Air Force Association's
CYBERPATRIOT
National High School Cyber Defense Competition
presented by NORTHROP GRUMMAN Foundation

The CyberSentinel

Commissioner's Cache

We at the CyberPatriot Program Office hope you are enjoying a great summer. We are, and we are fast at work preparing for CyberPatriot V. This month we are excited to announce our new competition software: The CyberPatriot Competition System (CCS). CCS will complement SAIC's CyberNEXS, which has powered our competition and will continue to be a critical part of our program. Also, our rules book is under development and will be released later in the summer. It will be the authoritative source for the CyberPatriot competition, and we know you will benefit from a good look at it when it comes out. Congratulations to Hamza Siddiqui (from University High School in Orlando, Florida), who created the winning entry in our CyberPatriot Poster contest! Thank you to all who participated. With all the positive changes in CyberPatriot, we are sad to note that the tenure of the program's earliest and strongest leader and supporter, AFA President and CEO Lt. Gen. Mike Dunn (USAF, Ret.), is drawing to a close. General Dunn oversaw the development and expansion of CyberPatriot, and through his brilliant visionary leadership and engagement with industry and government leaders he significantly contributed to the National High School Cyber Defense Competition. We wish General Dunn well as he moves on to bigger and better things. As you can see, there is a lot going on, so please stay connected. See you back here in August!

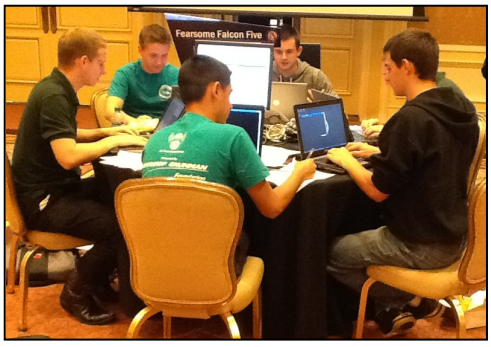
Bernard K. Skoch
Commissioner
CyberPatriot Program
Air Force Association

Program Office Bits

CyberPatriot V Coach and Mentor Registration is Open!

Go to: www.uscyberpatriot.org

- Coaches' Online Meetings: Aug. 14 and 15, 2012
- Coaches' registration ends Sept. 30, 2012
- Students must be entered into the team websites by Oct. 26, 2012
- Team registration payments are due Oct. 31, 2012
- Competition dates for CyberPatriot V can be downloaded at: http://www.uscyberpatriot.org/CP5/CP%20V%20Documents/CPV_Competition_Sked.pdf



Clearfield High School's "Fearsome Falcons" competing at the Utah Cyber Defense Challenge. The team took first place against college and industry teams. ***(See Page 2.)***

Elevators to BMWs: Major New Cybersecurity Flaws Found

By Alison Fang Yuen, Assistant Editor

Imagine this: Your air conditioning doesn't work, you can't set the alarm in your apartment, the elevator stopped working, and to top it all off, your car has been stolen.

This scenario is not as far-fetched as you might think. Recently the press reported major security flaws with infrastructure and automobiles.

The Tridium Corporation's Niagara Framework was supposed to be a secure way to link companies together and to the Internet; it supports over 11 million devices in 52 countries. From security and surveillance to elevators to personnel trackers to medical equipment, many devices use Niagara.

However, the *Washington Post* examined the network and found an unknown number of Niagara-run networks are vulnerable to hackers. Following the discovery, Tridium released a bulletin to warn customers about the vulnerabilities and how to limit them.

The *Washington Post* stated, "[The situation] demonstrates how even small missteps in writing software or configuring systems can have huge implications. In cyberspace, determined hackers routinely transform obscure gaps into major security holes." Click here for the *Washington Post* article.

Though it is unknown if the security holes in Niagara are being exploited, NBC.com reports that car thieves in the United Kingdom are using them to steal BMWs.

Hackers plug blank key fobs into a car's OBD (On-Board Diagnostics) port and download the car's unique digital ID. Using that ID, the thieves are able to drive off with the car without activating alarms or immobilizers. To read the rest of the NBC.com article click here.

But there is good news: BMW is working with other manufacturers and authorities to fix the OBD loophole.

