The CyberSentinel

Commissioner's Cache

Congratulations CyberPatriot competitors! Another online competition is in the record books, and your impressive performances made all of us proud. You trained hard and it showed. Our coaches and mentors selflessly dedicated many hours of their time to give you the opportunity to compete in a challenging, fair, and safe environment. This year more teams than ever made strong showings in the online competition. To recognize your efforts, you will soon receive CyberPatriot participant kits. The national finalists are now heading to the in-person National Finals Competition in the Washington, D.C. area. This year's National Finals Competition will include a scored forensics event as well as the head-to-head cyberdefense event. Additionally, this year's competition is an international competition!

Upcoming Events

- March 22-23 National Finals Competition (Washington, D.C.)

Program Office Bits

- **Internships**—Great news! Northrop Gruman has internship opportunities for CyberPatriot students! See page 4 for more details and stay tuned to their careers page at:

  http://careers.northropgrumman.com/cyberpatriot.html

Cyber Crime: Silent — but Costly

Daily, we are bombarded with media reports of crimes. But few reports mention the crime that goes unnoticed until it is too late: cyber crime.

Silently, cyber criminals steal money and identities from victims of all ages. They harm businesses and steal technology. According to Symantec's press release of September 7, 2011, the cost of global cyber crime is $114 billion annually, with more than one million victims of cyber crime every day. For details, go to: http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02

Protecting our computers with antivirus software, software updates, etc., is important to the prevention of cyber crime, but is only part of the solution. The Federal Bureau of Investigation (FBI) and other government agencies

are another part of the solution.

The FBI leads the national effort to investigate high-tech crimes, including cyber-based terrorism, computer intrusions, and major cyber frauds. An example of the FBI's work was on display in late 2011.

The FBI announced that it shut down an international cyber crime ring in Operation Ghost Click, on November 9, 2011. The cyber crime ring used malicious software (malware) to infect about 500,000 computers in the U.S.

According to the FBI statement, the thieves were able to manipulate Internet advertising on the infected computers to generate at least $14 million in illicit fees. Additionally, the malware prevented users' antivirus software and operating systems from up-

dating, which exposed infected machines to even more malicious software. To learn about the FBI and Operation Ghost Click, go to: http://www.fbi.gov/news/stories/2011/november/malware_110911/malware_110911

Another agency, the Department of Defense Cyber Crime Center (DC3), is part of a joint task force which mitigates, neutralizes, and disrupts cyber intrusions presenting a national security threat. For DC3 information go to: http://www.dc3.mil

Cyber crime is silent and can be costly. But it can be curbed if we protect ourselves, while the FBI and other agencies actively disrupt cyber crime activities and apprehend the cyber criminals.

This Month's Question

What are the differences between a hacker, a cracker, and a script kiddy/kiddie?
(The answer appears on Page 3.)

Features

Round 3 Ends – U.S. and Canadian Teams Head to D.C.

CyberPatriot IV, Round 3, has ended. Twenty-four U.S. teams are heading to the National Finals Competition in Washington, D.C. Two Canadian teams will compete in an international exhibition competition in conjunction with our U.S. competition.

Round 3 was tough. During January 13-14, 2012, the All Service Division teams well represented their four Services' Junior Reserve Officer Training Corps (JROTC) programs and the Civil Air Patrol (CAP). The competition was actually _five_ different competitions, one for each of the four JROTC programs and CAP. The two top scoring teams from each of the four Services' JROTC programs and CAP advanced to the National Finals Competition.

To round out the 12 All Service finalist teams, the two teams with the top overall average scores, that were not their Service finalists, were Wild Card teams. This year both Wild Card teams were from CAP.

The Open Division competition was held during January 27-28, 2012. The competition was delayed six hours, on Saturday morning, due to a West Coast power outage. But the Open Division teams held the line. When the competition resumed, the teams were at their peak, though some teams waited up to six hours to begin the competition. Only six percentage points separated the average scores of the finalists. The Spokane, Washington area teams finished strong.

Like the All Service Division, multiple competitions occurred during the Open Division, Round 3. Six teams from Canada competed at the same time as the U.S. teams. The Canadian teams competed against each other to advance to the international exhibition, during the National Finals Competition. Open Division, Round 3, scores were released in a combined list to include the Canadian teams' scores.

It was a good round of competition. The national finalist teams are listed at: http://www.uscyberpatriot.org

Spotlight on Spokane

With the national championship mere weeks away, CyberPatriot IV teams nationwide are preparing for their final round of competition.

One school district in Washington State will be exceptionally busy. Seven teams from Spokane, Washington, are among the top 24 competing in the National Finals Championship round. And four of those teams are out of John R. Rogers High School.

