Challenge Based Learning in Cybersecurity Education

Ronald S. Cheung (cheungr@cs.umb.edu), Joseph P. Cohen (joecohen@cs.umb.edu)
Henry Z. Lo (henryzlo@cs.umb.edu), Fabio Elia (fabioel@cs.umb.edu)
Department of Computer Science, University of Massachusetts, Boston, MA, USA

Abstract— *This paper describes the application of the Challenge Based Learning (CBL) methodology to cybersecurity education. The overall goal is to improve student learning via a multidisciplinary approach which encourages students to collaborate with their peers, ask questions, develop a deeper understanding of the subject and take actions in solving real-world challenges. In this study, students established essential questions which reflected their interests in information security, formulated challenges on how to safeguard confidential information from cyber attacks and then came up with solutions to secure their information and network. For guiding activities, students participated in two cybersecurity competitions against their peers from other local universities. In these simulated real-life competitions, students were forced to work together, think on their own two feet and apply their knowledge to defend against cyber attacks. Assessments performed after the study showed improvement in students' computer and security skills, interest in learning security and ability to teach others. Student learning was further reinforced with publication of their research findings and making presentations to their fellow classmates.*

Keywords: cybersecurity, education, challenge based learning, CBL

1. Introduction

It is well known that cyber threats to the United States are prevalent and they affect our society, business, and government, yet there is no concerted effort among our government and private industries to overcome them. In 2010, the former Director of the National Security Agency, Mike McConnell, testified in the Senate that if there were a cyber war breaking out against our nation's infrastructure, we would lose. He reiterated his grim assessment a year later that we are no better off, though the stakes have risen higher [1]. His concern is realized with recent cyber attacks emanating from servers in China on Google and several dozen U.S. companies. These attackers were able to penetrate the defense of company networks and attempted to steal email accounts, information on weapon systems, and intellectual property.

Top officials in the Defense Department have long believed that the reason why the country's cyber defense is not up to the challenge is due to a shortage of computer security specialists who can battle attackers from other countries. The protection of U.S. computer systems requires an army of cyber warriors and the current estimate is that there are only 1000 workers skilled in this area. However, to meet the computer security needs of government agencies and large corporations, a force of 20,000 to 30,000 skilled specialists is needed [2]. In response to these heightened concerns, the Senate Commerce Committee recently approved the Cybersecurity Act (S.773) which recommends actions the government should take to improve the nation's cybersecurity preparedness. Among them, the government should fund research leading to the development of new security technologies, promote public awareness of cybersecurity issues, and encourage the growth of a trained and certified cybersecurity workforce [3].

Universities are slow to react to the need of cybersecurity education. It is very common for a computer science major to go through four or five years of undergraduate schooling without taking a single required class on security[4]. Consequently, they graduate without knowing anything about it. At the University of Massachusetts Boston, the Computer Science Department offers an ABET accredited curriculum which covers traditional courses in programming, compilers, operating systems and others. These courses tend to be theoretical and they do not deal with real-world problems in security. Recently, the department has added a more hands-on BS in IT program that offers a course in Network Security Administration. Since this is a new course, enrollment is limited. Furthermore, CS majors interested in cybersecurity often cannot take it because they lack the required IT prerequisites. The goal for this study is to apply innovative student learning methodologies to teach cybersecurity to a group of motivated CS/IT students who are interested in the topic.

2. Challenge Based Learning Methodology

Research has shown that student-centered learning approaches are efficacious in improving student learning [5]. In particular, the challenge based learning (CBL) methodology proposed by Apple Computer Inc., which employs a multidisciplinary approach in encouraging students to use their knowledge and technology to solve real-world problems, has reported to yield outstanding results [6]. The challenge approach works because most students are familiar with the concept since they have watched multiple reality TV shows

that are based on it. The common theme is that contestants are presented with a challenge that requires them to draw on prior learning, acquire new knowledge, work as a team, and use their creativity to arrive at solutions. Another reason why this concept is successful is that the participants are highly motivated by the common goal of potentially winning a big reward afterwards.

