Proceedings of the 14th Colloquium for Information Systems Security Education
Baltimore Marriott Inner Harbor
Baltimore, Maryland June 7 - 9, 2010

Developing a National High School Cyber Defense Competition

Gregory B.White, Ph.D., *UTSA*, Dwayne Williams, *UTSA*, and Keith Harrison, *UTSA*

Abstract – The Cyber Patriot National High School Cyber Defense Competition has completed its second pilot year. Results have been very promising with 170 schools participating in the 2009-2010 school year. Much, however, still needs to be accomplished in order for the competition to be a truly national competition. This paper will discuss the Cyber Patriot program, what has been accomplished, what is planned, and what is needed for it to be a national program. The paper will also discuss the ties between this program and the National Collegiate Cyber Defense Competition and how the relationship will benefit the competitions specifically and the state of cyber security education in general.

Index terms – Computer Security, Competitions, High School

I. Introduction

The United States is facing what some security experts have described as a "radical shortage" of cyber security professionals. [1] Efforts to attract more individuals to this critical career field have largely been focused at the collegiate level. Initiatives such as the DHS/NSA sponsored National Centers of Academic Excellence in Information Assurance Education as well as competitions such as the National Collegiate Cyber Defense Competition and the service academy's Cyber Defense Exercise have been developed to encourage faculty members and to attract college students to consider a concentration in this field. While tremendous programs, reaching out to students at only the college level limits the number of potential recruits as many at this age have already selected their chosen major. Instead, what is needed is a program that will reach into the nation's high schools to capture the interest of students when they are beginning to consider their possible future career goals.

The Cyber Patriot National High School Cyber Defense Competition was designed to address the nation's shortage of cyber security professionals by introducing high school students to the career field. The goal is to excite students about cyber security, and to motivate them to consider pursuing a career in the field. Even if the student competitors decide to major in a different field, the hope of the developers of Cyber Patriot is that they will have learned enough about cyber security to positively impact their use of computer systems and networks by making them more aware of what they need to do to ensure the security of their own or their employer's systems. The Cyber Patriot program is now entering its third year and is gaining momentum with a growing number of high schools anxious to participate.

II. Other Cyber Security Competitions

The Cyber Patriot National High School Cyber Defense Competition is not the first or only cyber security competition. In fact, it is not the only attempt at developing a competition aimed at the high school level. Most of the well-known competitions, however, are aimed at an older audience with a number of collegiate competitions in existence.

One of the earliest and best known computer security competitions is the capture the flag (CTF) competition at DEFCON. The first competition was held at DEFCON I in 1993 and the competition is currently in its 18th year. Competing teams are selected using a security related qualifier. The DEFCON CTF competition has both offensive and defensive aspects. Although the specific rules change yearly, typically each team is given servers to defend while trying to compromise the other teams' servers [2,3].

The United States Military Academy created the Cyber Defense Exercise (CDX) in 2001 in order to fill the CAPSTONE requirement for their information assurance course. The CDX is a distributed, wide-area competition created using VPNs [4]. The CDX is currently sponsored and designed by the National Security Agency/Central Security Service (NSA/CSS). In 2009 eight teams participated in the CDX including, for the first time, the Royal Military College of Canada. The CDX is a defensive only competition, meaning that each team is responsible for defending their own network against a team of attackers known as the Red Team. Offensive actions against other teams, including the Red Team, are

Dr. White and Mr. Williams are members of the Center for Infrastructure Assurance and Security in the Institute for Cyber Security (ICS-CIAS) at The University of Texas at San Antonio (UTSA). Dr White is also an Associate Professor of Computer Science. Mr. Harrison is a Ph.D. student in the Department of Computer Science at UTSA.

prohibited. Each team is given a computer network with common services designed to simulate the network of a business. The teams must work to secure their network and services while staying within budget [5].

In 2004 the University of California at Santa Barbra began hosting the iCTF, an international/intercontinental academic capture the flag competition. The iCTF is designed to be a distributed, wide-area security exercise with both offensive and defensive aspects. The teams are given identical virtual hosts. Each team is responsible for defending their own hosts' services while attacking the services of other teams. Originally the iCTF was loosely based the DEFCON CTF competitions with modifications to make it geographically distributed. In 2009, 56 teams and more than 800 students participated in the iCTF [6].