This isn't Rogers High School's first appearance in the CyberPatriot competition. In CyberPatriot III, two teams registered to compete, one in each division. With the enthusiasm of the Rogers' team's Air Force JROTC instructor and the cybersecurity insight brought by Dan Wordell, Supervisor for Instructional Technology Support Center for Spokane Public Schools, Rogers was able to compete rather successfully last year. The All Service team made an appearance at the All Service qualifer in Orlando, Florida, and the Open Division team made it to the finals. (Prior to his position with the school system, Wordell worked for Lockheed Martin as a Cyber Security Project Manager.)

CyberPatriot wasn't just seen as a competition or an opportunity to learn about cyber-defense, but also as a nonathletic activity that would allow students to excel. And so it got a lot of attention in the school.

"The school administration picked it up and said this is an opportunity for the students to learn," Wordell said. "The kids ate it up, went wild with it, and were very motivated to learn about cybersecurity."

However, Wordell realized the students needed skills greater than his own and recruited other specialists for mentors.

They call it their "Mentoring Model," using an array of specialists to cover different topics of cybersecurity. Throughout the competition, the John R. Rogers teams have attended weekly (and sometimes biweekly) meetings, having mentors address different operating systems with the goal of giving their students the knowledge to build Linux and Windows servers from the ground up.

Wordell said, "Some mentors have put in over 150 hours across the district."

But it isn't only about mentors.

"We can, as mentors, provide fabulous instruction and checklists, but unless the students are able to work together as a team and execute their plan, they are going to fail," Wordell said.

There are several elements that led to their success.

"It's definitely a combination of the hours each team spent together, that they created a quality checklist and process to evaluate each operating system, and that they communicated very, very well as a team," he added.

But now these students aren't just peers, but are each other's competition.

"They are starting to look at each other differently," Wordell said. "Since all of the students have had the opportunity to be exposed to the same material, it will come down to the team at the nationals that keeps their composure and executes their plan the best."

U.S. Takes the Silver; Is That Really Good Enough?   By James Christy, DoD Cyber Crime Center

The U.S. Department of Defense Cyber Crime Center (DC3) has just finished its 6th Annual DC3 Digital Forensics Challenge, and by all measures conducted another successful contest. The original objective of the DC3 Digital Forensics Challenge was simple: to solve thorny real-world digital forensics issues that DC3 encountered in its Defense Computer Forensics Lab (DCFL). Launched in 2006, the challenge was for U.S. teams only, with the prize a modest plaque and a free trip to the DC3 annual DoD Cyber Crime Conference.

We almost immediately received requests to participate from several international teams the first couple of years so we let them compete for points only.

Our collective goal was to encourage and nurture young students to fill the ranks of the additional 30,000 cybersecurity practitioners, researchers, and warriors we needed in the U.S. government.

The first three years of the Challenge, the winners were obviously U.S. teams but everything changed in 2009. Below are the results.

International Challenge Teams
2009 – Results
   1 South Korea - undergraduate
   2 U.S. - Air Force Institute of Technology
2010 - Results
   1 South Korea – undergraduate
   2 South Korea - commercial
   3 U.S. - civilian
2011 - Results
   1 Turkey - graduate
   2 U.S. - undergraduate
   3 U.S. - commercial

Since we opened the competition to the international community, the U.S. has not won the Gold. In 2010 we had teams from eight different countries in the top 13 of the DC3 Challenge (South Korea, U.S., Turkey,

Password Security

By Eric Danner, CyberPatriot Program Office

If you're a frequent computer user, chances are you've found yourself annoyed when a program or website prompts you to change your password — *again*. And to make matters worse, because of password history policies, you often can't use passwords you've used in the past. Before you know it, you have a vast, complicated array of passwords that is difficult to keep straight.

After the Playstation network was hacked last year, and the CNET report that the Microsoft India site was hacked this past week exposing unencrypted personal information on the server, I paused to reflect on the implications of such events.

If the policies mentioned above didn't exist, there would be nothing to stop you from using the same password across all of your secured sites. If you did this (and some of us are no doubt guilty), and any of the sites on which you have an account is hacked, the perpetrators would have a pretty good idea of how to gain access to the other sites you use.

Suddenly, having to keep track of a few dif-

ferent passwords would seem like a small price to pay for your security; it's certainly less hassle than having to deal with the aftermath of identity theft.

There's an additional element to consider: password strength. While many sites require a certain degree of complexity, some do not. It's important to resist the temptation to pick something that's easy to remember — because this often means it's easier to crack. When I heard the report on CBS that the e-mail account of Syrian President Bashar al-Assad had been hacked by Anonymous, I was shocked to learn that the password for the account in question was "12345." I could hardly believe that anybody could be that naïve, but this type of thing happens literally every day.

Do yourself a favor: Take the time to pick strong, unique passwords for the various sites that you use. A bit of inconvenience now can save you untold hassles and headaches down the road.