The challenge concept has been applied to the development of cybersecurity skills among high school and college students. One example is the U. S. Cyber Challenge sponsored by the Center for Strategic and International Studies (CSIS), the SANS Institute, the U.S. Department of Defense (DoD), universities and private industrial firms [7]. It is both a national cybersecurity talent search and skills development program. High school students compete on-line in the CyberPatriot Competition sponsored by the Air Force Association where they learn how to control computer networks, defend and protect computer systems from cyber threats and hackers. High school, college and graduate students participate in the DoD Cyber Crime Center (DC3) Digital Forensics Challenge and the NetWars competition. The DC3 Digital Forensic Challenge is an on-line event that tests students on individual scenario-based, investigative tools, techniques and methodologies. The competition fosters innovation among students and encourage them to provide technical solutions for computer forensic examiners in the lab and in the field. The NetWars is an interactive security challenge that tests students‘ security knowledge and capture the flag skills. Successful contestants in these competitions are immediately recognized and invited to attend regional security camps, national challenges, or given grants or scholarships to study cybersecurity.

Apple Computer Inc. has applied CBL to the collaboration project, Apple Classrooms of Tomorrow (ACOT), between public schools, universities, and research agencies with great success [8]. In this study, we adapt the CBL methodology to teach practical cybersecurity education to a team of nine CS/IT students with different backgrounds of computer education. Some members are sophomores and some are seniors. Most students have no prior formal training on cybersecurity. They enroll in this study in addition to taking their regular course load.

The CBL framework, as shown in Figure 1, is implemented in this study as follows:

2.1 Big Idea

The team considered the topic: Cybersecurity, which has broad meanings and importance to the students and society.

2.2 Essential Questions

The team came up with the following questions that reflected their interests and the needs of the community:

- What kind of information does one need to keep secure? The classification of information would dictate the security, management, use and disposition of these data. For those that have been classified as Confidential, such as Personally Identifiable Information (PII) and Protected Information, federal, state laws/regulations or organization rules may govern how they should be protected.
- What does one do to safe guard Confidential information?
  Depending on whether the threat is internal or external to the organization, the methods of safeguarding information are different. In the case of internal threats, one may have to take precautions against social engineering tactics. In dealing with external threats, the most effective way is to secure the network and computer systems.

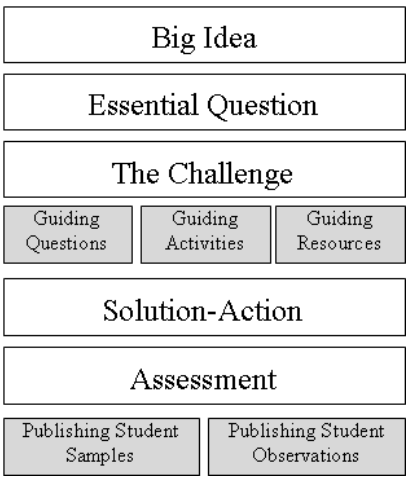

Fig. 1: The CBL Framework

2.3 The Challenge

For each essential question, a challenge was formulated that asked the students to come up with a specific answer or solution. In our study, the students came up with:

- Keep confidential information safe
- Keep network safe from cyber attacks

2.4 Guiding Questions

Students generated questions that they would need to discover solutions for in order to meet the challenges. Some guiding questions were:

- What are social engineering tactics? How does one guard against them?
- For sensitive information such as administrator passwords, how can they be changed frequently without the excessive burden of remembering the changes?
- How does one know that the organization is being attacked?

- What are the techniques of configuring firewalls to secure the perimeter of the network?
- What techniques do attackers use to penetrate a network's defense?

2.5 Guiding Activities

The students held weekly discussions with the coach, learned network security techniques from our university IT security experts, attended seminars, practiced on their own time the installation of different computer operating systems and software applications, and practiced configuration of network services such as Domain Name Service (DNS), Network Information Services (NIS), mail server and firewall etc.

In order to gain practical knowledge, the students competed in the Northeast Collegiate Cyber Defense Competition (NECCDC) [9] and the MIT Lincoln Laboratory/CSAIL Capture the Flag competition (MITCTF) [10] against their peers from universities in the Northeast region. In these two competitions, students got a chance to practice what they had learned. They defended against cyber attacks as well as generated attacks onto others in a simulated live networking environment.

