CYBERPATRIOT
INTEGRITY SERVICE EXCELLENCE
NATIONAL HIGH SCHOOL CYBER DEFENSE COMPETITION

[Name this Newsletter]

Issue 0001
January 2012

and win an Apple iPod Shuffle
or an iTunes gift card!
(See page 4 for details.)

Commissioner's Cache

This is our first issue of the CyberPatriot Bulletin. We hope you enjoy it. It will be published on a regular basis to update you on CyberPatriot news and cybersecurity information. In this month's issue, you will find articles on our nation's blueprint for a secure cyber future, on "phishing," on cyberbullying, and on other great topics. If you have any suggestions to improve the bulletin, please e-mail them to info@uscyberpatriot.org.

As we move into the final rounds of CyberPatriot IV, I want to thank all of you -- competitors, coaches, mentors, and supporters -- for the time you invested in our competition and each other. Each team is a part of a greater community of well-trained Cyber Citizens. And with each competition, we grow together. We can have the best network security software and hardware, but they are useless, without trained people.

(Continued on Page 3)

Upcoming Events

- January 27-28 Round 3 Open Division (Online)
- March 22-23 National Finals (Washington, DC)

Program Office Bits

- **Participant Kits**—Great news! Participant kits are almost ready to ship. Each participant in CyberPatriot IV will receive a bag, coin, and T-shirt with the CyberPatriot logo. Details will follow in next month's bulletin!
- **Scorebot** — If during competition, your "Get_My_Status.html" scorebot is not updating, do not worry! Continue working on the image. The page will refresh when server connectivity is re-established.

Blueprint for a Secure Cyber Future

The electricity in our homes, our bank accounts, and mass transit systems are some of the things that rely on our nation's cyber infrastructure. If our cyber infrastructure is not reliable, our daily way of life would be easily affected by manmade and natural causes.

November 2011, the Department of Homeland Security (DHS) released its "*Blueprint for a Secure Cyber Future*." The strategy in the document is designed to protect the critical systems and assets that are vital to the United States from criminals and other nations. If our critical cyber systems are degraded, the DHS plans to have processes and resources in place to minimize the effects on us.

What the *Blueprint* means to us is that the U.S. government is focusing its efforts on people, processes, and developing technologies to ensure we have a safe and secure cyber environment. A few excerpts from the *Blueprint* are listed below.

The *Blueprint* lists four goals for protecting critical information infrastructure:

- Reduce exposure to cyber risk
- Ensure priority response and recovery
- Maintain shared situational awareness
- Increase resilience

The *Blueprint* also lists four goals for strengthening the cyber "ecosystem":

- Empower individuals and organizations to operate securely
- Make and use more trustworthy cyber protocols, products, services, configurations and architectures
- Build collaborative communities
- Establish transparent processes

To see the entire document, go to:

http://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf

This Month's Question

What is a "checksum," such as that used in MD5?

(The answer appears on Page 3.)

Features

• Air Force Association/ CyberPatriot Program •
1501 Lee Hwy Arlington, VA 22209 • www.uscyberpatriot.org •

Social Engineering and Phishing Attacks

Have you received an e-mail from a bank requesting that you update your account information, but you did not have an account with that bank? If so, you were the target of social engineering, known as phishing.

Social engineering is a technique frequently used by attackers to cause a person to divulge information or to unknowingly allow entry to a system. Normally, an attacker poses as a person or organization familiar to the individual. Then the attacker solicits information or entry. Social engineering is not limited to the Internet.

Phishing is a specific form of social engineering, using e-mail or Web sites to solicit personal information such as credit card or social security numbers. In the past, phishing attackers have pretended to be PayPal, banks, and humanitarian organizations. Inevitably, the attacker requests a credit card number or other personal information.

To avoid becoming a victim of social engineering or a phishing attack, the U.S. Computer Emergency Readiness Team (US-CERT) recommends: "Do not give sensitive information to anyone unless you are sure that they are indeed who they claim to be and that they should have access to the information."

Some ways to avoid phishing attacks are:

- Do not communicate with a person in distress who offers you money for "safe keeping."
- Check hyperlinked URL s to ensure they link to a legitimate institution. (If a foreign nation's domain, (e.g., .tv, .kr, .ch, .ru, etc.) appears for a U.S. company or organization, the link is likely a phishing attack.)
- Go directly to a bank's or organization's Web site without using a hyperlink from an e-mail or other Web site.

The bottomline: If it is too good to be true, then it is probably too good to be true.

If you believe you are a victim of a phishing attack, immediately contact the institution(s) involved.

