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

Expanding the Educational Boundaries of Cyber Defense Exercises

Kara Nance and Brian Hay, *University of Alaska Fairbanks* and Amelia Phillips, *Highline Community College*

Abstract – Despite the continuous hard work that educators and organizations undertake to develop the skill-base necessary to defend our national assets, it has become increasingly obvious that the United States and the rest of the world are ill prepared for an all out cyber attack. One very valuable contribution to creating a workforce capable of addressing this important issue is the cyber defense exercises which simulate the very environments our students will be charged with defending in their careers. In this paper, we explore cyber defense exercises from an educational perspective and investigate how recent work in this area can be leveraged to improve the security posture of the nation. In addition, we focus on promising methods for horizontal and vertical expansion of cyber defense exercises in order to continue to evolve the range and types of exercise and participants to maximize the proven effectiveness of this valuable educational activity.

Index terms – Information assurance curriculum, cyber defense exercises, security education

I. Introduction

Cyber attacks are common in the IT world, and the recent mainstream focus on well organized and funded attacks by skilled attackers, dubbed the Advanced Persistent Threat (APT), shows how serious this problem is. The academic community is working to overcome the challenges associated with mitigating these threats by preparing the next generation of cyber security professionals. Although it was somewhat contrived, a recent cyber exercise held sent a chilling message to the country that the U.S. is not ready to face an all out cyber attack. [1] Among the many issues raised by the exercise, was the preparation of IT departments to respond to cyber emergencies. While this came as no surprise to the academic cyber security community, this exercise marked one of the first major publications in popular press that demonstrated the vulnerability of our critical infrastructure to a cyber security attack.

To improve our country's security posture, improved training, education, and recruitment activities are needed to repopulate, reeducate, and reinforce the existing workforce, many of whom have migrated into the IT professional without a formal educational foundation in cyber security. A paradigm shift is occurring, but it needs to be accelerated. It requires hands-on, integrated learning. Lectures and theory are strong foundational components, but frequently inadequate to meet the needs of the workplace.

II. Background

This section provides a representative sample of three current levels of the many cyber defense exercises. The intention is to demonstrate the evolution of the exercises and the main focus on the existing annual exercises in educational settings.

A. CDX

The military academies led the way in creating cyber defense exercises through the Inter-Service Academy Cyber Defense Exercise (CDX). These exercises are intense, realistic, hands-on team competitions stretching over several days with the National Security Agency serving as the attackers. The first CDX competition was held in 2001 and included the participation of the United States Military Academy (USMA), the United States Air Force Academy (USAFA), and the Naval Postgraduate School (NPS). [2]

This initial competition was the result of several years of research and design, motivated by the recognition of the growing dependence upon digital communication. The competition has evolved and in its ninth year included participants from U.S. Air Force Academy, U.S. Coast Guard Academy, U.S. Merchant Marine Academy, U.S. Naval Academy, and U.S. Military Academy, as well as the Air Force Institute of Technology, the Naval Postgraduate School and Royal Military College of Canada. [3]

B. CCDC

As the military schools were evolving and expanding the CDX, the non-military institutions of higher learning started the national CCDC (Collegiate Cyber Defense Competition) in 2005 at the University of Texas at San Antonio. Teams of up to eight students, including up to 2 graduate students, are charged with managing and defending their network and hosts while maintaining services and responding to the activities of various "teams" that have evolved as discussed in section IV –

Vertical Expansion. Since 2005 the national competition has grown to include eight regional qualifying competitions. Some areas conduct state or local level qualifiers for the regional events. The winning team at each regional event currently receives a funded trip to participate in the national competition.

C. High School

High school competitions are becoming increasingly popular. The Air Force Association (AFA) conducted the largest high school competition in November 2009 with over 200 teams competing. [4] The Colloquium for Information System and Security Education (CISSE) has been involved for several years in developing more high school exercises through panels and discussions facilitated at their annual meetings. [5] High Schools experience many of the new participant challenges that could potentially be mitigated by the strategies discussed in section III – Horizontal Expansion.