2.6 Guiding Resources

Students did their research using books, class lecture notes, papers, the Internet and expert opinions in developing solutions to their guiding questions. They watched videos on the Internet to learn how to fend off social engineering tactics. They purchased equipment, set up and maintained a small standalone network that allowed them to practice network security exercises.

2.7 Solutions

Students devised situation-specific solutions as well as general solutions during the two competitions. Critical aspects of computer system configurations such as firewalls, bound ports, logging, updating, and user accounts were itemized and worked on by the entire group. Students learned how to whitelist needed ports in the firewall, scrutinize event logs for possible break-ins, and update operating systems and applications.

The group debated on user account management and came up with a solution in protecting passwords from people stealing them via social engineering tactics. In general, the most effective method against them is to change passwords frequently. Unfortunately, this increases the burden of users having to remember many different ones. Some users resort to writing them down on a piece of paper or their notebooks, and these are easy targets for people to steal them using social engineering means. To alleviate this burden, students came up with a password selection card from which the password could be derived using a code sequence. This solution greatly reduced the chance of attackers stealing the password because they had to pilfer the selection card, the code and the way to interpret the code in order to construct the exact password. At the NECCDC, this approach was openly recognised as a good idea.

3. Cybersecurity Competitions

The two major activities in which students applied the knowledge they had learned were the NECCDC and the MITCTF competitions. The NECCDC is an annual competition to train students on managing and protecting an existing network infrastructure from a group of unbiased "Red Team" attackers. These attackers comprised of Information Assurance (IA) professionals who were very experienced in computer security. In NECCDC 2011, eleven universities from the Northeast region competed. Each team was given an identically pre-configured computer network which simulated that of a working business. Teams earned points by maintaining the availability of services and integrity of the systems. Participants were not allowed to attack the networks of the "Red Team" or other student teams.

In preparation for the event, the University of Massachusetts Boston team set up a network of computers using the topology provided in the rules. Two learning groups were formed based on the students' expertise. One focused on maintaining services and the other on network/system security. During weekly meetings, methods to defend the system/network and install various services were researched and practiced. As the days for the competition approached, the team's focus shifted towards formulating a strategy, and created lists of tasks needed to be completed. Specific roles were assigned to each of the members and a hierarchical communication structure was established.

At the competition, each team was presented with an identical network of computers, switches and routers. Students were given instructions (or injects) by a member of the "White Team" acting as a liaison for the company. Examples of these injects included generating audit reports, setting up a network printer, installing new software and services, and updating existing packages. From the very beginning, the team was bombarded with an onslaught of attacks from the "Red Team". The need to simultaneously maintain business services and defend the network against attacks created a stressful, fast-paced learning environment. After a three-day struggle, the NECCDC competition ended with the University of Massachusetts Boston team placing in the last place.

After the competition, the team got together and did an assessment. The general consensus was that the team learned a lot from the experts on defending the network. This included utilities such as, netstat, ncat, lsof, operating system internals and others. Also, this competition pointed out knowledge we did not know; for example, securing the Cisco router and switch against attacks, knowing whether or not our systems were compromised, and how to setup a

spanning port to track all traffic on the network. The students realized that there were communication problems during the competition. As a result, a smaller core team was formed and it consisted of motivated students with higher networking knowledge. Meetings became more effective in exchanging ideas. The team was better focused and spent time on studying web applications, researching Linux vulnerabilities and properly configuring services.

The MITCTF competition, hosted by MIT Lincoln Laboratory and MIT Computer Science and Artificial Intelligence Laboratory (CSAIL), was also focused on educating and increasing students‘ awareness on cybersecurity. In 2011, there were thirteen teams in the competition and the goal was to test students on their knowledge of cyber offensive and defensive techniques. They defended and attacked a plug-in based Content Management System (CMS) which simulated a working business website hosted on a local server. Before the competition, MITCTF ran training sessions on the CMS details, cyber defense basics, web-based attack vectors, and also provided a downloadable virtual machine image for students to practice on.