Billy Rios and Terry McCorkle, a pair of security researchers found holes in Niagara that would allow

(Continued on Page 4.)

This Month's Question

Is my cell phone open to an attack the same way a computer is?

(The answer appears on Page 4.)

Features

Page

CyberPatriot to Introduce New Competition System in CP-V

CyberPatriot V will have a new competition system to complement SAIC's CyberNEXS (Cyber Network Exercise System) which powers CyberPatriot. The CyberPatriot Competition System (CCS) was developed by CIAS for the CyberPatriot National High School Cyber Defense Competition.

The new CCS software will be introduced to competitors during the combined practice round, October 1 - 12, 2012. Then CCS will be used in rounds 1, 2, and 3.5 (Consolation Round). Round 3 (Semifinals) and the National Finals Competition will be powered by CyberNEXS.

CCS requires Internet access to report scores. Competitors will receive immediate feedback from CCS on their performance. A screenshot of the scoring report is shown to the right.

Training documents for CCS will be under the "CyberPatriot Training Materials" link under the "CyberPatriot V" tab at www.uscyberpatriot.org.

Competitors using CCS will use the same business rules as used in previous years— find and fix vulnerabilities.

More info on CCS will be presented at future coaches' meetings.

AFA President and CEO Lt. Gen. Mike Dunn (USAF, Ret.) will step down from his post on July 31st. He was a major supporter of CyberPatriot and due to his engagement and visionary leadership, CyberPatriot grew exponentially. (See Commissioner's Cache on Page 1.)

Clearfield Falcons Soar to First Place at Utah Competition

Salt Lake City— The Clearfield High School AFJROTC CyberPatriot team, the *Fearsome Falcons*, defeated college and industry teams to walk away with first place at the first Utah Cyber Defense Challenge.

The State of Utah hosted the Cyber Defense Challenge, with the support of one of CyberPatriot's Founding Partners, SAIC, and local corporations, to increase involvement in the cybersecurity field. The live network defense competition was held to challenge the skills of corporate cyber professionals and college cyber teams. However, officials were excited to have the Clearfield High School Falcons join the competition.

The AFJROTC cadets defeated teams such as Brigham Young University, which took second place, and a Utah Information Security team that took third place.

With a virtual qualifying round, the Falcons were one of seven teams to advance. The competition was a live six-hour event. Each team managed eight networks while under attack by a red team. In what was a very challenging and close competition, the Clearfield Cadets shocked the room by winning. "We may have had a little home field advantage," stated retired Major Kit Workman, the Clearfield coach. "The kids [had] experienced the CyberNEXS software before, and have competed as a team, but we never imagined being able to compete [with], let alone beat, college teams and cyber professionals. It speaks volumes about our kids, and especially our coach, Mr. Dave Boswell, from SabiOso Inc. in Clearfield."

Because three seniors from the CyberPatriot team were graduating, the team had been searching for another competition after taking third place in CyberPatriot IV's National Finals Competition in March. Then the opportunity came to participate in the first Utah Cyber Challenge in June. The challenge was part of the inaugural Utah Cyber Defense Challenge and Symposium.

The symposium was designed to bring the industry, education, and government cyber communities together to help direct Utah's cyber future. Central to the event was the Utah Cyber Defense Challenge powered by SAIC's CyberNEXS network defense software.

CyberPatriot is also powered by CyberNEXS which supports competitions around the country.

Additionally, the cadets will have one more opportunity to compete as 2012 team. Their victory qualified the Falcons to participate in the 2012 Global CyberLympics, a worldwide virtual cyber competition that started this month.

Congratulations to Cadets Braxton Allen, Daniel Hargrave, John Maxfield, Hunter Poe, Eric Takacs, and Preston Boss who competed in the Cyber Defense Challenge. Good luck in the CyberLympics! — Edited by Alison Fang Yuen

"Fearsome Falcons" Cadets Braxton Allen, Daniel Hargrave, John Maxfield, Hunter Poe, Eric Takacs and Preston Boss (Boss is not pictured above) competed in the Utah Cyber Defense Challenge. The photograph is of the team at the CP-IV National Finals Competition, where they won third place in the All Service Division.