For more information, see the US-CERT's National Cyber Alert System Cyber Security Tip ST04-014 at:

http://www.us-cert.gov/cas/tips/ST04-014.html

Software Piracy: Big Consequences

Sharing software with your friends is a good thing, right? Well, not when it lands you in jail. What you may not realize is that this seemingly innocent act can draw the attention of federal law enforcement.

According to www.marketwatch.com, in December 2011, the Federal Bureau of Investigation (FBI), working with over a dozen state police forces and Canadian law enforcement, arrested 31 people for pirating Rosetta Stone language training software. Earlier in the year, Rosetta Stone reached a settlement with 119 people accused of copyright or trademark infringement. (For the full story, see the link at the end of the article.)

These people were most likely not considering the consequences of what is a seemingly victimless crime. However, these people now face a best-case outcome of hefty fines, and a worst-case of criminal charges at the federal level.

Beyond the moral dimension of software piracy, it is important that we consider the potential legal consequences. Failing to do so can lead to the kind of trouble that haunts you for literally the rest of your life.

Unless someone wants to explain in every job interview or college application how they came to be arrested by the FBI, they should think twice before lending out an install disc or product key.

http://www.marketwatch.com/story/rosetta-stone-commends-law-enforcement-for-31-piracy-arrests-and-announces-119-civil-settlements-for-copyright-violations-and-illegal-software-distribution-2011-12-19

How's your "netiquette?"

"Netiquette" stands for "Internet Etiquette." It refers to a set of practices created over the years to make the Internet experience pleasant for everyone. Netiquette has been around since 1983 and adapted for the Internet.

There are many rules of netiquette but some important ones to remember are:

- Think before you post.
- Be honest.
- Would you say it to the person's face?
- Your family or future employer may be reading!

CyberPatriot Newsletter

Publisher
Bernard K. Skoch

Editor
Francis S. Zaborowski

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

Commissioner's Cache (Cont'd)

Our program differs from other types of competitions, where the goal may be to infiltrate networks , control networks, or compromise information. We seek purely to teach defending networks by closing network and system vulnerabilities. We regularly see and hear that our nation's networks are under constant attack. During the CyberPatriot Competition, we develop the skills to defend our networks from those attacks.

As network defenders, we set the standard for online activity. Not only do we practice good cybersecurity, but we are examples for our fellow network users. Compromising other people's information, cyberbullying, and other attacks are against what we stand for. The Internet should be a safe place to conduct business or to interact with friends. And we can help make it that way. Please read the CyberPatriot Competitor Code of Conduct, elsewhere in this issue, to familiarize yourself with our program's values and as a basis to teach others about good Cyber Citizenship.

Again, thanks for your investment in the CyberPatriot Program. People are our most valuable asset and that is you!

Bernard K. Skoch
Commissioner
CyberPatriot Program
Air Force Association

Coaches' Corner

- **Participant Kits**. Thank you for registering your students on your team site. Check for an e-mail soon regarding participant kits.
- **Air Cards**—The Program Office processed shipping labels for the return of the air cards. If your team is no longer competing and you have not received a shipping label, please contact the Program Office.

CyberPatriot Competitor Code of Conduct

1. I will consider the ethical and legal implications of my online actions every time I participate in CyberPatriot.

2. I will not conduct, nor will I condone, any actions that attack, hack, penetrate, or interfere with another team's or individual's computer system, nor will I use the cyber defense skills I learn in CyberPatriot to develop hacking or other offensive skills.

3. I will not illegally copy or distribute software or other intellectual property.

4. I will not visit inappropriate Web sites while preparing for or participating in CyberPatriot .

5. I will not participate in or condone cyberbullying which includes such behaviors as teasing, threatening, intimidating, humiliating, sexual harassment, racial harassment, and stalking.

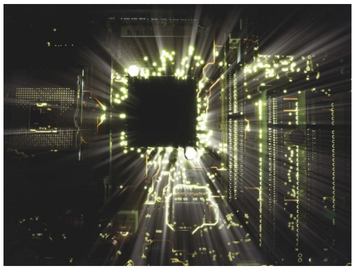
6. I will follow the CyberPatriot rules of competition and will accept appropriate guidance from my coach.

7. I will not tamper with, modify, or attempt to manipulate any element of the CyberPatriot competition or scoring systems.

8. I will not attempt to deceive, hoax, or "prank" other teams by forwarding or posting erroneous or deceptive information on the Internet, by e-mail, or on social networking sites.

9. I understand that violation of this code of conduct is grounds for my immediate dismissal from my team and the disqualification of my team from CyberPatriot competition.

10. I will strive to use my participation in CyberPatriot to further my understanding of cybersecurity.



Answer to Monthly Question

A checksum is an algorithm (method) for checking the integrity (completeness) of a received block of data. To understand how a checksum works, it may be helpful to look at its history.