At the competition, each team was given a virtual machine image where flags, consisting of a string of random characters scattered throughout the file system, would rotate every five minutes. Opposing teams attempted to capture these flags and submit them for points. Grading was based on the availability of the sites, the number and integrity of flags captured. Throughout the competition, teams were required to install new plug-ins to the CMS. Each new plug-in introduced new vulnerabilities, requiring patches to be implemented and exploits to be developed on the spot. Failure to do so could potentially allow opposing teams gaining access into systems and wreak havoc.

Prior to the competition, using the virtual machine image provided by MITCTF, students studied the provided code and discovered system vulnerabilities and improper configurations. They also spent time on developing scripts to secure their own system and exploit others. During the competition, the team was able to break into other systems using these scripts and caused havoc to them. These scripts included SQL Injections, Cross Site Scripting, and a PHP vulnerability on a calculator plug-in allowing execution of arbitrary code. After two days of competition, the University of Massachusetts Boston team was placed second among all thirteen teams.

4. Student Learning Results

Research has shown that group dynamics plays a crucial role in student learning [11]. In our CBL study, the group formed had various levels of technical expertise. Students were encouraged to participate in open discussions and work together in smaller groups based on their expertise. Meetings served as a conduit for students to research topics, voice their questions and opinions on topics which they had no prior knowledge. This was an important aspect in improving student learning.

After performing assessments, outcomes of our study are summarized as follows:

In Figure 2, most students reported that their computer skills increased at the end of the study. For example, one student started training without a strong background in Linux and is now proficient enough to teach other students on how to configure Linux. This perceived increase in computer skills can be interpreted in two ways: they acquired new knowledge, or applied what they already knew in different ways.

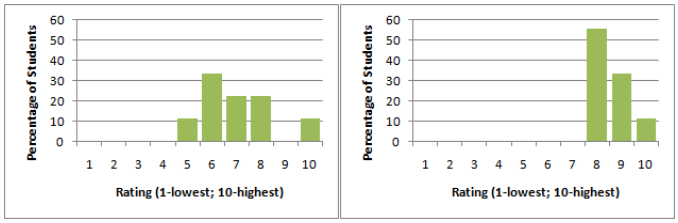

Fig. 2: Student’s self-reported computer skills, before (left) and after (right) the study.

There was an improvement in perceived computer security skills as shown in Figure 3. Very few students prior to the study knew anything about computer security. Afterwards, they all seemed to have understood what the field of security involved and felt that they had gained knowledge in this area. The improvement in skills could be influenced by the frequent interaction with students that had high technical expertise, as well as industry experts, such as the “Red” and “White Team” members during the competitions.

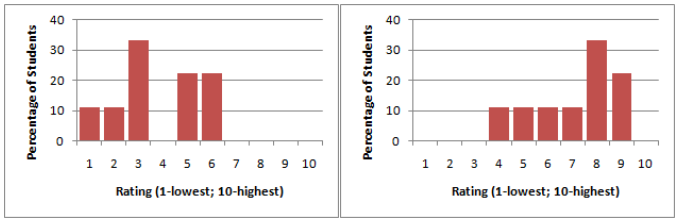

Fig. 3: Student’s self-reported security skills, before (left) and after (right) the study.

There was a sharp increase of student interest in computer security after the study as depicted in Figure 4. This may be due to the frequent meetings where students learned from each other. Another reason is that students saw how their knowledge was applied in a real world environment. Several students from the team, after the study, formed a new student group with the purpose of spreading security knowledge and interest among other fellow students in the CS department.

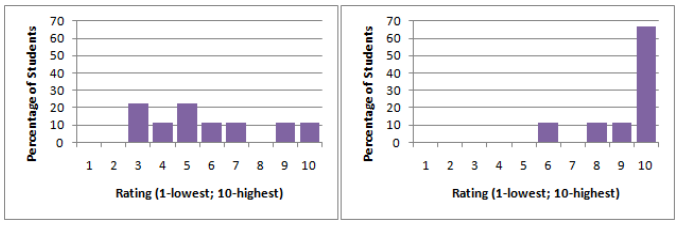

Fig. 4: Student's self-reported interest in computer security, before (left) and after (right).

Figure 5 shows that about half of the students, after going through the study, felt they could teach computer security and half could not. Although all students gained computer and security skills, some still did not feel comfortable enough to teach others.

