Florida high schoolers square off in an unusual battle to defend a computer network.

CyberPatriot Smackdown

By Peter Grier

Photo by Dan Higgins

Air Force JROTC cadets (l-r) Michael Velaquez, Mark Schoeni, and Robert DeWitt work together on Team Doolittle to defend their network.

When the results were announced, the winning team erupted in celebration. Teens from Osceola High School, in Kissimmee, Fla., cheered and fist-bumped as if they had just won a national debate contest or major athletic event.

In fact, their triumph had come in a more unusual, 21st century kind of challenge. It was called *CyberPatriot,* the first-ever computer network defense contest designed as a national competition for high schoolers.

The Air Force Association held *CyberPatriot* Feb. 26-27 in conjunction with AFA's Air Warfare Symposium in Orlando, Fla. The point was to hook as many teens as possible on the challenge of cyber security—a discipline for which military and commercial demand will only increase.

"We have very little computer security expertise in this country," said Gregory B. White, director of the

Center for Infrastructure Assurance and Security (CIAS) at the University of Texas, San Antonio. "We need a lot more."

White was instrumental in the competition's design and implementation. A veteran of 19 years of active duty in the Air Force, he is a colonel in the Air Force Reserve, and one of the nation's leading experts on computer security. At CIAS, he has run collegiate-level security competitions for years.

A national high school-level cyber competition has been a dream of White's since he initiated the National Collegiate Cyber Defense Competition more than five years ago. But *CyberPatriot* 2009 was finally made possible by a convergence of interests and the persistence of an AFA national officer. For AFA, it is an aerospace education initiative with a potential national impact. Taking point on the project was S. Sanford Schlitt, AFA's vice chairman of the board for aerospace education, who pushed the project to completion in just a single year.

Science Applications International Corp. (SAIC) was a third partner in the effort. The firm provided its TeamDefend commercial cyber security training system as the competition platform during *CyperPatriot I.*

Photo by Dan Higgins

Two members of Team Spaatz, JROTC cadets Linval Overdiep and Gretchen Rivera, plot cyber defense strategies at the competition.

The Roar of the Crowd

CyberPatriot 2009 was a prototype event, and its field organizers did not really know the extent to which entrants would be engaged. They were worried that teenagers would find computer security challenges to be dull, or too hard, or that participants would throw up their hands in disgust or frustration.

Nobody thinks that anymore. The roar of the champions proved the enthusiasm was real. "People in the exhibit area heard those guys screaming and yelling," said David T. Buckwalter, AFA's executive vice president. "That was cool."

The first *CyberPatriot* games were limited to eight high school-age teams from Junior ROTC and Civil Air Patrol units within easy driving distance of Orlando. The teens were fired up even about the first day's results. When Osceola was named champion, the noise was so loud it passed through two walls and a corridor, into the exhibit hall.

To prepare the teams for the competition, *CyberPatriot's* organizers had posted some material on the main Web site of CIAS. SAIC held a distance-learning introduction to familiarize the students with the TeamDefend box. The TeamDefend system allows users to assume administrative and protective duties for a "network" similar to that used by a small commercial firm. Typically, that means a system of 50 or so users, with seven to 10 servers, Web and e-mail service, and an e-commerce site.

Buckwalter said he was worried that the organizers had not done too well in producing this academic introduction. Then he listened to a conference call following the TeamDefend introduction. The SAIC engineer running the call asked if anyone had questions, and a student piped up with something that Buckwalter describes as "computer gibberish."

"So we figured the kids are smarter than we are, and we went with it," he said.

Photo by Dan Higgins

***Gen. Norton Schwartz, USAF Chief of Staff, speaks with Diana Londono and Michael Roach from Team Schriever at* CyberPatriot I.**

Photo by Dan Higgins

Team Wilson, composed of cadets from the Florida Civil Air Patrol, celebrates its Day Two win. (L-r): Charles Walker, Timothy Walker (coach), Joshua Dovi, and Isaac Haring.