The National Collegiate Cyber Defense Competition (NCCDC) is organized by the Center for Infrastructure Assurance and Security (CIAS) at the University of Texas at San Antonio. The first Collegiate Cyber Defense Competition (CCDC) was held in 2005 for the southwestern region only. Currently the CCDC is organized into eight regional competitions with the winners going on to compete at the NCCDC [7].

At the NCCDC all teams compete at the same location. All teams are given identical networks of hardware and identical software including operating systems and business critical services. Each competing team must work to defend their network against a team of attackers known as the Red Team. The winning team at the NCCDC is the team with highest score at the end of the three day competition. Teams gain points by keeping business critical services up and running and by completing business injects. Teams lose points when they are compromised by the red team and when their business critical services are down for an extended period of time. Business injects are security related tasks given to the teams by a simulated management and are scored by the White Team. The NCCDC scoring engine is responsible for determining if the teams' services are running and properly configured. The Red Team takes extra care to attack all teams equally and in the same manner and to report successful intrusions to be used in scoring [8,9].

The IT-Olympics competition is the capstone for the IT-Adventures operation created for high school students by Iowa State University, The Iowa State Government, and Iowa businesses. The IT-Olympics are a two day competition in which students compete in cyber defense, game design, and robotics [1]. For the cyber security portion of the competition, teams are given remote access to computers approximately one month before the competition and physical access to the machines are given on the first day of the competition. Student teams, or Blue Teams, must setup and secure services, operating systems, and possibly wireless network access. On the second day of the competition the Red Team, graduate students and IT professionals, begin penetration testing the teams' networks. The Green Team tests the usability of the teams' networks, gives the teams tasks to complete, and requests changes. The White Team is responsible for scoring and enforcing the rules. The teams are judged on community service, the primary competition, and the real-time competition [10, 11].

In 2009 the US Cyber Challenge was announced to help the United States regain the lead in cyberspace. The US Cyber Challenge has 3 main components: The DC3 Digital Forensics Challenge, The Network Attack Competition, and Cyber Patriot. The DC3 Digital Forensics Challenge is a competition in which contestants are given increasingly difficult digital forensics challenges The Network Attack Competition is an offensive cyber security competition that deals with network vulnerability discovery and exploitation. The DC3 Digital Forensics Challenge and the Network Attack Competition are open to top high school students, college students, and graduate students. Cyber Patriot is open to high school students only and is the focus for the rest of this paper [12, 13].

III. CYBER PATRIOT I

In 2005, the Institute for Cyber Securities Center for Infrastructure Assurance and Security (ICS-CIAS) conducted a one-day high school cyber security competition with the assistance and sponsorship of the Alamo Chapter of the Air Force Association (AFA). The event had two parts to it, an individual competition open to any San Antonio area high school student and a team component open to any San Antonio area high school with an Air Force Junior ROTC (AFJROTC) unit. The Alamo Chapter of the AFA provided scholarships to both the winning team and the winning individual and the event was considered a success. Unfortunately, the ICS-CIAS was also heavily involved in the development of the National Collegiate Cyber Defense Competition and with limited available time to develop such programs, a decision was made to concentrate on the high school level at that time.

By 2008 the landscape had changed somewhat. Cyber security was gaining momentum in the federal government and commands were being formed in the Department of Defense to address the growing concerns that the nation was vulnerable to cyber attacks. The Air Force, in particular, was making a concerted effort to develop a "Cyber Command". The Air Force Association, a long-time advocate of air and space power, saw the growing importance of cyber security to the Air Force and, as a supporter of this military service, saw a

growing need to help support this new aspect of military defense. The AFA Aerospace Education Council (AEC), a portion of the non-profit Air Force Association dedicated to encouraging America's youth to enter the aerospace industry through scholarships and outreach programs, decided to expand to the cyber arena as well. AEC leaders approached the Air Force and suggested that a high school program be developed to encourage America's youth to consider cyber security as a possible career path. The Air Force agreed that this would be a valuable program and reached out to other organizations and a partnership was formed, under the leadership of the AEC, to develop a cyber security program for high school students. The partnership formed included organizations from government, academia, and industry and included the Air Force, the AFA/AEC, the ICS-CIAS, and defense contractors Science Applications International Corporation (SAIC) and General Dynamics. The decision was made to call this program Cyber Patriot.