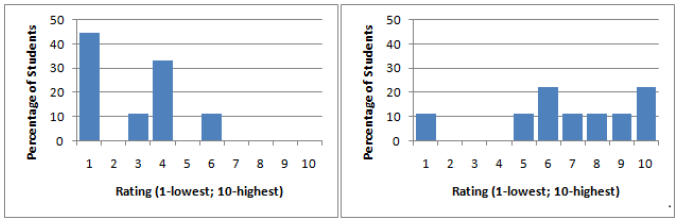

Fig. 5: Student's self-reported ability to teach others security topics, before (left) and after (right).

Although the students came with a range of technical abilities and initial interest, Figure 6 shows that all students who participated in the study benefited greatly from the CBL experience. These benefits included knowledge gained by networking with industry professionals, improving computer and security skills, and applying these skills in a practical, real world environment.

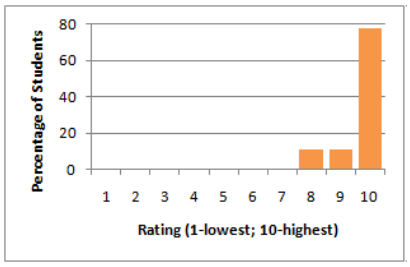

Fig. 6: Student's self-reported benefit of the study.

5. Student Observations

Our study is based on one student group comprising of students with different skill levels. Though the sample size is small, we believe the CBL methodology is beneficial to teaching cybersecurity education. Our student group exhibits the six team basics required for high team performance [12].

In this study, we formed a small group of nine students. Group members had complementary skills in computer programming and course knowledge. Some students had working Windows and Linux knowledge, while others had none. The team shared a common purpose of increasing their computer security knowledge. Team members knew they had to achieve a common set of specific performance goals. In this study, these performance goals were specified by the competition organizers. For both NECCDC and MITCTF, students were aware of the services they needed to install and maintain. Throughout the study, students agreed on a common working approach. This included meeting and discussion in a democratic manner. Students with technical expertise tended to guide in this area by suggesting topics to research and troubleshoot configurations. Students voted to decide which direction to take. For example, if no students were familiar with a piece of software application or tool, then the group jointly determined the best course of action to take. All group members felt they were mutually accountable for the success of the team. In our case, the group was highly critical of each others' performance. Students divided up technical functions such as email configuration, central authentication, and DNS; they were then held responsible for that function. If a student did not master the configuration and security for that function, other students would remind him that he needed to do so. Each student expected other students to become experts in some technical area or some configuration of a particular system after they had studied it.

In our study, students found the guiding activities in participating in the NECCDC, and MITCTF competitions most beneficial. The competition provided a real-world cyber defense situation that our students practiced their knowledge on. Students were forced to work in an intense atmosphere that they had to band together to work as a team in solving a problem. Each team member contributed to the solution based on his individual training. Also, what students found most stimulating were discussions with security professionals from industry afterwards and learning from them techniques on securing the network. They also appreciated the opportunity to network with company recruiters and students from other universities in sharing their experience.

Though the CBL methodology seems to improve overall student learning, its benefits vary from one student to another based on their interest and motivation. As compared to that of conventional teaching methodologies, CBL student learning depends more heavily on self-study and peer instruction efforts. Those who are not sufficiently motivated to learn new concepts or technologies on their own have less to gain. Furthermore, those who have less interest tend not to show up at the meetings as often. Since these activities are mostly student-organized, there is no penalty for not showing up except for the fact that these students will learn less. Also, the presence of indifferent and unmotivated individuals

hinders the progress of the group.

The loose structure of the teams in CBL, though beneficial to some team members, may not work for others. The lack of an instructor-student hierarchical structure may not give enough direction for some students to follow. As a result, they lose the motivation of attending meetings. Student ability is also an important factor in learning a highly technical subject such as cybersecurity. For example, the students need to have basic knowledge in networking and scripting in order to configure the firewall to fend off attackers. These are not only key security concepts, they are also vital skills for system administration. Without them, they cannot learn how to secure a system in a short time. Consequently, more experienced students have to spend time teaching the less knowledgeable ones. This slows down the team's progress and reduces their overall learning. These observations suggest that the CBL methodology, especially on teaching a highly technical subject like cybersecurity, can achieve a better outcome if all team members start with the basic prerequisite knowledge.