The previous section provides examples of some of the best known cyber defense exercises (as opposed to the Capture the Flag type events which also include an offensive component). The following sections discuss potential horizontal (increasing the number of participants) and vertical (increasing the scope of the event) expansions to the exercises to ensure that the benefits of the CCDC reach as wide an audience as possible, and further enrich the educational experience of all contributors by addressing current and emerging issues.

III. HORIZONTAL EXPANSION

In order to support a horizontal expansion of cyber defense exercises, we need to investigate and try to minimize potential barriers to entry for new participants, find methods to include more community colleges, consider the emerging potential for virtual and media-based cyber defense exercises, and investigate curriculum issues.

A. New Participants

As the popularity and value of the exercises grow, more schools become curious about the associated opportunities. The immediate barriers to participation include facilities, faculty initiation, team initiation, individual student initiation, and a lack of appreciation of the overall objectives of the exercises.

1. Facilities

Many schools do not have isolated labs which allow their students to install and configure full operating systems and applications, program their own routers and switches, create ACLs, and further develop the skill sets that will help them succeed in the exercises as well as the workforce. Those schools that do have access to such facilities also need to provide personnel to manage the lab, which can include the issue of ensuring sufficient isolation while also providing enough flexibility to allow the inclusion of new tools and updates.

2. Faculty Initiation

Faculty involvement and initiative is needed in addition to guide, encourage, and direct the enthusiasm of the students. A major stumbling block is that many instructors may be overwhelmed with the daunting task of organizing or participating in a cyber defense exercise. As networks have become more sophisticated, the specialties have become increasingly isolated. A competent Cisco instructor may not be comfortable teaching Active Directory and an instructor who excels in Active Directory may shirk from an Apache Server. While most IT instructors have some familiarity with a wide range of topics, it would be helpful to create more formal methods to "train the trainers" for those putting together teams. This is currently primarily accomplished as an informal mentoring process, but as the events become more organized, increased automation and documentation can simplify the role of the new faculty. The new role would be more as a facilitator and coach.

Most of the competitive exercises have not been spectator events due largely to the physical limitations of the facilities. However, that may need to change to involve the local community, nearby schools, and potential employers. As the popularity continues to grow, documentation which guides event organization and preparation can help minimize the barriers to entry.

3. Exercise Objectives

While not all cyber defense exercises are organized as competitions, the CCDC is organized as a competitive event, in which winning teams can move on to the next level (or are eventually crowned as the national champion). This can be a great motivating factor for some teams in both the lead up to, and during, the event. However, there is also a perception, particularly amongst those considering competing for the first time, that if a team cannot be competitive, or cannot dedicate time for team preparation over a significant portion of their academic year, that there is no value in the event (i.e., if you can't win, then why play?).

One solution is to run local non-competitive events with a focus on team problem-solving and working together to accomplish a goal. Perhaps the least appreciated lesson at cyber defense exercises is the value of the experience.

While one team at each event will be crowned as the winner, every team at these events, no matter how they ultimately place, is likely to get great benefit from the process of preparing and participating. Each CCDC event will have one winning team, but can easily have 70-100 students who improve their understanding of cyber security issues.

4. Team Initiation

Since most cyber defense exercises use a team approach to problem solving, it is important that materials and methods are available to assist in the development of new teams. Discussions of skill sets required, group dynamics, problems-solving approaches, and operational methods all come in to play as teams are developed. A facilitated approach to in-house cyber defense mini-exercises could help to build the experience and confidence that teams need to prepare for participation in a larger event. While potentially a useful preparatory experience for all teams, this is especially important for new participants and also a valuable component for coursework.

These short duration events could be used as components of a course or extended to "cyber scrimmages" (possibly two college teams or two high school teams, or even mixed teams from a local college /high school pairing). This allows team members to become comfortable with what happens in a larger cyber defense exercise environment. When performed in high-schools, or mixed college/high school environments, colleges could use these events as a method for recruitment.

