agency] and other agencies, has spent hundreds and hundreds of millions of dollars on information security research over the last 15 to 20 years,” Terry Benzel, the DETER program director at ISI, told HSToday. “Yet, as a nation, we still lack wide-scale deployment of security technologies sufficient to protect us, particularly from deliberate cyberattacks. DETER will help develop those technologies.”

DETER is a physical test bed that simulates the Internet. Malicious code can be tested in this enclosed, quarantined network and its properties isolated and studied so that countermeasures can be developed—like studying a virus in an isolated laboratory environment in order to develop vaccines.

THE NODES

At press time, DETER had about 200 nodes (in contrast to the millions of nodes that make up the Internet). However, ISI was planning to increase that number to 300. ISI uses Cisco 6590 switches to connect the nodes together and run a software application called Emulab, which was developed at the University of Utah, to configure the nodes in arbitrary topologies.

The DETER nodes simulate any piece of equipment or connection that might be found on the Internet, including an entire network, if necessary. The Emulab software can also run virtual software at a 10:1 ratio, enabling ISI to simulate up to 10 times as many nodes in a virtual environment.

“You can connect together these nodes and represent something that looks like the Internet,” Benzel said. “In addition, the DETER test bed is designed specifically to allow our experimenters to run tests with malicious code, so we can have true live malware running in the test bed.”

DETER is not the only simulated Internet in the country. However, most of the other simulations are owned by private...
companies that don’t open their doors to individual researchers. Few offer the ability to connect to a test bed through an Internet interface, according to Benzel.

Further, because of the predominance of closed, private research in cybersecurity, the United States government has lacked a way to conduct research and development into new cybersecurity technologies. That has left a technological gap that is difficult to measure.

“It’s particularly hard in security because security is sort of defined as the absence of something bad happening. You build a new technology and deploy it, and then say, ‘Well, see, you didn’t get attacked,’” Benzel pointed out.

“Cybersecurity is of national importance, and research is a fundamental aspect that must be funded to ease current security concerns,” Douglas Maughan, HSARPA program manager for DETER, said in a statement. “Through investment in projects like DETER, which leverage the best academic and private-sector capabilities in the world, the government can better understand the requirements for continued security of this country’s networks.”

BEST THINKERS

About 20 top researchers from different academic institutes have formed an organization called Evaluation Methods for Internet Security Technology (EMIST) to work with the DETER test bed. Also funded through the HSARPA and NSF grant, EMIST conducts scientific experimentation and analysis with emerging security technologies for a “true apples-to-apples comparison” of their effectiveness.

“They were the first set of users on the test bed that helped us shake out the test bed as we built it,” she said. “They’re now publishing a number of papers that are describing how to use the test bed and create scientifically valid results.”

REQUIREMENTS FOR CONTINUED SECURITY

“It’s the reason for that is there are not a whole lot of good places to test for these types of worms and issues without possibly affecting live gear.”

“DETER is one of those instances that prove that government can get things right and provide unique capabilities that will provide widespread benefits.

Cybersecurity provides a unique opportunity for government—and, particularly, DHS—to fill a gap that private industry has been unable to cover. As Benzel pointed out, many corporations find it difficult to effectively determine what proportion of their budgets they should spend on cybersecurity. Chief information officers and chief financial officers want to know the return on investment for security products, which can be difficult to determine without the proper data.

Moreover, cyber vulnerabilities affect all of the country’s critical systems. But by testing malicious code in the safe confines of the DETER network and then sharing the results, the project can provide the antidotes that everyone needs—and that no single private corporation can provide. 