Although our CBL study does not need much instructor intervention, it requires additional resources, such as equipment and support staff to support the activities of the group. For example, to build a practice network, the students need dedicated computers, routers and switches. This equipment is often deployed at irregular times and their malfunction requires off-hours support. Also, because this study deals with computer security, students have to negotiate firewall policy with the university's IT department so that the practice network will not be blocked from the Internet. These difficulties highlight the importance of additional support resources and their flexibility in support hours that are needed to effectively apply CBL to cybersecurity education. However, we believe that the potential gain in student learning justifies the extra effort to overcome these obstacles.

6. Conclusions

This paper has described the application of the Challenge Based Learning methodology to cybersecurity education. By formulating challenges based on students' interest in securing information and systems, students worked together as a team on devising solutions to meet the challenges. Students in this study practiced what they had learned in two cybersecurity competitions. Formative assessments performed showed that students benefited greatly from the CBL approach, though the amount of benefit varied from one student to another. The students were able to improve their computer skills, security knowledge, ability to teach others and interest on the topic of cybersecurity. Though the approach may require additional support resources and may require meetings at irregular hours, the increase in student learning justifies the extra effort.

7. Acknowledgments

This research was supported by the Spring 2011 Program on Instructional Innovation (Pi2) grant, the College of Science and Mathematics, University of Massachusetts Boston. The authors would also like to thank the UMB-NECCDC team members for their participation in the research.

References

[1] M. McConnell,"To win the cyber war we have to reinforce the cloud", Financial Times, April 24, 2011. [Online]. Available: http://www.ft.com/cms/s/0/078bf734-6e9b-11e0-a13b-00144feabdc0.html

[2] K. Evans and F. Matters, "A Human Capital Crisis in Cybersecurity", Center for Strategic and International Studies (CSIS), Nov. 15, 2010. [Online]. Available: http://csis.org/files/publication/101111_Evans_HumanCapital_Web.pdf

[3] J. Vijayan, "Cybersecurity bill passes first hurdle", Computerworld, March 24, 2010. [Online]. Available: http://www.computerworld.com/s/article/9174065/ Cybersecurity_bill_passes_first_hurdle/

[4] (2011) "Security Lessons still lacking for Computer Science grads", InfoWorld. [Online]. Available: http://www.infoworld.com/t/application-security/security-lessons-still-lacking-computer-science-grads-769

[5] G. O'Neill, T. McMahon "Student-Centered Learning: What does it mean for students and lecturers", University of College Dublin. [Online]. Available: http://www.aishe.org/readings/2005-1/oneill-mcmahon-Tues_19th_Oct_SCL.html

[6] L.F. Johnson,R.S. Smith, J.T. Smythe, R.K. Varon "Challenge-Based Learning: An Approach for Our Time", The New Media Consortium, Austin, Texas. [Online]. Available: http://ali.apple.com/cbl/global/files/Challenge-Based%20Learning%20-%20An%20Approach%20for%20Our%20Time.pdf

[7] (2011) "U. S. Cyber Challenge", Cybersecurity Workforce Development Division, Center for Internet Security. [Online]. Available: http://workforce.cisecurity.org/

[8] (2011) "Challenge Based Learning- Take action and make a difference", Apple Computer Inc.. [Online]. Available: http://ali.apple.com/cbl/global/files/CBL_Paper.pdf

[9] (2011) Northeast Collegiate Cyber Defense Competition (NECCDC) on March 4-6, 2011 in EMC Corporation, Franklin, MA. [Online]. Available: http://www.ccs.neu.edu/neccdc2011/index.html

[10] (2011) MIT Lincoln Laboratory/CSAIL Capture the Flag Competition on April 2-3, 2011 in MIT, Cambridge, MA. [Online]. Available: http://mitctf2011.wikispaces.com/

[11] D.R. Forsyth,Group Dynamics, 5th ed., Wadsworth Publishing, 2009.

[12] J.R. Katzenbach, D.K. Smith. "The Wisdom of Teams", New York, NY: HarperCollins, 2003.