5. Individual Initiation

Ultimately, teams are made up of individuals and expanding the pool of individuals that participate in cyber defense exercises effectively expands the number of people with increased awareness of how to protect our digital assets. Many of the options and new role definitions in the Team Expansion section of this paper will necessitate the involvement of new skill sets that are not currently present in many cyber defense exercise teams.

Beyond the need for new skill sets, there is a need to increase the involvement of traditionally underrepresented populations in cyber defense exercises. There has been significant research into how curriculum and programs can be changed to work towards more balanced populations in IT. Margolis, et al observe that a frequent barrier is the lack of the very experimental opportunities which can lead to an appreciation of and passion for computer science. Many groups underrepresented in the field do not have computers in the home and thus do not have the opportunity to discover the "fun" associated with computing. [6]

The National Science Foundation has funded the Broadening Participation in Computing program and has many associated successful programs that could feed into additional cyber defense exercises including national, regional, and local alliances as well as demonstration projects. [7] Another opportunity available through the National Science Foundation that could be utilized to improve all of the New Participant categories is National Lab Day (NLD). NLD is a nationwide initiative to build local communities of support that will foster ongoing collaborations in STEM disciplines. [8] Teachers can register and express an interest or need and will be partnered with registered "scientists and techies" from a volunteer pool that can assist them in building capacity in cyber defense appropriate to their particular needs.

There is much that can be done to increase the range of individuals and teams using cyber defense exercises as part of their educational experience.

B. Virtual Exercises

In today's economic climate, many schools cannot afford the time and expense associated with student travel. In some regions, such as areas on the East Coast with high academic population densities, this may not be a problem. But in areas such as that served by the Pacific Rim Collegiate Cyber Defense Competition, students in places such as Alaska and Hawaii find it cost prohibitive to purchase 8 or more tickets plus lodging to compete in Washington state, while lacking enough local teams to hold local/statewide events. Cost is also a significant barrier to the development of a high-school version of the CCDC. High School budgets for travel to and the operation of events are likely to be even more restricted than at the college level. [4]

At HICCS this year, it was agreed to run a trial version of a regional CCDC event in 2010 using a virtual environment, with the goal of including at virtual at-large regional event (with the winner going to nationals) in 2011. This event will take place on April 10, 2010 using the ASSERT virtual lab environment at the University of Alaska Fairbanks (UAF). In this model all competition systems will run on servers at UAF, and students will interact with their assigned systems via connection that look and act like RemoteDesktop or VNC sessions. From a technical perspective, these sessions will actually be managed by the VMware Virtual Center software to ensure that the competition VMs remain isolated from external networks. This model is already employed by

the UAF ASSERT Center to support security remotely accessible security labs for 18 institutions nationwide. [9]

While the teams in this event will not meet in a single location (as is the case in the more traditional CCDC events), each team is required to have an isolated room on their campus (computer lab, classroom, etc) from which that team will participate. Local faculty members will then ensure that their team follows the event rules regarding outside assistance during the event.

If successful this architecture could provide significant costs and time savings over physical CCDC events. In addition to travel expenses, the deployment of virtual machines on servers is substantially less time consuming than imaging, connecting, and configuring the large numbers of physical hosts often used at CCDC events. In addition, it could be used as a training environment prior to the event, thus ensuring that all teams can prepare for the event in a consistent manner.

C. Media-based Exercises

Many schools simply do not have the facilities or time to nurture a team or organize a large-scale cyber defense exercise. A possible alternative for them would be CD or DVD based exercises or even a browser-based game experience where they have to defend a network. This could also be used to promote participation of individuals who want to experiment before committing.

IV. VERTICAL EXPANSION

In this section we will consider methods for vertical expansion of the cyber defense exercises, in which the scope of the event is increased. We will address the issues of team expansion, device expansion, and integrating participants.