In the pre-digital age, navigators used the checksum on radio and teletype, to check location messages for errors. They posted sums after the latitude and longitude cardinal direction. For example: 38°53'42"N133 (38+53+42=133)

Sometimes the checksum was abbreviated as the last number of the checksum (e.g., 38°53'42"N3).

If the numbers did not add-up to the checksum, then a navigator knew the location was in error and requested a retransmission of the location message from the originator.

In the same way, if the MD5 checksum does not match your downloaded image file's checksum, then you would download the image, again or request a new image file.

Cyberbullying

In the past few years, cyberbullying has made news headlines. Sadly, that was due to suicides attributed to it. In the CyberPatriot Program, we want to be cyber leaders and stop cyberbullying whenever possible.

The US-CERT Cyber Security Tip ST06-005 refers to cyberbullying as “the practice of using technology to harass or bully someone else.” Further, the tip states that "forms of cyberbullying can range in severity from cruel or embarrassing rumors to threats, harassment, or stalking.”

Moral courage is required to break the cycle of cyberbullying and the pain it causes. If you know of a cyberbullying act, then it is up to you to take action. Let your parents or another responsible adult know what is happening. And let the bully know that their on-line harassment of another person is wrong, no matter if the harassment seems funny or deserved.

To find out more about cyberbullying and what you can do to help stop it, please see the US-CERT Cyber Security Tip ST06-005 at:

http://www.us-cert.gov/cas/tips/ST06-005.html

Northrop Grumman - Grooming Tomorrow’s Cyber Workforce

The Northrop Grumman Foundation is thrilled to be serving in its second year as presenting sponsor of the Air Force Association’s CyberPatriot program. As the largest cybersecurity provider to the federal government, we know the importance of employing highly skilled cyber pros to defend and protect our nation’s critical assets.

Grooming tomorrow’s workforce is a top priority at Northrop Grumman. CyberPatriot is one of several STEM outreach opportunities the company is engaged in to help meet the ever-growing demand for cyber pros.

“With the dearth of cyber talent in the U.S., programs like CyberPatriot are essential to filling the gap and building excitement around this career path,” said Diane Miller, Northrop Grumman Program Director for CyberPatriot. “The students are so impressive, exhibiting critical thinking, leadership, and teamwork skills that will be instrumental to their success as a cyber defender.”

CyberPatriot competitors are a valuable part of the Northrop Grumman workforce. Last year, the company hired 11 high school students and expects to grow that number in 2012.

Winning CyberPatriot also has many rewards. Last year, Northrop Grumman presented $54,000 in scholarships to 36 students on the winning teams at the National Finals Competition, helping tomorrow’s cyber defenders take the next step in their education.

Northrop Grumman employees are actively engaged and proud to lend their support as technical advisors for the program. “We’re reaching out to high schools in our local communities and dedicating time, talent, and resources to make CyberPatriot a success,” added Miller.

For more information about Northrop Grumman career opportunities, go to http://careers.northropgrumman.com/pdfs/NorthropGrummanCyberSecurity.pdf

Editor’s *“Name This Newsletter”* Contest

Win an Apple iPod Shuffle
or a $50 iTunes gift card!

Welcome to our newsletter! Like all new things, our newsletter needs a name. Our newsletter should have a name that reflects the spirit of the CyberPatriot Program. I invite you to submit a name for the newsletter in the “Name This Newsletter” contest.

To make it worth your while, the winner of the contest will receive an Apple iPod Shuffle or a $50 iTunes gift card!

To enter the contest, please send an e-mail to:
NameThisNewsletter@uscyberpatriot.org

with a subject line of:
Newsletter Contest (Type Your Last Name Here)

In the body of the e-mail, use the following format:
Name:
CyberPatriot Team:
Mailing Address:
E-mail Address:
Suggested Newsletter Name: (No more than 22 characters and spaces.)

The deadline for entries is midnight EST, February 5, 2012. The CyberPatriot Program Office will choose a newsletter name from entries received by the deadline. In the case of identical entries of the winning newsletter name, the winner will be chosen by a drawing of the entrants’ names who submitted the winning name .

Thanks!

Frank Zaborowski
Editor

Presenting Sponsor:

NORTHROP GRUMMAN
Foundation

Sponsors:

SAIC From Science to Solutions · CIAS Center for Infrastructure Assurance and Security UTSA · BOEING · URS · Raytheon · LINCOLN LABORATORY Massachusetts Institute of Technology 244 Wood Street, Lexington, MA 02420-9108 · CISCO · Microsoft imagine cup · GENERAL DYNAMICS Advanced Information Systems · at&t