Effectiveness of Cybersecurity Competitions

Ronald S. Cheung, Joseph Paul Cohen, Henry Z. Lo, Fabio Elia, Veronica Carrillo-Marquez
Department of Computer Science
University of Massachusetts Boston
Boston, Massachusetts 02125-3393
Email: {cheungr,joecohen,henryzlo,fabioel,veiko}@cs.umb.edu

***Abstract*—There has been a heightened interest among U.S. government agencies to fund cybersecurity workforce development. These efforts include offering universities funding for student scholarships, funding for building capacity in cybersecurity education, as well as sponsoring cybersecurity competitions, games, and outreach programs. This paper examines the effectiveness of cybersecurity competitions in educating students. Our study shows that though competitions do pique students' interest, the effectiveness of this approach in producing more high quality professionals can be limited. One reason is that the knowledge barrier to compete in these competitions is high. To be successful, students have to be proficient in operating systems, application services, software engineering, system administration and networking. Many Computer Science and Information Technology students do not feel qualified, and consequently this reduces participation from a wider student audience. Our approach takes aims at lowering this barrier to entry. We employ a hands-on learning methodology where students attend lectures on background knowledge on weekdays and practice what they learn in weekend workshops. A virtual networking environment is provided for students to practice network defense in the workshops and on their own time.**

I. Introduction

It has been known for some time that there is a severe shortage of computer security specialists in the U.S., yet universities are slow to react to this need of educating more cybersecurity professionals. In fact, most universities currently do not offer degrees or concentrations in Information Assurance (IA) or Information Security (IS). A survey of 260 universities in the Northeast (Maine, New Hampshire, Vermont, Massachusetts, Rhode Island, Connecticut, Massachusetts, and New York) shows that less than 8% of the schools offer concentrations or degrees in IA/IS. Over 60% of the schools surveyed do not even offer a single course on network or information security. So, it is quite common for CS/IT majors to graduate from universities without knowing anything about security. This problem has not improved in the past few years when funding for higher education was flat lined or decreased due to the economic downturn.

In light of this shortcoming, President Obama has requested $57 million R&D fund in the FY2013 federal budget for a coordinated cybersecurity research initiative [1]. Together with other efforts, this will fund the NSF Federal Cyber Service: Scholarship for Service (SFS) program that awards scholarships to qualifying students entering the IA and cybersecurity field, and provides funding to higher education enterprises to build up the capacity to educate cybersecurity professionals [2]. The Scholarships for Service track will grant scholarships to students attending schools that have an established IA/IS program. According to our survey, less than 8% of universities in the Northeast can apply for this. The capacity building track is highly competitive and it will take winning schools several years to develop all the necessary IA/IS courses. It probably will take additional years to establish the program in order to graduate students in this area. These programs may help alleviate the cybersecurity workforce shortage in the future, but the impact may not be felt for some time to come.

Several DOD government agencies and public companies are sponsoring cyber defense competitions with the hope of training more cybersecurity professionals in the near term. Schools participate in these competitions or games in order to promote student interest, even though they have no formal cybersecurity programs or courses. At the University of Massachusetts Boston (UMB), the CS Department has no degree program or concentration in IA/IS, but it offers two security courses (IT 428: Information Security and IT 443: Network Security Administration) in the undergraduate IT curriculum. The CS Department formed a cyber defense team and students in the team competed in the 2011 and 2012 Northeast Collegiate Cyber Defense Competitions (NECCDC) [3] and the 2011 MIT Lincoln Lab Capture the Flag (CTF) contest [4]. This research attempts to study the effectiveness of these competitions in increasing the ability of universities to produce more IA and cybersecurity professionals.

II. Statement of the Problem

Past research has shown that these competitions are very effective in elevating student interest in cybersecurity [5], [6]. One reason is that they provide simulated real-world cyber attacks for students to practice network defense. Students find that interesting because they get a lot of hands-on experience that they cannot get in a classroom. During the competitions, students learn how to work as a team. They are forced to work in an intense atmosphere where they have to band together to solve a common problem, viz., defending their network against outside attackers. Also, students are excited to network with security professionals from industry and learn from them.