A. Team Expansion

There are many defined roles that have evolved as cyber defense exercises evolve. The following section briefly describes the traditional roles of the Red Team, the Blue Team, the White Team, and suggests new teams that might be included to expand the educational experience associated with an exercise. As seen with the original CDX competitions, the number of teams grew as the games became more popular and more intense in scope. The new threats appearing on the horizon offer new areas of concentration for groups to be involved.

1. Attacking Team - Red Team

Traditionally known as the "Red Team", the attacking team is the main adversary for the participants. In the case of the CDX competition, the NSA fulfills this role. In the CCDC events red team members are often professional penetration testers who volunteer to help with the event, but in at least one case the red team has been composed of the core of a student team who participated for two years as undergraduates, and who then returned to run the red team as graduate students.

One issue is the importance of ensuring that the academic goals of the event are clearly communicated to the red team members, who are typically not from an academic environment. Such a discussion should include appropriate types of post-compromise behavior designed to ensure that students spend the event truly learning about cyber security, as opposed to merely reinstalling compromised operating systems. It is also important to ensure that the red team can document the successful compromise of systems in a manner that can be used to both allow teams to earn back some lost points by identifying compromises and fixing the associated vulnerabilities, and to provide post-event feedback to teams about compromises that they did not detect. If possible, a wider description of red team activities, to include all actions (successful or otherwise) would be useful for post event feedback to educate teams about the activities of their adversaries, and even the types of attacks they prevented (knowingly or otherwise). Ensuring that this documentation is produced during the event can be challenging, but if done successfully it can have tremendous educational value for the students.

At the start of the event the red team is likely to find many exploitable systems, but as the event continues, the red team will hopefully find the student systems less vulnerable to attack. The activities of the red team can be scaled accordingly, so that in the early stages of the event successful compromise results in a basic level of post-compromise activity (e.g., the addition of a file on the user's desktop, or a new user account on the system). Later in the event more substantial post-compromise behavior may be appropriate. For example, a weak web server password on the web server found in the early stages of the event may result in a minor change to the home page. The same weak password found on the second day of the event is more serious, and may result in a greater "penalty" by the red team, such as the encryption and "ransom" of the website contents or database data.

2. Injection Team – White Team

While the role of this can vary, they frequently act as the event judges, and their role commonly involves providing the business tasks ("injects") to the teams, assigning points for completed or partially completed injects, and addressing questions that the students may raise during the event. The white team is typically defined as trusted

during the event, meaning that the student teams can be assured that any interaction with actual white team members is free from any deceit or malice, and that white team members will not make any conscious effort to attack the student's networks or hosts.

3. Event Management Team

This group is sometimes referred to as the Blue Team, and their role is to ensure that the exercise infrastructure is operational at the start of the event, and remains in that state throughout the event. In some cases some of the equipment and systems may fail, in which case it needs to be repaired or replaced with the lowest impact on any team using that hardware. The blue team may also have to address problems in the environment caused by the activities of the participants, or quite commonly the red team. In the heat of the event it is quite possible for a red team member to inadvertently attack some key component of the infrastructure (either directly or indirectly), causing it to fail or function in a manner inconsistent with the event requirements. For example, a poorly constrained attack against the routing tables of the student teams may also have an impact on the core routers in the competition network, resulting in a failure of the scoring engine to successfully contact each team's required services. Teams have no control over these core network components (i.e. the network devices upstream from their defined network), and in such an example it would be the responsibility of the blue team to determine that such a failure had occurred in the environment, and to correct it with as little impact on the event as possible.

Like the White team, the Blue team is defined to be trusted, and as such if a blue team member interacts with the student teams they can be assumed to be acting without deceit or malice.

4. Social Engineering Team

This group may be the same as the red team, or may form a separate group focused on social engineering. Example of activities that this team could conduct include masquerading as white or blue team members in an effort to gain access to network devices or hosts, or sending messages purporting to be legitimate business injects using a variety of communicating methods. Although legitimate white and blue team members are defined as trusted, it is the responsibility of each student team to authenticate members of those teams in some manner. Such physical authentication could be conducted using a team badges (provided by event organizers), and electronic communications could be authenticated using a variety of techniques, but it would be the responsibility of each student team to perform such authentication for anyone claiming to be a member of a trusted team.