The goal of the program, as conceived by the partners, was to excite and motivate high schools students in cyber security. It was also seen as an initiative that would also address one are of the nation's lack of interest at the high school level in Science, Technology, Engineering, and Math (STEM). As discussions were held through the summer and fall of 2008, the plan developed to create a phased approach beginning with a "proof-of-concept" demonstration leading to the development of a true national program. In order to control the growth, and because it provided an already existing means of communicating with high schools, the decision was made to initially limit the competition to high school AFJROTC and Civil Air Patrol (CAP) units. The AFA already had planned a symposium in Orlando for February, 2009 and volunteered to provide facilities to conduct the proof-of-concept competition in conjunction with the symposium. As it turned out, this also had the advantage of placing the competition at a location where senior leaders of the Air Force were already planning on attending and ensured a steady stream of senior leaders, including the Chief of Staff of the Air Force, through the competition area. Eight AFJROTC and CAP units quickly volunteered to participate in the program and the competition was "a go". Team size was limited to 5 individual plus possible alternates.

One of the first decisions to make was what format the competition should take. As a result of the success of the NCCDC, the decision was made to develop a program similar in nature – i.e. one that was focused team efforts on the defense of a "corporate" network. This format fit well with a training solution that SAIC had already made headway with and they volunteered to run the competition using their *TeamDefend* platform. The SAIC platform allowed the students to secure a small network of Windows-based systems and also provided the ability to conduct some low-intensity attacks of the networks to simulate to a certain level the hostile Internet environment organizations face on a daily basis. A built-in scoring engine scored the students based on what they did to secure their networks and how quickly they did this. Thus the winner of the competition was the team that did the best job at securing their systems as quickly as possible.

From the start, the creators of the competition recognized both the similarities and the differences between what was being developed and the NCCDC. The complexity of the high school competition was obviously not as great as that of the NCCDC as a result of the level of security expertise possessed by the high school students. This level of understanding and expertise applied not only to the competitors but the coaches and advisors as well. As a result, it was quickly realized that a significant part of the Cyber Patriot program was going to have to be an educational component. The products developed were not intended to be inserted into already busy high school curriculums but rather were intended for the coaches or advisors to use as part of an after-school program for a club or team. For the first competition the lessons developed primarily were aimed at teaching the competitors what was minimally necessary for them to be able to compete in the competition. Very little additional security information was provided this first year due to the time constraints.

Despite having less than a year to put the competition together, the event was a tremendous success. No significant technical issues marred the competition, the competitors were all excited about the event, and the location ensured a steady stream of VIPs. The winning team from this first competition was from Osceola High School in Orlando. In order to try and improved the competition, and to help judge the benefit of it, separate surveys were distributed to competitors, coaches, and visitors. All responded that the competition was valuable and that it should continue. The participants overwhelmingly stated that they had both learned something, and that they enjoyed the competition. One surprising, but very significant response from the competitors was that just over 50% of them said that they were more likely to attend college as a result of their participation in the event. Based on the very positive results from this proof-of-concept, the partners decided to continue with the competition and planning immediately commenced on the next year's event.

IV. CYBER PATRIOT II

Limiting who could compete in the program to AFJROTC and CAP units allowed for a controlled growth of the program. It also provided a built-in mechanism to

advertise the program. Utilizing AFJROTC and CAP communication chains, an announcement was sent out and the response was phenomenal. The founding partners were initially concerned that there might not be a sufficient response to the initial call for interest and that the hoped for minimum of 32 teams might not be obtained. Instead, there was a phenomenal response with over 300 schools asking for more information. Due to a number of considerations (e.g. drill meets that conflicted with the Cyber Patriot competition dates), the number of teams that actually participated in Cyber Patriot II was just over 170. To address the explosive growth of the competition and facilitate future expansion, it was apparent that a multi-tiered competition system was needed. Working with SAIC, the operations team decided to implement a hybrid virtual-physical competition system consisting of qualifying rounds conducted virtually and the finals requiring the team's physical presence at the CP II finals in Orlando, FL. Adopting a virtual competition model for qualifying rounds helped address the need to accommodate hundreds of teams, control cost, and ensure equity between competitors.