Though these cybersecurity competitions do pique student interest, the effectiveness of this approach in producing high quality cybersecurity professionals is limited. One reason is that the knowledge barrier needed to compete in these competitions is extremely high. To be successful at these contests, students have to be proficient in numerous topics, namely, operating systems, application services, software engineering, system administration and networking. A majority of CS majors feel that they do not possess the right skill set. Most universities offer a traditional curriculum in CS which teaches theory of operating systems, compilers and databases. However, the critical skills needed for cybersecurity are hands-on knowledge on script programming, system administra-

tion and network configuration. Learning these skills from scratch and be able to use them proficiently during competition take a lot time and effort. Consequently, this discourages participation from a wider student audience.

Another shortcoming for the competition approach is that most universities consider cybersecurity competitions as extracurricular activities. Students spend time on their own preparing for the competitions in addition to carrying their regular course load. When the demand for school work increases, students tend to reduce their involvement in cybersecurity training. For the NECCDC competition, it is not uncommon to see a 50% drop out rate between the Fall semester when students are recruited and the Spring semester when students have to spend a lot of time on preparations. Also, these activities depend mostly on self studies and peer instruction efforts. Those who are not sufficiently motivated to learn new concepts or technologies on their own tend not to show up as often. Since these activities are mostly student organized, there is no penalty for not showing up. This further reduces the number of students from learning cybersecurity.

Furthermore, for schools that do not have a formal program in IA/IS, it is difficult to sustain the interest generated by participating in one cybersecurity competition. Students from these schools work extra hard preparing for the competition and they learn a lot at the event. However, they may not retain any of the knowledge if they do not apply or refresh it after the competition. There are fewer opportunities if the school does not offer any courses or a formal curriculum in cybersecurity. As a result, students will lose interest in this area.

III. Hands-On methodology

To lower this knowledge barrier, schools participating in cybersecurity competitions are trying to spend extra effort. This includes teaching students on installation of operating systems and applications, configuration of services, setting up a network and its firewall. They also provide a networking environment for students to practice what they learn. The UMB Cyber Defense Team employed a hands-on learning methodology to prepare students for the competitions. Instead of using a standalone network consisting of hardware switches, routers and servers, the team constructed a virtual network based on Virtual Machines (VM) for students to practice network configuration and defense.

A. Lectures and Presentations

Lectures were offered twice a week and they were presented by students that had participated in previous cybersecurity competitions. These students selected the topics based on what they had learned in previous years and they paced the presentations for the new students. Focus was placed on making the lectures interactive and hands-on. Students were encouraged to follow the lessons and do exercises on their laptops. At the end of each lecture, feedback was solicited from these students and this provided guidance for the content of the next lecture.

As an example, the first few lectures offered were on learning and/or brushing up on their basic Linux skills. They were consisted of topics on basic Linux administration, networking and fundamental concepts of cybersecurity. The feedback we got from the students was that the talks could be more advanced. After discussing these basic topics, focus was shifted towards specific tools. In particular, the talk was on what tools were available and how one would use them. At the end of the week, the group held a workshop where they practiced the tools that they had learned during the week.

Students had been spending a lot time each week on the workshops and lectures. As the weeks progressed, the students became overwhelmed with regular classwork. Student participation began to drop off. This was the shortcoming of participating in cybersecurity competition as an extracurricular activity. There were no real incentives for students to attend lectures and workshops aside from students' pure interest in learning the subject. If the preparation for the competition was treated as a part of a regular course, the result would be different. In our case, as the numbers of student dwindled, we refocused the remaining group on competition-specific activities. For example, we invited our IT staff to give detailed lectures on mail server configuration and the DNS.

B. Workshops

A workshop was held at the end of each week. Sometimes students engaged in mock competitions. Students put to use what they had learned from the lectures, presentations and their own practice. Initially the less experienced students were presented with VMs filled with back-doors, some as obvious as open ports that connected directly to root shells, all the way down to cleverly concealed root kits that reopened ports and allowed the attackers (in this case, the more experienced students) to maintain persistence on these machines. Step by step, students taught one another how to detect each of these different vulnerabilities and how to rid the machines of any trace of an attack. Students were able to participate both as attackers and defenders, allowing them to see both sides. The workshop was a hands-on review of the topics that had been covered during the week, and it advanced in difficulty as the weeks progressed. Most participants found these workshops more useful than the lectures themselves. They made students aware of their shortcomings and forced them to apply what they had learned.