5. Operational Budget Team

An Operational Budget or Green Team could set a variety of budgetary constraints on the students, designed to ensure that they have to make decisions about responses to a variety of threats based on factors beyond merely the technical issues. For example, teams may be allowed to "buy" additional hardware, software, or service for their environment but could be constrained by some budget defined by the Green Team. However, the budget may extend beyond just a financial budget other factors, such as a power budget for which the Green Team could develop metrics and measures that address and assess sustainable computing. Power consumption concerns, a long time focus of the sensor web community, has evolved and is now being extended to include computing in general. We expect sustainably computing issues to continue to gain importance in light of the massive and growing volume of data used to manage and understand our IT-centric world. A recent issue of The Economist included a special report on handling the data deluge. The article discussed the concern about energy consumption and the need to decrease our data processing power consumption as we will soon begin to saturate infrastructure capabilities. [10] IEEE and the IEEE Computer Society are co-sponsoring the first International Green Computing Conference in the summer of 2010 to begin to look at associated issues. [11] Metrics and measures could include utilization of runtime systems that assist in saving power, tools for collective optimization of power and performance, and monitoring tools for power and performance.

6. Business Continuity Team

This team could provide a series of activities designed to determine the business continuity readiness of each student team. The activities conducted by this team could include failing a component in the student environments (such as the web server), and assigning points based on the time taken to return the impacted service to an operational state. For teams with server redundancy this may involve no downtime at all, and even for those with a good backup plan this may be a relatively quick and trivial task. However, less prepared teams may find this to be a more time consuming challenge.

Another activity for this team may be requiring student teams to maintain up to date system management and configuration documentation, which would then be assessed against the current system configuration at some point(s) during the event (e.g., at the end of the first day of the exercise). For example, the Business Continuity Team could attempt to perform a database backup, followed by a restore from that backup using the directions in the documentation provided by each student

team. Points would be assigned based on the effectiveness and completeness of the documentation.

One interesting aspect of these types of actives is that they can be a way to involve non- or less-technical students in the cyber defense exercise process. For example, the business continuity plan may be architected by someone who is not a highly technical student, but who understands the concepts of risk management. The documentation could similarly be written and maintained by a student from outside the highly technical CS/IT domain. Alternatively the Business Continuity Team itself could primarily be composed of non-CS participants.

7. Architecture Team

Running a cyber defense competitive exercise can require several months of planning and a clear understanding of the resources available for the event, which often drives the type and scale of the competition.

The event architect must decide on the scenario, and then identify the types of systems that are appropriate for that scenario. For example, the scenario may involve a power company in a small town, and the associated systems could include:

- Infrastructure and services for the employees, including HR services, such as personnel records, communication tools, and job ticketing and accounting tools.
- Customer related infrastructure and services, including customer web site/portals, customer databases, billing systems, and communication systems (e.g., email).
- Partner resources, including systems to allow this power utility to interact with power grid partners to describe power needs and availability.
- Network infrastructure, including DHCP and DNS services, and network components such as switches, routers, and firewalls.
- Server infrastructure, including web servers, database servers, and file servers.
- Communication systems (email, IM, VoIP, etc).

An important architectural issue is the level of isolation of the exercise environment, as it is vital that red team activities not "leak" into production networks and hosts. The simplest solution from the perspective of ensuring no impact on production systems is to completely isolate the exercise environment using an air-gap. However, this also means that if components such as update or download servers are needed they must be replicated within the environment itself, and that a mechanism must be provided to allow teams to move tools into the exercise environment during the event.

The red team must also be connected into the environment, as must the scoring engine, judging systems, and any traffic generators that will be deployed.

In addition, a description of the environment must be produced (the scenario document that will be given to the teams at the start of the event). This will typically include the scenario back-story, a description of the required services/systems, and any account/password/host information that is to be provided to teams.