Coaches' Corner

- **Participant Kits.** Please order your teams' participant kits at http://events.constantcontact.com/register/event?llr=ltxvdceab&oeidk=a07e5kgq6y34b8a2b8e
 Thank you to those who already ordered their kits!

- **National Finals Coaches**—National Finals coaches please pay special attention to competition details in your e-mail. More competition information will be sent to you in the next few weeks.

Answer to Monthly Question

The answer is: *It depends on the source.* According to M-W.com, one definition of a hacker is: a person who illegally gains access to and sometimes tampers with information in a computer system.

In the cybersecurity field, definitions generally are applied to the skill level and intent of a person. Below are informal definitions from the cybersecurity "street."

Hacker - a highly skilled computer programming, networking, or systems enthusiast who enters systems with *no* malicious intent. A hacker may program a network or system to improve it, debug it, or to learn its nuances. In the early days of computing, hackers were highly regarded.

Cracker - a person with skills like the hacker, but who uses unauthorized or illegal access with malicious intent. Crackers take information from, tamper with, or cause damage to a system or network.

Script Kiddy/Kiddie - an immature cracker who uses existing tools to find and exploit weaknesses in other computers on the Internet—without consideration or understanding of the potentially harmful consequences of their actions**.**

U.S. Takes the Silver (Cont'd)

Australia, Sweden, Italy, Hungary, India). Again, in 2011 the top team was not a U.S. team. It was an individual graduate student from Turkey that won the Gold. Our team was initially very elated at the success and the global participation in the DC3 Challenge. We were very proud for about 10 minutes until we realized that the U.S. had captured only the Silver! For the third straight year, the U.S. didn't score the Gold in our own global contest. South Korea had captured the Gold for two years running and now a Turkish graduate student had won!

Immediately, the sports metaphor came to mind. The U.S., the only remaining world super power and leader in technology and everything cyber had finished only 2nd! If this were the Summer or Winter Olympics and the U.S. finished only capturing the Silver or the Bronze, would Americans be disappointed? Outraged?

I respectfully suggest we are in a Cyberspace Race today and our national pride and national security rests on our success. I would hope that the same disappointment we would feel as a nation if our Olympic Team finished 2nd or 3rd and the same determination and effort to reach the moon first while trailing in the Space Race would now apply to the current Cyberspace Race. Are you disappointed? Are you outraged? Or is Silver or Bronze good enough?

(Note: DC3 will conduct the forensics portion of the National Finals Competition.)

Northrop Grumman Seeks Cyber Interns

As presenting sponsor of CyberPatriot IV, Northrop Grumman is cultivating the exceptional talent exhibited by competitors throughout the year by offering summer internship opportunities to qualified students.

Students can put their CyberPatriot skills to the test in a real life cyber environment, working side-by-side with Northrop Grumman cyber pros to help develop innovative cyber solutions for intelligence, defense, and civil/federal agencies. Positions are already posted in the Northern Virginia area; Annapolis Junction and Columbia, Maryland; and Aurora, Colorado with more positions coming soon.

"Our CyberPatriot high school competitors are an extremely valuable part of the Northrop Grumman workforce," said Diane Miller, Northrop Grumman Program Director for Cyber-Patriot. "Building the pipeline of qualified cyber pros is a national imperative and we are doing our part to fill the pipeline and keep America's networks safe."

Last year, the company hired 11 CyberPatriot students and expects to grow that number in 2012. One returning internship opportunity is called "CyberCell." Here, eight students worked on a company-funded cyber modeling and simulation research project that challenged the students' ability to understand how attackers can penetrate a network. "We set an aggressive schedule with some "stretch-goals" just in case. Our interns blew us away, meeting deadlines ahead of schedule and asking for more challenging tasks," said Amy Tsao, system engineer, Northrop Grumman Information Systems.

Basic requirements to participate include proof of U.S. citizenship, must be 16-years of age or older, GPA of 3.0 or higher, have participated in CyberPatriot, and currently enrolled and attending a high school.

Northrop Grumman has designed a career site to explore job opportunities and get advice about your career path. For more information, go to http://careers.northropgrumman.com/cyberpatriot.html

Sponsors:

Commissioner's Cache (Cont'd)

Our friends from Canada will hold an international exhibition competition in conjunction with our U.S. competition. This year promises the best competition yet. Thank you for your role in it. (Oh, as you no doubt noticed, our newsletter now has a name. Thanks to all of you who participated in the "Name This Newsletter" contest, and congratulations to Caitlin Albright of the Anoka County, Minnesota Composite Squadron Team, Civil Air Patrol, for the winning entry!)

Bernard K. Skoch
Commissioner
CyberPatriot Program
Air Force Association

Presenting Sponsor:

NORTHROP GRUMMAN
Foundation