The VMs presented to the students also came with the ability to log all activities performed. These logs were on an individual student basis and they were analyzed for the purpose of improving teaching methods and improving skills of each individual student. During the last few workshops, students were encouraged to build their own VMs with vulnerabilities and challenged the more experienced students to find and fix them.

IV. Virtual Networking Environment

To enable interactive lecture sessions and workshops, we needed a network to demonstrate vulnerabilities and host mock competitions. The virtual networking solution had to be very versatile and unrestricted. The following are requirements that were taken into consideration:

- Allow full control of machines on school network by participants without taking on liability
- Allow full network access to machines from anywhere
- Allow only participants to host and access services
- Allow machines Internet access
- Allow fast provisioning of machines
- Allow auditing of usage of machines by participants

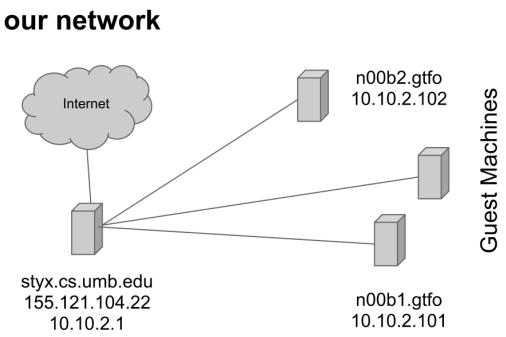

Fig. 1. Our network layout with respect to the Internet

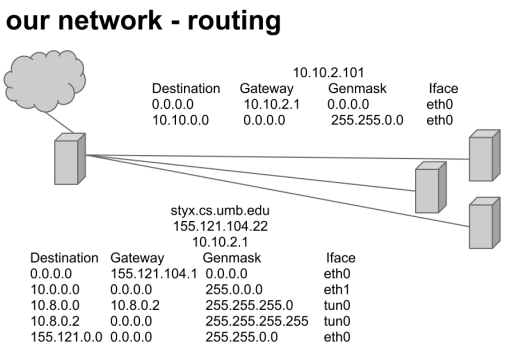

Fig. 3. The IP routing configuration

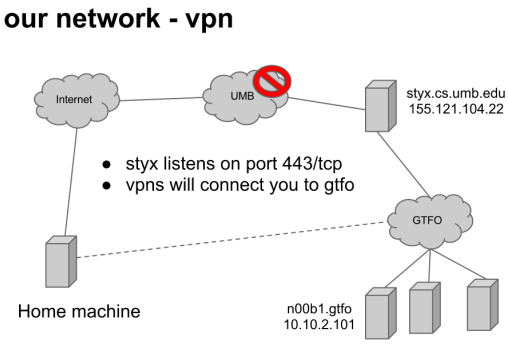

Fig. 2. The network layout with respect to the Internet

A. Network

For both logistical and convenience reasons, a virtual private network (VPN) was used. We needed a powerful VPN that offered tunneling via pseudo adaptors on client machines as well as a connection mechanism that would not be be blocked by most IT departments. OpenVPN [7] was used to accept connections on port 443/tcp. The connections were secured with the 2048-bit TLS encryption using public key cryptography (PKC). OpenVPN supports almost every platform and creates a pseudo interface to allow routing level access to the sandbox network. This method could allow any university to create a sandbox network even with heavy IT restrictions. VPN access to a sandbox network is of primary importance for participants' to do remotely a variety of functions:

- Reverse shells
- Full port range scanning
- Service hosting

The VPN system is displayed in Figure 2. We are able to simulate each participants home or personal machine being plugged into our sandbox network wherever they are. With the VPN system, participants could be given full access to a NAT network without the risk of them launching Internet facing services. Understanding the VPN system was another important aspect of the workshops. We developed VPN configuration tools for Mac and Linux which involved installing a tunneling driver that allowed transparent access to our sandbox network. This allowed students a truly versatile platform for exploit exploration and development without having to worry about university IT policy restrictions.