8. Communication Team

Modern life is dependent on electronic communication systems, as this is particularly true of the business environments that students may encounter in the cyber defense events. To support corporate communications teams may be required to implement and support communication infrastructures (e.g., email, VoIP, IM), and to define policies (and implement enforcement mechanisms) for the use of these systems. For example, internal corporate communications via email may require strong encryption and digital signatures to preserve confidentiality and integrity. In support of that requirement, each student team may need to define such a policy, and implement controls to enforce it. The communications team would be responsible for setting such requirements, and then assessing the documentation and enforcement mechanism to ensure compliance.

9. Behavioral Research Team

This team keeps track of time stamps and interviews the students as they respond to an inject or attack. They also do analysis of emotional response to stress to help gauge how to alleviate job burnout in this occupation. An analytical study of a cyber defense exercise could be an excellent research project for social scientists at a variety of levels, and could provide valuable information for further evolution of the events.

10. Virtualization

Virtualization may also provide opportunities to extend the event in new ways. For example, it may be possible for teams to be given some tasks in the week(s) prior to the actual exercise. Such activities may include making the teams responsible for deploying some part of the infrastructure (e.g., given some requirements for a website or web application, have each team design and deploy their own solution to that problem in the exercise environment). This may also add another level of

challenge to the red team (heterogeneous as opposed to environments), which could be used as a recruiting tool for that group.

Another option, suggested by Vincent Nester [12], is to include a physical security component based in a SecondLife type virtual environment, in which teams are required to identify the potential hazards and vulnerabilities in a virtual model of a physical environment (such as the corporate headquarters and data center for the company used in the event scenario)

These potential horizontal team expansions can be selectively mixed and matched in order to achieve the desired educational objectives for a particular target audience. Beyond just the participating defense teams, involvement in the other teams could also have associated educational objectives. Cybersecurity is multidisciplinary field that is strengthened through partnerships across degrees and disciplines. In addition to individualized skills associated with the participation category that an individual is in, an appreciation for the roles of others and the associated cybersecurity issues can be a positive emergent property of the cyber defense exercises.

It is important to note that all of the participants in every role at a cyber defense competition will likely strengthen their cyber defense skills. Thus including a wide range of participants and allowing them to experience a variety of roles from the conceptual, planning, and design phases—all the way through to execution and the subsequent analysis. In addition to expansion of the many roles that are part of a cyber defense exercise, the range of technologies included in the exercises can be expanded.

B. Device Expansion

Modern IT systems no longer simply consist of servers and workstations inside a firewalled perimeter, and our cyber security events should reflect that reality. Some alternative aspects to consider including in these events (some of which are already included in a limited number of events) are:

- Business to business connections: Many real businesses cooperate with other businesses at some level in their IT infrastructure, and we should include such dependencies in our events. For example, in the power company example we may require that each team also communicate with the other teams to express their current power availability and demand. Alternatively, consider a hospital scenario in which the accounting system involves communication with insurance billing systems. The important issue is that the IT infrastructure under the students control is dependent on other systems beyond their control for data input/output.
- Wireless networking is very widely deployed, and is often a point of access for attackers due to weak or nonexistent encryption and authentication capabilities in many products or configurations. Wireless networking may be added to the student environments to allow for easy connectivity in “meeting rooms”.
- Mobile computing: mobile computing is obviously a huge issue for real businesses, and includes handheld devices such as iPods/iPhones and Blackberrys, and also laptops/netbooks that can connect to and interact with corporate systems from both inside and outside the perimeter. In the power system example, we may require that technicians in the field be able to connect to account information using an iPhone application, or that employees can work from home or on the road, with full access to the corporate Intranet.
- Cyber-physical systems: IT systems commonly interact with, control, and receive data from physical systems (e.g., HVAC, lighting, and manufacturing systems). In the power example, some small set of lights could be controlled (turned on/off) by a cyber-physical system so as to simulate the power grid for the town.
- Outsourced services: Outsourced IT services (including “cloud computing”) are very much a part of IT infrastructure today, and while they can reduce costs they may also offer a business less control over a service than they would have if they managed it themselves. For example, an outsourced email system could be part of the scenario, to which the student teams could connect and administer (e.g., add/delete users), but which they would not fully control (i.e., no software update access to the outsourced mailservers). Teams could then choose to continue such outsourcing, augment it in some way (e.g., require encryption and/or digital signatures), or move it in-house. Such a decision could have budgetary implications within the event scenario that would be part of the team’s decision making process.
- Communication systems: Cell service and VoIP services could be included in the scenario, for example. This may allow communication with customers, employees, and partners, including the option for the white team to deliver some injects using the phone, for example.