The qualifying rounds of CP II all followed the same model. Teams downloaded a password-protected VMWare image of an insecure system. At the start of the competition, the password to unlock the system was posted on a restricted website. Competitors then had a number of hours, depending on which round of competition it was, to secure their VMWare images and address the vulnerabilities contained in those images. Each image contained a software client that communicated with SAIC's CyberNEXS™ system – the primary scoring and evaluation mechanism for qualifying rounds. The agent would examine the team's system for mitigated vulnerabilities and report results back to a centralized CyberNEXS system that tracked results for all teams. The agent also generated a local web page for teams to view informing them of their connect status to the central scoring system and their progress in addressing the vulnerabilities present on their VMWare image.

The initial qualifying round consisted of over 170 teams each using identical VMWare images. As all teams competed simultaneously and were scored using the same criteria, competition organizers were able to select the top 24 teams from the initial qualifying round for advancement to the "Medalist" round. The remaining teams then competed in a second qualification round using a new VMWare image but using the same CyberNEXS agent and scoring system. The winner of the second qualification round was also advanced to the Medalist round.

The first two qualifying rounds were conducted using a Windows-based server operating as the system teams were assessing and securing. During the Medalist round, each team was presented with three VMWare images – one Linux server, one Windows server, and one Windows client. The timeframe of the competition was extended slightly, but the same scoring approach and system was used. The top 8 finalists from the Medalist round advanced to the CyberPatriot II finals held in Orlando, FL.

For the CP II finals, the decision was made to bring the teams together and have them compete in the same physical space at the same time. CP II finals were held in conjunction with the Air Force Association's Air Warfare Symposium and Technology Exposition. The competitor's challenge consisted of 5 VMWare images – 2 Linux-based and 3 Windows-based. As with previous rounds teams were challenged to assess and secure each virtual image while the CyberNEXS system providing automated tracking and scoring of each team's progress. In addition to increasing the number of system images, the CP II finals added several new elements not seen during qualifying rounds – Red Team activity, an IDS, and a "trouble ticket" system.

Red Team activity at the CP II finals was very carefully orchestrated and scripted. At set points during the competition, the Red Team launched identical attacks against each team probing for very specific vulnerabilities. If the Red Team was able to exploit the vulnerability, it indicated that the competitors had not addressed the vulnerability and the team lost points. While the CP II finals used humans to perform the scripted Red Team attacks, future versions of CP will likely automate the Red Team attack function. To help them, defend against Red Team activity, each team was provided with a pre-configured, Snort-based IDS. If competitors were able to correctly identify Red Team activity and report it through the trouble ticket system, points could be restored from Red Team generated losses.

The CP II finals also used a web-based "trouble ticket" system that is part of the CyberNEXS technology. Teams used the ticketing system to document their corrective actions, request actions from the operations team such as restoring a virtual image, report Red Team activity, and so on. Teams were incentivized to submit tickets as tickets were a scored item earning teams anywhere from 0 to 10 points.

The hybrid approach combining virtual qualifying rounds with a physical final round worked quite well and proved to be a sustainable and viable model that will be continued as the competition expands in the 2010-2011 season. As with any activity of this scope, there were some significant lessons learned:

1. Connectivity and bandwidth were significant issues for some schools. In some cases students

were unable to download the virtual images at school due to incredibly slow connections at school. In other cases firewall restrictions prevented teams from connecting back to the central scoring system. Teams were remarkably resilient in addressing these problems and travelled to team member's homes, public libraries, coffee shops, or any other place where they could locate reliable bandwidth.

2. Security measures at some schools reloaded student and lab systems on a daily basis forcing students to find dedicated systems to store virtual images or even use their own personal systems.

3. The exposure of staff and faculty members to technologies such as VMWare was quite low – an issue that will be partially addressed through an expanded CyberPatriot training and education program.