In competitions, each team gets an identical hardware and software setup. They then must detect and respond to outside threats, patch holes, and keep the network and services up and running. Part of the point is to balance the need for cyber protections against business requirements. "You don't get to devote 100 percent of your time to security," said CIAS' White.

The collegiate-level competitions White runs are more challenging than the *CyberPatriot* scenarios. But that does not mean the high school-level problems are easy ones. They are meant to mimic the sort of thing competitors might encounter in the real world.

"If they were to graduate from high school and were to get a job as an IT professional at some company, they could walk into a situation just like this," said White. "You are pretty much guaranteed that somebody is going to attack you."

A Red Team of adult experts runs the attacks. The three-by-five-foot SAIC TeamDefend box monitors both their efforts and the defensive response.

The result is a quantitative score, updated in real time, so declaring a winner was a simple matter of comparing final scores.

The beauty of TeamDefend is that when you are finished with the three-hour exercise period, you get a log of all the things that happened, so you can clearly explain what the students thought was happening versus the reality of what was, said Carleton Ayers, SAIC's chief systems engineer for TeamDefend.

One need only look at the march of news to see the need for expanded US training of and interest in cyber defense professionals.

In 2007, a cyber attack on Estonia blocked Web sites and paralyzed the country's Internet service. At the height of the crisis, Estonian use of bank cards and mobile phones was sharply curtailed.

In 2008, Russia's physical invasion of Georgian territory was accompanied by a cyber invasion. Georgian government Web sites were blocked, among other electronic tricks.

The New Threat Arena

Also in 2008, US military computers were subjected to a severe and painful cyber assault that damaged some US Central Command networks. There is some evidence the attack was connected to the Russian government.

Then in early 2009, a University of Toronto study unveiled the so-called "Ghostnet," a web of thousands of computers in more than a hundred countries that had been infiltrated by cyber spies. Researchers said the hackers who carried out the assault were based almost exclusively in China, though the Chinese government denied any official involvement.

For the US, the particular problem in this area is that it has the most cyber "coastline" to defend. It has the world's largest economy and the biggest, most advanced military. Both are heavily dependent on smooth operation of advanced computer systems.

Yet an assault on these networks can be mounted by anyone with knowledge and a high-speed connection to the Web.

One thing *CyberPatriot* is not meant to be is a training ground for hackers. Hackers are searching for one chink in a computer system's armor; defenders have to mount a broader effort that takes into account all the different ways hackers might work.

While attacking things sounds fun, the more difficult academic and real world problem is defense of a network, said Ayers. Hackers need find only a single weakness; defenders have to protect the entire network while keeping their business systems running.

Realization of this vulnerability is one reason the Air Force has decided to establish 24th Air Force, under Air Force Space Command, to lead cyber defense operations.

In the cyber area, "we have near-peer competitors, which is something we've not had with other traditional warfighting assets," said Maj. Gen. William T. Lord, head of USAF's provisional Cyber Command, last year. "In the cyber domain, ... we have to run to stay ahead."

Running to stay ahead means, among other things, developing as many cyber warriors as possible. And despite all the buzz surrounding everything cyber, that is not happening in the nation as a whole.

"We need upwards of 10,000 [computer] security professionals a year, and we're not producing them," said White.

Hence *CyberPatriot.* It is intended as a sort of first step toward the big leagues for youngsters who might think the area is interesting, but have little idea of what it really entails.

Collegiate-level studies and competitions are great, but "the high school competition is meant to get people into this at an even earlier age," said White.

For AFA, the idea of *CyberPatriot* began with its Aerospace Education Council. The need was obvious—so why not try something that could potentially raise the profile of cyber security nationwide?

With Schlitt's networking and persistence, AFA connected with White and SAIC. By holding the proof-of-concept

Staff photo by David T. Buckwalter

CyberPatriot's *winning team was Team Spaatz from Osceola High School in Kissimmee. Pictured are (kneeling): Jacob Caudill, Gretchen Rivera, Madiha Majeed, (standing, l-r) Joseph Delhoyo, AFA Chairman of the Board Joseph Sutter, Linval Overdiep, AFA Vice Chairman of the Board for Aerospace Education Sanford Schlitt, Kiara Vazquez, John Borrero, (back row) Rick Hamilton, and SASI retired Maj. Jeffrey Miller.*

event at AFA's Orlando symposium, *CyberPatriot* would be on display for senior Air Force and defense industry officials.

