The CyberPatriot National High School Cyber Defense Competition

Lewis Shepherd, the chief technology officer at Microsoft’s Institute for Advanced Technology in Governments, has stated that the need for talented cybersecurity professionals is quickly outpacing the numbers produced by the educational systems in the US and other nations. He points out that the creation of the new US Cyber Command, along with the recruiting goals of organizations such as the US National Security Agency (NSA) and Department of Homeland Security (DHS), has created an environment in which the government is hiring the few professionals being produced, leaving industry to scramble to fill its own positions.

Government efforts to attract more individuals to this critical career field have so far centered around initiatives such as the DHS/NSA National Centers of Academic Excellence in Information Assurance Education, which recently expanded to include two-year undergraduate institutions. Other efforts include the development of cybersecurity competitions such as the Cyber Defense Exercise and the National Collegiate Cyber Defense Competition (NCCDC). (For more on these and other competitions, see the sidebar.)

Collegiate competitions have proven successful at introducing students to the possibility of a cybersecurity or information assurance career. However, they haven’t been overly successful at attracting new students to majors in science, technology, engineering, or math (STEM) in college. This is because these competitions typically appeal to those who have already decided to enter one of these fields. We need STEM-focused programs reaching into high schools to help attract those who might not have decided on a major, a career field, or even an area of interest. One approach is to move cybersecurity competitions to the high school level. This is the goal of the CyberPatriot National High School Cyber Defense Competition (www.uscyberpatriot.org).

**CyberPatriot**

In 2005, the Center for Infrastructure Assurance and Security (CIAS) at the University of Texas at San Antonio conducted a one-day cybersecurity competition similar to the NCCDC. The event was cosponsored by the Alamo Chapter of the Air Force Association (AFA). Although the event was a success (with scholarships awarded to members of the winning team and the overall winning individual), the CIAS elected to focus its limited resources on the NCCDC, which was still in its early years.

Over the next three years, cybersecurity’s importance continued to increase, as did the demand for more trained cybersecurity professionals. Several organizations in the US federal government began calling for additional programs to encourage students to consider information assurance and cybersecurity careers. In particular, the US Air Force added cyberspace defense to its mission statement and began creating a “cyber command.” The AFA, a long-time supporter of Air Force programs and initiatives, saw the need for someone to step up and develop a program to excite high school students about STEM programs in general and cybersecurity in particular. The AFA’s Aerospace Education Council (AEC) is dedicated to encouraging America’s youth to enter the aerospace industry through scholarships and outreach programs. With the Air Force expanding its mission to include cyberspace, the AEC expanded its program to include cyberspace security as well. It formed a partnership including the AFA, the Air Force, the CIAS, and Science Applications International (SAIC). Together, they began developing CyberPatriot, a national program to excite and motivate high school students in cybersecurity.
Other Cybersecurity Competitions

The CyberPatriot competition certainly isn’t the only, or even the first, cybersecurity competition. It’s also not the only high school cybersecurity competition or competition focused on a program related to science, technology, engineering, or math (STEM). One of the earliest and best-known cybersecurity competitions is the annual capture-the-flag (CTF) event at DEF CON in Las Vegas. That event is open to participants from any background and has included teams from academia and industry. The competitors might also be any age, so in theory high school students or teams could compete.

The US Military Academy created the Cyber Defense Exercise (CDX) in 2001 to meet the capstone requirements for their information assurance course. The CDX, sponsored by the US National Security Agency, uses virtual private networks to create a distributed, wide-area competition involving all the US military academies. In 2009, it became international by including the Royal Military College of Canada. Each team receives a computer network with common services running that it must secure while staying within a provided budget. Each team defends its network against a team of attackers called the red team. Gray-team players cause problems as mischievous or clueless insiders. Offensive actions against other teams aren’t allowed.

Since 2004, the University of California, Santa Barbara, has hosted the iCTF (http://ictf.cs.ucsb.edu), an international academic CTF competition. Like the CDX, the iCTF is a distributed, wide-area security exercise, but it includes both offensive and defensive components. The teams have identical virtual hosts that they must defend while simultaneously attacking other teams’ services. The iCTF was based loosely on the original DEF CON CTF but has been modified to allow for its geographically distributed nature. In 2009, 800 students in 56 teams participated.

The National Collegiate Cyber Defense Competition (NCCDC; www.nationalccdc.org) was created by the Center for Infrastructure Assurance and Security (CIAS) at the University of Texas at San Antonio. The NCCDC is open to all two- and four-year US institutions. It started in 2005 with a single competition involving five teams from Texas schools. It has grown into a program that, in 2011, will include nine regional competitions, with the winning team from each regional event competing for the national championship in San Antonio. In this competition, all teams have identical networks on which they must maintain a set of business-critical services. Teams accrue points by keeping those services running and by completing business tasks representing duties common in government and industry. Teams can lose points when their services are down for an extended period or when the red team successfully gains some level of access to their network.