4. A surprising number of schools did not have the computer systems to support running a virtual image on a laptop of desktop containing at least 2GB of physical RAM. This coupled with the lack of bandwidth shows a lack of technology resources at many of the participating schools.

Overall, the competition went very well and we have seen that there is a great deal of interest in cyber security competitions among high school students. The amount of interest was evident from the initial expansion from 8 teams to over 170 teams, but as the competition progressed we encountered more and more teams that were initially assembled and organized by an interested student and not by a faculty or staff member. The competition ended with scholarships being awarded to the team members from the top three teams. SAIC provided $500 scholarships for each member of the 3rd place team, $1500 for each member of the 2nd place team, and $3000 for each member of the winning team from Clearfield High School in Utah. As a final note on CPII, the value of the competition program was highlighted when Maj Kit Workman, the coach of the Clearfield HS team, reported that, as a result of their participating and the scholarship money, two of his cadets had been inspired to pursue college who might not have considered it before. [14]

V. Educational Component

A primary goal of the CyberPatriot competition system was to provide competitors with some basic knowledge of cyber security at both the theoretical and practical level. From the beginning, the CyberPatriot competition was designed to incorporate an education component and, as most of the coaches had no cyber security background, the educational component needed to accommodate both self-paced and instructor led learning models.

In the inaugural year of CyberPatriot, the educational component was focused primarily on teaching teams how to compete and how to use the competition technologies. At the end of CyberPatriot I, the decision was made to dramatically expand the educational component.

The educational component for CyberPatriot II provided basic cyber security lessons using a combination of web-based CBTs, video clips, and traditional instructor led presentations. Topics included an overview of cyber security principles, network basics, protocol basics, password, safe computing, firewalls, securing Windows systems, and securing Linux systems. All materials were made available to teams through CyberPatriot websites or partner sites such as the ACT Online program.

Based on reviews from CyberPatriot II, the educational program will be expanded even more with the CyberPatriot III program including more materials focusing on practical aspects of cyber security and technologies such as VMWare.

VI. Future Plans

The first two proof-of-concept years for Cyber Patriot has convinced the founding partners that this is a valuable program and that there is enough interest at the high school level to continue building the program. As the number of schools wishing to participate grows, there is a recognition that there is still much to be done to expand the program to a true national program. In order to build toward the goal of a national competition, the following is a list of the planned enhancements for the 2011 competition year:

1. The competition will be split into two parts and opened up to schools beyond the current AFJROTC and CAP teams. One portion of the competition will continue the affiliation with the service JROTC programs but will open it up to include not just the Air Force but JROTC units from any of the services. The other portion of the competition will be open to any high school team in the country and is not restricted to those with JROTC units. For Cyber Patriot III, the competition will be limited to 500 teams in each of these categories and there will be a winner crowned from both. The limitation has been implemented to again control the growth of the competition to ensure that the size of the program does not

negatively impact the events as the program expands. After the 2011 competition year, the plan is to gradually expand the program to eventually allow as many high schools to participate as want to. Advertising the competition to the service JROTC units is not an issue since there are already existing mechanisms to reach each of these units. Advertising the competition to high schools without JROTC units is a separate issue but there is already a significant number of schools that have expressed an interest in participating and there are school districts that are already gearing up to help their schools participate. The word is already spreading through academic circles without any overt attempt to advertise the competition.

2. The education component is going to be significantly expanded to provide more training materials for the high schools. The materials will include student manuals along with additional materials for those training the students. The material will also include suggested labs to provide a hands-on aspect to the training as well. There are also pilot programs in school systems that have volunteered to explore building cyber security programs in their district.

3. As the program grows, the ability to involve thousands of teams in the competition will be problematic. One of the ideas that is being explored is whether a game can be developed to take the place of the 1st level of remote competition (e.g. "you have to at least score XYX points in the game before you can sign up for the competition"). The idea of having a game be part of the program has been discussed since the beginning and the current thought is that there might actually be multiple games accomplishing different goals. The first game that will be introduced, hopefully for the 2011 competition year, will be one that is designed to a) create an interest in security among high school students, and b) provide some basic security instruction for those who play it.