But where to get the contestants? The answer to that was Junior ROTC, which is made up of students already inclined to citizenship and service. The Civil Air Patrol's teen division wanted to be included, as well. In the end, eight teams from the Orlando area entered—seven from Air Force JROTC and one from CAP.

Each team was given the name of a prominent former Air Force or Civil Air Patrol leader. Thus Osceola High School's group was nicknamed "Team Spaatz," after Gen. Carl A. "Tooey" Spaatz, the first USAF Chief of Staff. The team from the Florida wing of CAP was named "Team Wilson," for Gill Robb Wilson, CAP co-founder.

Each five-member group of students took their turn at one three-hour exercise, and to keep interest as high as possible, the organizers decided to name a daily winner. Team Spaatz from Osceola was Thursday's champ.

Though their active involvement was over, Team Spaatz showed up to watch Friday's competitors. If no one beat their score, they would be *CyberPatriot's* overall victors. But—somewhat to the surprise of contest organizers—two of the first day's teams out of the running showed up, too.

Of the four teams that competed the first day, only one didn't return. Their instructor, via e-mail, said their experience had been great—but that two team members had other commitments, and their colleagues did not want to attend without them—and that team voted to start preparing for next year's competition right away.

A Very Close Race

Team Wilson, the CAP contingent, won Friday's heat. Their result was very close to that of Team Spaatz. But the final score, announced by Gen. Stephen R. Lorenz, commander of Air Education and Training Command, showed Osceola the overall champion, by a nose.

That is when the noise began. Collegiate-level cyber security competitions may be more difficult, and the competitors more experienced, "but the excitement is probably much greater at the high school level," said White.

The winning team's primary competitors were cadets Linval Overdiep, Gretchen Rivera, Jacob Caudill, Joseph Delhoyo, and Rick Hamilton. Alternates were Madiha Majeed, Kiara Vazquez, and John Borrero. Their leader was Senior Aerospace Science Instructor retired Maj. Jeffrey A. Miller.

The first *CyberPatriot* event showed that the competition's formula is viable. Though the sample size was small, feedback from participants was very positive.

The goal now is to expand *CyberPatriot's* geographic breadth, and scale up the size of the contest. Organizers hope that this academic year, they will be able to attract entrants from 75 to 300 JROTC or CAP units, and have them engage in a preliminary round of distance competition. "What we're going to be having now is a multitiered concept," said White.

The first level will not involve travel. Instead, competitors will receive a disk containing a virtual image of an unsecured computer system. At some point they will receive a key to unlock the virtual system. They will then have a certain number of hours to plug the system's holes, as a remote scoring system watches.

"The more problems they find and secure, the more points they will get," said White.

Teams with the highest score will advance to the next level, consisting of perhaps 24 schools. They will then get a virtual image that will be a little tougher, with more problems, and perhaps a Unix-based system, as well as a Windows-based one.

An elite group of eight or so winners will advance and then travel to the *CyberPatriot II* finals in Orlando in February 2010.

As far as attracting teams goes, "we've had a lot of unsolicited interest," said White.

Beyond 2010, the hope is that *CyberPatriot* can expand beyond the bounds of JROTC and CAP units. The ultimate goal is a competition open to any high school in the US.

"Our ultimate goal, years and years in the future, is that any high school student in the country can sign up to compete in a national competition and through some phasing and staging ... fight a mini-cyber-war for some days, and be crowned the winner," said Schlitt. ■

Peter Grier, a Washington editor for the Christian Science Monitor, i*s a longtime defense correspondent and a contributing editor to* Air Force *Magazine. His most recent article, "Gary, You Better Get Back In It!," appeared in the April issue.*