The IT-Olympics is the culmination of the high school IT-Adventures event (www.it-adventures.org), created by Iowa State University, the Iowa state government, and Iowa businesses. It’s a multifaceted, two-day competition involving cyberdefense, game design, and robotics. The cybersecurity portion starts approximately one month before the actual competition, when the teams receive remote access to their computers. They get physical access to the machines on the competition’s first day. The teams must set up and secure services, operating systems, and the network. On the second day, a red team simulates the hostile environment found on the Internet. A green team tests the usability of the student teams’ networks, gives the teams tasks to complete, and requests network changes. Teams are judged on an IT-related community service they had to accomplish before the IT-Olympics and on how they perform in the competition’s other parts.

In 2009, the US Cyber Challenge was unveiled as an initiative to help the US regain the lead in cyberspace. This competition has three components. In the US Department of Defense Digital Crime Center’s Digital Forensics Challenge, contestants must deal with a succession of increasingly difficult digital-forensics tasks. The Network Attack Competition focuses on discovering and exploiting network vulnerabilities. These two components are open to high school, undergraduate, and graduate students. The third component, CyberPatriot, is specifically for high school students.

For more on CyberPatriot, see the main article.

References


During discussions in the summer and fall of 2008, the partnership developed plans to conduct the first pilot of CyberPatriot in Orlando, Florida, in February 2009. The first teams were from Orlando–area high school Junior Air Force Reserve Officer Training Corps (ROTC) or Civil Air Patrol (CAP) programs. This strategy provided an existing infrastructure for promoting the program at schools and was seen as a way to control the growth of what would likely be a popular event.

The competition’s format was similar to the NCCDC. Each team received an identical network to secure and protect. No offensive activity was allowed. A
team of attackers (called the red team) simulated the environment that students would see if they were protecting a real-world network. SAIC provided its CyberNEXS hardware and software platform (www.saic.com/cybernexs) for the competition. As the planners anticipated, the first competition was well received, and the students were engaged and excited. One surprising response from a survey of coaches and students was that more than 50 percent of the students said they were more likely to attend college as a result of their participation. This encouraged the CyberPatriot partners to immediately start planning the next year’s event.

The first goal for the competition’s second year was to expand the competition to the national level. The partnership still wanted to control the competition’s growth, so it continued to limit the competition to Junior Air Force ROTC and CAP units. Expanding the competition also meant changing its format to allow for the increased numbers. CyberPatriot II therefore included preliminary virtual competitions. Over 170 five-person teams competed in two elimination rounds in which they connected with CyberNEXS through the Internet. Both rounds focused only on Windows-based operating systems, with the second round increasing in complexity. The top eight teams from these rounds received a trip to Orlando for the championship, which added Unix-based systems and a red team. Members of the top three teams won scholarships. Again, the competition was a tremendous success. Plans immediately commenced for the 2011 competition.

The biggest change for 2011 is that the competition is now open to any interested high school team. There are two categories, a military-service category for teams consisting of any Junior ROTC or CAP unit, and an open category for all students enrolled in a US high school. The competition even has provisions for homeschooled students. The maximum number of teams in each category is only 500, however. Future years will see the elimination of this restriction so that any number of teams can compete.

The Educational Component

A significant difference between collegiate and high school programs is the need to include education or training. For example, the NCCDC assumes that the students either are from a university with an established cybersecurity program or are interested in cybersecurity and have a faculty sponsor. It provides no training or educational materials to competitors. For a high school competition, this expectation is unrealistic. Few high schools will have a teacher with a cybersecurity background, and many might have problems finding a teacher with even a modest IT background.

Therefore, the CyberPatriot program from the start has included an educational and training component. This component continues to develop; it currently consists of a series of training videos and presentations that coaches can use to prepare their teams. In addition, SAIC provides training on security in general and on using CyberNEXS. All the training materials are provided to the schools at no cost.

Competitions are a valuable tool for exciting and motivating students at the college and high school levels. CyberPatriot has established the framework for what’s proving to be a viable, sustainable program with both government and industry interest. Recently, Northrop Grumman signed on as the presenting sponsor, providing significant funding to keep CyberPatriot running for the next three years. Although CyberPatriot has made great strides, much remains to be done, especially regarding educational programs to prepare the teams to compete.

As the program expands, we expect that a number of the competitors will choose cybersecurity careers. However, even those who take a different path will have learned how to better secure their computer systems and networks. No matter where life takes them, this skill will help them and the US.

Reference


Gregory B. White is an associate professor in the Department of Computer Science at the University of Texas at San Antonio. Contact him at greg.white@utsa.edu.

Dwayne Williams is an associate director for special projects in the Center for Infrastructure Assurance and Security at the University of Texas at San Antonio. Contact him at dwayne.williams@utsa.edu.

Keith Harrison is a PhD student in the Department of Computer Science at the University of Texas at San Antonio. Contact him at kharrison@cs.utsa.edu.

Selected CS articles and columns are also available for free at http://ComputingNow.computer.org.

Interested in writing for this department? Please contact editors Matt Bishop (bishop@cs.ucdavis.edu) and Cynthia Irvine (irvine@nps.edu).