4. Up to this point, the program has survived on the donations of the founding partners. In order for the program to grow, additional significant sponsorships need to be obtained. Early indications, however, have shown that there is tremendous interest by industry in supporting the program and it is the hope of the founding partners that sponsorships will be obtained to allow for expansion of the program and for an increase in things such as scholarships for the top teams.

Another desire in the future is to establish a stronger tie between the Cyber Patriot and NCCDC programs. The winning team from CP currently receives a free trip to the NCCDC championship. At the event, the students do not compete against the college teams but are given an opportunity to sit with the red team, help the white team judges, and to interact with the college students during networking events. This provides them an opportunity to talk to students from different colleges with established cyber security program. The colleges, for their part, can use the opportunity to start recruiting future members for their own team. The founders of CP believe this is an extremely valuable experience for the high school students but would like to see more students have the opportunity to talk to college students about their majors, plans, and employment opportunities. The lesson the high school students will hopefully take with them is that cyber security is a possible career major and career path.

VII. Conclusion

The Cyber Patriot National High School Cyber Defense Competition is entering its third year and the prospects for its future look extremely bright. The competition has grown in its first two pilot years from 8 in 2009 to over 170 in 2010. It is anticipated that the number will approach 1000 teams in 2011 and will continue to grow after that. The educational component of Cyber Patriot is expanding and will soon also include a cyber security game designed to help interest students in the competition and in security. The competition, originally only open to AFJROTC and CAP units, will open up to any interested high school team in 2011. The responses from coaches and competitors who have participated in the competition are extremely positive and it appears that the goals of the program are being met. Cyber Patriot may not be a national program at this point, but it appears to be well on the way to becoming one. In doing so, it is introducing a new generation of students to computer security and is helping to ensure this generation has the knowledge and understanding to secure the nation's future computer systems and networks.

VIII. References

[1] Jackson, Williams, "Uncle Sam, industry scout for cyber security talent", *Government Computer News*, July 27, 2009, www.gcn.com

[2] Nops R Us, *DefCon CTF 2008 Overview*, http://nopsr.us/ctf2008/overview.html

[3] Diutinus Defense Technologies Corp, *Diutinus Defense Technologies Corp. / Home*, http://ddtek.biz/

[4] Schepens, W.J. and J.R. James, *Architecture of a Cyber Defense Competition*, 2003 IEEE International Conference on Systems, Man & Cybernetics, 2003.

[5] W. J. Adams, E. Gavas, T. Lacey, and S. P. Leblanc, *Collective Views of the NSA/CSS Cyber Defense Exercise on Curricula and Learning Objectives*, USENIX 2nd Workshop on Cyber Security Experimentation and Test, 2009

[6] University of California at Santa Barbra, *The UCSB iCTF*, http://ictf.cs.ucsb.edu/

[7] UTSA Center for Infrastructure Assurance and Security, *Welcome to the National Collegiate Cyber Defense Competition*, http://www.nationalccdc.org/

[8] K. Harrison and G. White, *A Framework for Modeling Security Measures*, 13th Colloquium for Information Systems Security Education, pages 133-138, June 2009.

[9] K. Harrison and G. White, *An Empirical Study on the Effectiveness of Common Security Measures*, 43rd Hawaii International Conference on System Sciences, January 2010.

[10] IT-Adventures. *What is IT-Adventures?* http://www.it-adventures.org/index.html

[11] D. Jacobson and J.A. Rursch, *Engaging Millenials with Information Technology: A Case Study Using High School Cyber Defense Competitions*, 12th Colloquium for Information Systems Security Education, June 2-4, 2008.

[12] SANS Institute, *Sans Institute – Us Cyber Challenge*, http://www.sans.org/uscc/

[13] *The United States Cyber Challenge 1.1 (updated 5-9-09)* http://www.whitehouse.gov/files/documents/cyber/The%20United%20States%20Cyber%20Challenge%201.1%20%28updated%205-8-09%29.pdf

[14] Miranda Lin, "Uncle Sam Is Looking For Few Good Hackers", *Columbia News Service*, 26 February 2010.