The networks routing configuration is shown in Figure 3. Here $eth0$ is connected to a public IP address, $eth1$ is connected to the internal switch and guests, and $tun0$ is a pseudo device provided by OpenVPN which handles VPN clients. In our configuration VPN clients are allowed to communicate with other VPN clients which allows for man in the middle (MITM) attacks and other educational vulnerabilities.

B. Virtualization

A virtualization host was used to create both a virtual switch and virtual guests. Virtualization is able to scale in a way that a dedicated standalone network cannot. Virtual machine templates were used to rapidly provision new virtual machines. A predefined list of MAC address to IP was configured in a DHCP server. When a machine was provisioned, its MAC address was the only change that needed to be made. When the machine was powered on, it received the correct IP address right away. This allowed support staff to avoid console access to these machines to configure IP addresses. It also allowed ARP entries to be clearly explained because where was a known mapping between MAC and IP. We set up a virtual Linux machine called Styx which was a dual-homed routable machine that served as a VPN server, NAT translator, Authoritative internal DNS server and resolver, and DHCP server.

C. Logging

A log server was set up along with an in-house keylogger to track participant sessions during workshops. This allowed us to generate statistics about login times and command usage. We used this tracking to see what commands students were still having trouble with after the lectures. This helped us determine what to spend more time on. We can also plot usage of the virtual environment. Figure 4 and Figure 5 show sample statistics of login sessions. It is not surprising that the environment was most often used on Saturdays and between 3:30 and 8pm.

V. Student Learning Results

After the competition, we conducted a survey to assess the effectiveness of our lectures and workshops. We asked questions

