Service Academy CyberStakes Proves Worth as Learning Tool

By Cheryl Pellerin, DoD News, Defense Media Activity / Published February 16, 2016

Three years into a program for building cyber proficiency in service academy midshipmen and cadets, the annual CyberStakes competition has proven its worth as an important learning tool for these high-tech skills, a senior Defense Department official said.

The Defense Advanced Research Projects Agency launched the competition as a pilot program in 2014, and this year transitioned its sponsorship to the Office of the Secretary of Defense, which expanded the program's scope.

DoD hosted the event Feb. 5-7 at Soldiers and Sailors Memorial Hall in Pittsburgh.

Midshipmen and cadets from the Navy, Army, Air Force and Coast Guard service academies participate in CyberStakes 2016,

an annual cutting-edge Defense Department cyber skills competition held in Pittsburgh, Feb. 5-7, 2016. Photo courtesy of ForAllSecure

Each service academy sent its best students: 14 from the U.S. Air Force Academy, 14 from the U.S. Military Academy, 14 from the U.S. Naval Academy and 10 from the U.S. Coast Guard Academy. A team of four active-duty members of a cyber protection brigade also participated for the first time.

Also at the competition were expert mentors from DoD, the National Security Agency, the services and Carnegie Mellon University.

Hands-on Engagement

"This year's CyberStakes competition represented an exciting new level of challenging hands-on engagement," Frank C. DiGiovanni, the Defense Department's director of force training, told DoD News in a recent interview. "It bodes well for our nation's cyber training pipeline."

Participants competed in a range of events that included reverse engineering, cyber forensics, cryptography, discovering and exploiting vulnerabilities in executable programs, and actual, not cyber, lock picking -- a physical counterpart to cyber vulnerability analysis that is traditional at cyber competitions.

Participants in the final live, full-spectrum, capture-the-flag exercise were chosen after completing up to six months of intensive online training.

When the dust cleared, each academy and the cyber protection brigade members had won their share of medals.

The U.S. Military Academy won 35 -- 15 gold, 12 silver and eight bronze medals. The U.S. Coast Guard Academy won 20 -- three gold, six silver and 11 bronze medals. The U.S. Air Force Academy won 19 -- two gold, seven silver and 10 bronze. The U.S. Naval Academy won 18 -- eight gold, seven silver and three bronze. The cyber protection team won four gold medals.

Practical Hacking

The competition, DiGiovanni said, took the abilities the midshipmen and cadets acquired at each academy and provided an arena where they could exercise those skill sets.

"CyberStakes is important to the department because it builds interest in this area and provides students learning [cyber] in the academies opportunities to exercise it in a … competitive environment," DiGiovanni explained.

Cybersecurity expert Dr. David Brumley, who helps to train teams in the competition, said that every year the midshipmen and cadets get more advanced.

Brumley heads a company called ForAllSecure, a high-tech spinoff of Carnegie Mellon University. Brumley also is a CMU professor of electrical and computer engineering and a founding member of the Plaid Parliament of Pwning.

The PPP is a CMU cybersecurity team that's highly ranked in international competitions and whose members acted as mentors to the midshipmen and cadets.

Better Every Year

"This year the participants were able to find not just vulnerabilities but also show they could harden exploits to defeat operating system security measures," Brumley said. "They were better at pulling attacks off the wire, analyzing them and being able to take action."

In his role as DoD's training director, DiGiovanni says CyberStakes has done innovative work in providing a practicum -- a supervised practical application of learning -- for the members of each service academy.

"We have learned in some of the research we've done in this area that you should look at cyber more as a cognitive trade than something that can be taught through a formal education traditional classroom model," DiGiovanni said.

Brumley agrees.

"We teach computer security the way elite hackers learn," he said.

Practiced Skill

"In CyberStakes we make computer security a practiced skill," Brumley explained. "We encapsulate the essence of concepts like finding

vulnerabilities, exploitation and defenses into hands-on exercises in a game environment. By playing the game, students solve problems, get better and can deliberately practice skills."

A similar DoD cyber-learning effort is the DoD Cyber Operations Academy, a cyber training course based at Fort McNair in Washington and introduced in early 2015 by DiGiovanni's office. The six-month, full-time course is designed for active-duty service members and government civilians whose organizations nominate them for participation.

This pilot course, during which students also learn from hackers, is based on an apprenticeship-journeyman learning model and encourages hands-on problem solving, DiGiovanni said.

The first run of the course produced strong results and positive feedback, he added, with most graduates passing the difficult Offensive Security Professional Certification Exam. The course will run again this spring.

"The course is really about understanding what it takes to train someone to be a cyber practitioner," DiGiovanni said.

Army 1st Lt. Benjamin Allison, now with the 780th Military Intelligence Brigade, participated in the first DARPA CyberStakes pilot in 2014 as a West Point senior.

"As the cadet in charge of our cyber team, CyberStakes Online was an incredible tool for me to use with new and veteran team members to hone their craft," he said in an email interview.

Outside CyberStakes, the participating teams competed against undergraduate, graduate and professional hacking teams from all over the world in online competitions, Allison added.

The final capture-the-flag competition, called CyberStakes Live, he said, "drove home the challenge of merging offensive and defensive cyber. Without the knowledge of how an attacker operates, it would have been near-impossible for us to defend our services."

Allison says his job today is a split between technical work and a more traditional officer role.

"I believe that officers in cyber should strive to be dual-hatted by being technical experts and leaders. … In the cyber domain, officers cannot be effective leaders unless they are technical experts," the lieutenant said.

(Follow Cheryl Pellerin on Twitter @PellerinDoDNews)

Related Biographies

Frank C. DiGiovanni