CyperPatriot now exceeds 500 teams. To check out the article about it, go to: http://www.afa.org/media/press/cp_500_milestone.asp

The CyberSentinel

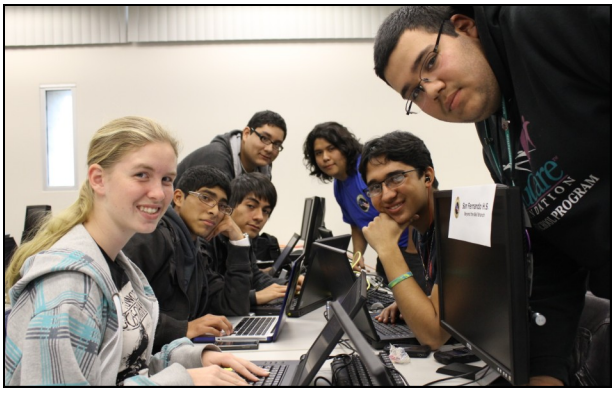
Publisher Bernard K. Skoch

Editor Francis S. Zaborowski

Assistant Editor Alison A. Fang Yuen

CyberPatriot Program Office
•1501 Lee Hwy Arlington, VA 22209 • www.uscyberpatriot.org
•E-mail: info@uscyberpatriot.org • Telephone: 877.885.5716

Spotlight on Los Angeles Unified School District (LAUSD)



***LAUSD CyberPatriot Teams:* San Fernando High School (left) and Reseda High School NJROTC (right).** *San Fernando will compete this year in CyberPatriot V's Open Division. Reseda was in the All Service Division and competed in the CyberPatriot IV National Finals Competition.*

LAUSD Intensifies Academic Support/Training

By Carey Peck, Beyond the Bell Program

CyberPatriot V is rapidly approaching and the Beyond the Bell (BTB) Branch of the Los Angeles Unified School District (LAUSD) has been stepping up the professional and academic support made available to its CyberPatriot teams.

The LAUSD landed two teams in the finals of CyberPatriot III and CyberPatriot IV. The district's goal is to send two or more teams to the finals every year. There are some excellent contenders and it will be difficult as BTB teams have yet to claim a medal.

This year, district teams will receive more training, more professional and academic support, especially through its affiliation with CyberWatch West (CWW), and an increased number of professional and industry contacts. CWW is a consortium of West Coast schools that have received multiyear funding from the National Science Foundation and Department of Homeland Security. The goal of the consortium is to increase the development of computer security courses in member institutions and to develop student outreach program. The program aims to develop secondary system students who are primed for careers in cybersecurity. The target is to bring students and academic/industry contacts together. That fits the bill for the LAUSD teams!

During the summer, the LAUSD teams have been studying course materials developed in conjunction with lead partner California State Polytechnic University. The materials include Internet study courses, past years' CyberPatriot competition images, and study courses specifically developed by LAUSD and Cal Poly's staff and consultants. These materials allow the teams to develop their skills, to study the systems they will have to master for the competition, and to practice with old competition images.

On the consultant side, BTB teams are able to develop new professional contacts with security firms, and with LAUSD system operators, to study systems security from the operational viewpoint and to learn techniques from people on the front lines. One of the consultants, Nicole, just landed a new position with SpaceX, and she will be returning for her third year to tutor BTB teams on the Linux operating system.

The success of BTB CyberPatriot teams has generated some buzz. Some of the national finalists of previous years returned to coach their school teams, and some campuses have doubled their program size. It seems that everybody has seen the photos and wants that trip to D.C.. Franklin High has been to the finals twice and will launch three teams to compete this year. North Hollywood has six teams, and Kennedy High has four, but more will come. This excitement and recruiting power will shine in the competition come fall. BTB is eagerly looking forward to another exciting year in the cyber defense competition!

LAUSD is a CyberPatriot Center of Excellence. *Nearly 50 LAUSD area teams participated in CP-IV, of which, two teams competed in The National Finals Competition.*

The Benjamin Franklin High School team competing in the CyberPatriot IV National Finals Competition. Franklin High School is part of LAUSD'S BTB.