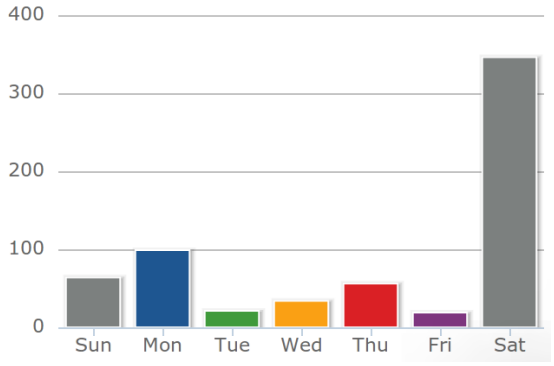

Fig. 4. Total number of logins over two months per weekday

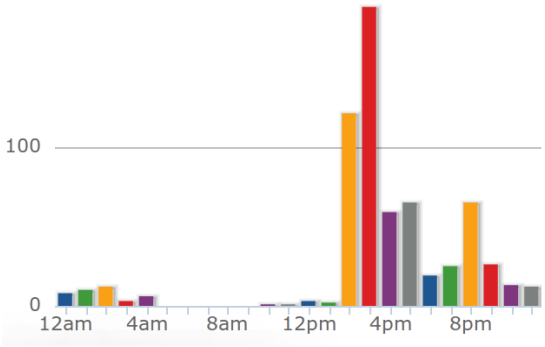

Fig. 5. Total number of logins over two months per hour

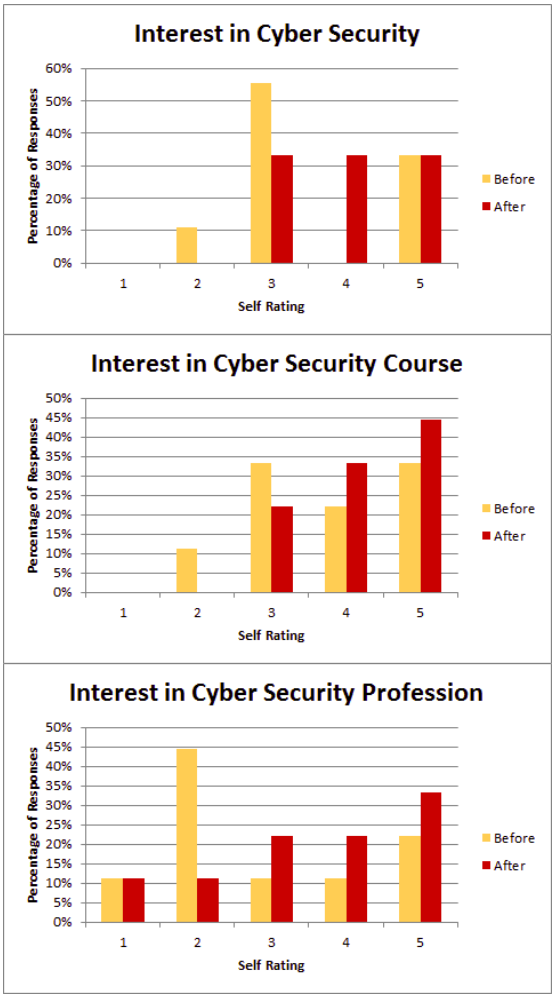

Fig. 6. Student's ratings of their own interest in various aspects of cybersecurity, before and after participation. The scale goes from 1 (low) to 5 (high).

about changes in student interest, ability, and participation before and after the NECCDC competition. A total of nine students responded to our survey. Our results are shown as follows:

Figure 6 shows that our lectures and workshops increased student interest in cybersecurity. Many students reported further interest in taking more university courses in security and knowing more about the cybersecurity profession. We see in particular that many students began inquiring about a career in cybersecurity after participating. Indeed, some students suggested that we help find internships, or offer course credit for the competition as a part of our CS/IT curriculum. Less experienced students reported a larger change in interest than those who had competed last year.

Figure 7 shows that students found both our lectures and workshops helpful for learning about cybersecurity and for improving their security and computer skills. Especially for less experienced students, the improvement is more visible.

Our lectures encompassed basic system administration, network troubleshooting, and IT skills, and our workshops provided an environment for which students could practice these skills. Figure 7 shows that students found the workshop to be more beneficial than the lectures. Inexperienced students particularly found the workshops beneficial for learning new subjects. Senior level students and those who have had previous experience found them helpful to practice and apply skills they have learned previously. However, senior students reported that the lectures were less useful for them since they were the ones who were organizing and teaching them.

This type of scenario-based learning employed in our workshops seemed to interest students significantly, and may prove to be a key to maintaining student interest and participation. Indeed, many students after the study suggested incorporating more scenarios in the workshops. Topics proposed included simulations of actual cyber attack / defense, identifying weak points in infrastructure, and larger scale attacks. One student even reported monitoring his or her own network more closely in order to learn cyber attack and defense.

Though the lectures and workshops initially attracted about 20 students, as the semester progressed, many students stopped attending. Towards the end, only a handful of students were present, and when the team was finally chosen, only those students who made it to the team continued participating. We conducted a survey of factors affecting student participation to find out the reasons. It reveals that neither boring lecture materials nor subject difficulty were the major factors that discouraged student participation. Surprisingly, even guaranteed inclusion of the individual in the cybersecurity team was not a strong motivator; it seems that most students were interested in the subject itself. The primary reason

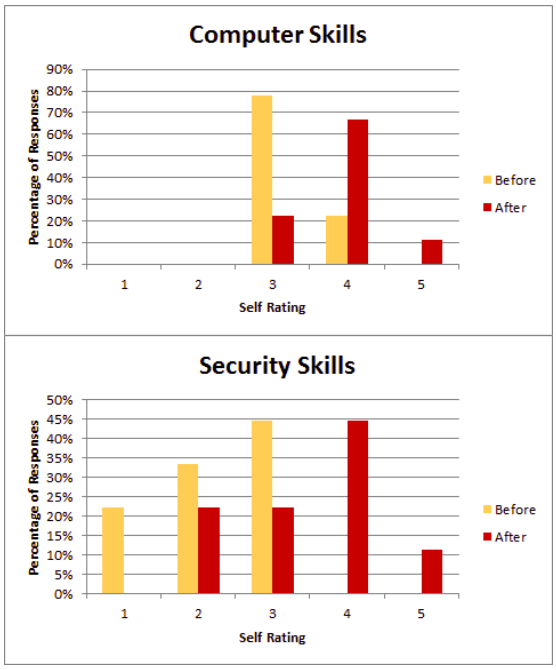

Fig. 7. Student's self reported security and computer skills, before and after participation.