This list will continue to evolve as new devices are added to the IT world, but this list provides a starting point from which a basic event environment could be augmented to address some more varied and current IT security challenges.

C. Integrating Participants

In the section on horizontal expansion of cyber defense exercises, we discussed some of the differences in the motivations of various entities for participating, in addition to identifying some of the challenges associated with the differences between educational objectives and outcomes. This was particularly emphasized between community college and university experiences. Currently most cyber defense exercises mandate that teams come from a single institution and have additional requirements such as full-time enrollments, etc. While this may be necessary to "level the playing field" for a competitive cyber defense exercise, it is not necessary in all situations. Cyber defense teams could be greatly enriched if teams from disparate backgrounds were formed to enrich the educational experience of the participants. Rather than bringing together a group of students from a cohesive background who learn together, teams could be formed that include practicing professionals, university students, community college students, and others. This rich combination would allow each team further appreciate their own strengths and weaknesses as well as the strengths and weaknesses of others This situation also more closely mirrors the diversity they are likely to encounter in the real-world, where team members are often drawn from widely varying backgrounds and levels of experience.

V. Summary

The current crop of cyber defense exercises have proven to be a valuable tool in the effort to provide students with a well-rounded understanding of the current state of cyber security. We have proposed areas in which this work can be extended to include more participants, more diversity, and more of the types of challenges that our students will have to address in the workplace or their research projects.

VI. References

[1] Nakashima, Ellen. *War Game reveals US lacks Cyber-Crisis Skills,* Retrieved 2/17/2010 from http://www.washingtonpost.com/wp-dyn/content/article/2010/02/16/AR2010021605762.html

[2] Ragsdale, Dan. Enhancing Network Security Through Competitive Cyber Exercises. Usenix -05 Annual Technical Conference.

[3] NSA Press Release. April 28, 2009. Retrieved March 1, 2010 from http://www.nsa.gov/public_info/press_room/2009/cyber_defense_trophy.shtml

[4] White, Col. Gregory B. Creating a National High School Cyber Defense Competition – A Joint Air Force / Air Force Association Project. Retrieved 3/16/2010 from http://www.afa.org/committees/ExecCommPDFs/0708/HS%20CDC%20whitepaper_2.pdf

[5] Colloquium for Information System Security Education. 2009 K-12 Outreach Panel.

[6] Margolis, J., et al. Stuck in the Shallow End: Education, Race, and Computing. MIT Press Books, 2008.

[7] BPC Portal – Making a World of Difference, Changing the Face of Computing. Retrieved March 10, 2010 from http://www.bpcportal.org/bpc/comm/projects.jhtml

[8] NLD-National Lab Day – A National Barn-raising for Hands-on Learning. Retrieved March 10, 2010 from http://www.nationallabday.org/about

[9] Hay, B. Applications of Virtualization to Digital Forensics Education. Digital Forensics Track of 43rd Hawaii International Conference on Systems Sciences. January 2010.

[10] The Economist. The Data Deluge and How to Handle it., A special report on managing information. The Economist. February 27th-March 5th 2010.

[11] GREEN. International Green Computing Conference. Retrieved March 12, 2010 from http://www.green-conf.org

[12] Nestler, Vincent. Personal Discussion with Brian Hay. July 2009.