About Beyond the Bell

The LAUSD Beyond the Bell Branch's goal is to "...ensure that all children and youth in LAUSD have access to high quality, safe, and supervised academic, enrichment, and recreation programs that inspire learning and achievement beyond the regular school day (before and after school and Saturdays)." (Source: Los Angeles Unified School District Beyond the Bell Branch's Web site.) If you would like to learn more about the Beyond the Bell Branch, visit their Web site at: btb.lausd.net/about/

Answer to Monthly Question

The answer is: Yes. As cell phones have advanced, they have become less like phones and more like computers. While these advancements provide increased features and functionality, they also introduce new risks. Attackers use these advancements to target devices previously considered safe. Any electronic equipment that uses some kind of computerized component is vulnerable to software imperfections and vulnerabilities. This expands the list of susceptible devices to tablets, video games, car navigation systems and many more. If the device is able to connect to the Internet or a network, the risks increase. To find out ways to protect your devices go to: http://www.us-cert.gov/cas/tips/ST05-017.html.

University of Maryland and Northrop Grumman Create Nation's First Cybersecurity Honors Program for Undergraduates

Building on the company's commitment to STEM and cyber workforce development, Northrop Grumman and the University of Maryland announced in June they will launch a landmark honors program designed to educate a new generation of advanced cybersecurity professionals. The unique program, Advanced Cybersecurity Experience for Students (ACES), will immerse undergraduate students in all aspects of the field to meet growing manpower needs in the nation and the State of Maryland.

ACES will engage a highly talented, diverse group of students—majors in computer science, engineering, business, public policy and the social sciences—in an intensive living-learning environment that focuses on the multifaceted aspects of cybersecurity and develops team-building skills. Students will take on an advanced, cross-disciplinary curriculum developed through industry consultation, and will interact directly with industry and government cybersecurity mentors. Students enrolled in the program will have the option of interning with Northrop Grumman and preparing for security clearance. ACES will produce skilled, experienced cybersecurity leaders highly sought by corporate and government organizations.

Finding employees fully prepared to take on complex cybersecurity issues is a major challenge for corporations and government agencies. Northrop Grumman's Chairman, Chief Executive Officer and President Wes Bush said, "We are fully committed to developing solutions to help eliminate the nation's shortage of critical STEM-educated talent, and by partnering with the University of Maryland, we will address workforce challenges in the increasingly important field of cybersecurity. The university has an outstanding track record for developing innovative educational programs to answer real-world needs, excellent research capabilities through its Maryland Cybersecurity Center, and close relationships with the many federal agencies and corporations in the Washington, D.C., area likewise concerned about cybersecurity."

Northrop Grumman will provide a grant of $1.1 million to launch the program, which is slated to accept its first students at the College Park campus in fall 2013. Over time, through distance education programs, online course offerings, transfer of students, and competitions, universities across the University System of Maryland will participate in the program.

For more about the program, go to http://www.irconnect.com/noc/press/pages/news_releases.html?d=258752.

Major New Cybersecurity Flaws Found (Cont'd)

(Continued from Page 1.)

hackers to download and decrypt user names and passwords. According to the *Washington Post* article, their findings were shared with the *Post* and given to cybersecurity officials at the Department of Homeland Security who then advised various measures to Tridium, such as security training for clients.

Known and unknown vulnerabilities may be present in the software that manages the devices we use day to day. Hackers can exploit the vulnerabilities to steal account and personal data. However, through good cyber security principles learned in CyberPatriot, we can make it difficult for hackers to enter programs.

Coaches' Corner

- **CyberPatriot V Coach Registration**. CyberPatriot V Coach Registration is open at: www.uscyberpatriot.org. Coaches must be *registered and cleared* before their teams may register.
- **Coaches' Online Meeting** will be held in three 45-minute repeat sessions on August 14 and 15 at different times to accommodate different time zones and work schedules. Check your e-mail in mid-August for details.
  To access the July Coaches meeting click here or go to www.uscyberpatriot.org/CP5/CP%20V%20Documents/Coaches%27Meeting_17_18July2012.pdf

CyberPatriot Poster Contest Winner

Hamza Siddiqui

from University High School (in Orlando, Florida) is the winner of the "CyberPatriot Poster" contest. Hamza will receive an iPod shuffle.

Thanks to all of you who entered the contest. It was difficult to choose a winner out of all the great posters we received.

Sincerely,

Frank Zaborowski
Editor