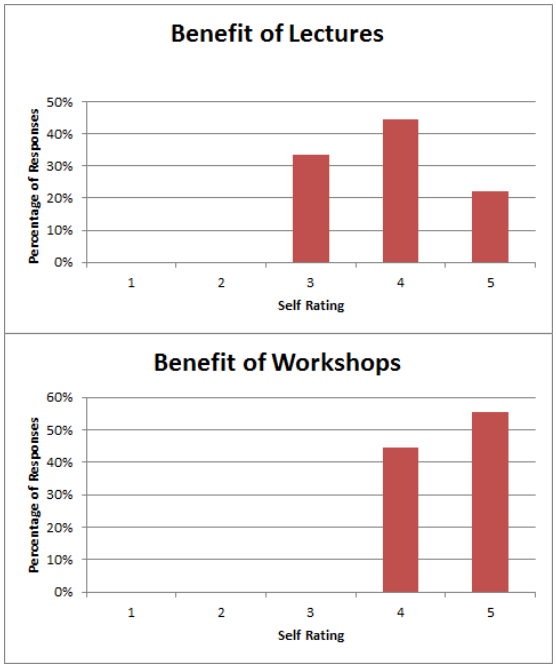

Fig. 8. Student's self reported benefit of the lectures and workshops.

was due to scheduling conflicts and the time commitments students had to made to participate in the competition. The frequency of our lectures and workshops was comparable to those of an university course, and the preparation required was no less. To address this issue, some students suggested incorporating competitions or mock competitions in cybersecurity courses. In this way, they can combine their interest in cybersecurity with their obligations to take classes. Indeed, many were interested after attending our lectures and workshops in taking more courses in security and learning more advanced topics.

The finding that inclusion in the cybersecurity team was not a strong motivator was particularly interesting. In light of the fact that students found real life applications of knowledge extremely helpful, the benefits derived from the competition may just be an instance of hands-on learning. Students were noticeably very excited to be able to practice what they had learned over the week in the workshops. Aside from solidifying their knowledge of concepts and giving them real life experience, students also derived more general benefits from the workshops, such as working in teams, communication, and leadership skills. We believe that the hands-on experience, both in workshops and actual competitions, is beneficial in invoking interest and teaching the cybersecurity subject to students,

VI. Conclusion

This paper has examined the effectiveness of cybersecurity competitions in educating students. Though competitions do pique student interest, using this approach to increase the ability of universities to produce more IA and cybersecurity professionals is limited. This is due to the high knowledge barrier, competition as a lower priority extracurricular activity, and the difficulty to maintain interest generated by the competitions. As a result, student participation is low. Our study has shown that by combining frequent hands-on workshops with lectures, we can lower the knowledge barrier for students to learn cybersecurity. The effectiveness of cybersecurity competitions can be further improved if they are incorporated into regular courses so that student can have less scheduling conflicts in attending them.

References

[1] G. C. New(GCN), "Budget reflects shift in scientific R&D, education," Feb. 2012. [Online]. Available: http://gcn.com/Articles/2012/02/13/2013-budget-science-technology-research-funding.aspx?Page=1

[2] "Federal cyber service: Scholarship for service (SFS) - NSF 12-531," http://www.nsf.gov/pubs/2012/nsf12531/nsf12531.htm, Apr. 2012. [Online]. Available: http://www.nsf.gov/pubs/2012/nsf12531/nsf12531.htm

[3] "Northeast collegiate cyber defense competition (NECCDC)," EMC Corporation, Franklin, MA, Mar. 2012. [Online]. Available: http://www.ccs.neu.edu/neccdc2012/index.html

[4] "MIT lincoln Laboratory/CSAIL capture the flag competition," Apr. 2011. [Online]. Available: http://mitctf2011.wikispaces.com

[5] R. S. Cheung, J. P. Cohen, H. Z. Lo, and F. Elia, "Challenge based learning in cybersecurity education," in *Proceedings of the 2011 International Conference on Security & Management*, vol. 1. Las Vegas, Nevada, USA: SAM 2011, Jul. 2011.

[6] J. Werther, M. Zhivich, T. Leek, and N. Zeldovich, "Experiences in cyber security education: The mit lincoln laboratory capture-the-flag exercise," *Cyber Security Experimentation And Test*, vol. 8, 2011.

[7] "OpenVPN," http://openvpn.net/index.php/open-source/downloads.html. [Online]. Available: http://openvpn.net/index.php/open-source/downloads.html