Cyber Defense Competitions and Information Security Education: An Active Learning Solution for a Capstone Course

Conference Paper · February 2006

DOI: 10.1109/HICSS.2006.110 · Source: IEEE Xplore

CITATIONS
47

READS
51

1 author:

Wm. Arthur Conklin
University of Houston
31 PUBLICATIONS **144** CITATIONS

SEE PROFILE

Cyber Defense Competitions and Information Security Education: An Active Learning Solution for a Capstone Course

Art Conklin
Center for Infrastructure Assurance and Security
The University of Texas at San Antonio
art.conklin@utsa.edu

Abstract

The content of information security curricula spans a wide array of topics. Because of this variety, a program needs to focus on some particular aspect and provide appropriate depth of education. Active learning theory provides insight into methods of increasing skill development and retention through specific instructional methods. Applying active learning to a capstone course in information security centered around management of security in a business setting has been shown to be highly effective. Using a Cyber Defense Competition to provide a hands-on opportunity for students to test their skills and develop team based management skills in an operational business environment impacts many constituencies. Participating students learn in a true active learning environment. Instructors are able to evaluate the thoroughness of their curriculum in its intended setting. Other students learn as teams prepare for the competition. In the end, everyone feels they had learned important lessons.

1. Introduction

The topic of computer security, sometimes referred to as information assurance, network security or information security is becoming increasingly popular in college programs. Driven by industry need for professionals with this skill set, numerous institutions have risen to the challenge of developing curricula to address this need. As the breadth of this topic is wide, from network design, to secure coding, to management of security, there exists a wide array of curricula, with different programs having differing emphasis.

The purpose of this paper is to explore issues associated with an information security management curriculum and how to effectively develop the necessary skills to be a successful professional in this challenging dynamic career field. This information was developed from actual classroom experiences at The University of Texas in San Antonio (UTSA), an NSA designated National Center of Academic Excellence in Information Assurance Education.[1] The graduate curriculum is designed around the management aspect of information security and is designed to produce future leaders and managers in this field.

To facilitate the development of student skills in this challenging field, the practice of active learning was adopted. Active learning is a means of delivering content using hands-on activities that involve the student directly in the learning process.[2] In addition to actively involving the students in the process, team based work was included forcing collaborative learning.[3] Many of the management challenges that will face professionals in the field of information security will require multiple people with differing skills to work together. Experiencing this during the educational process better develops the students for coordinated collaborative activities needed to succeed professionally.

The graduate level curriculum includes coursework in security principles, incident response, digital forensics, and security assessments. The first three courses are primarily lecture classes with minor lab components. The assessment class has a major hands on component designed to utilize active and collaborate learning modalities.[4] This past spring, a new educational opportunity, a collegiate cyber defense competition was hosted by UTSA, offering students from regional universities the opportunity to test their skills and enhance their learning in a simulated operational business environment. [5] The outcome of this event as measured in exit surveys of the participants, both student and faculty, was enlightening. All parties felt that their preparation needed fine tuning and all felt that the addition of this active learning exercise provided them with much desired opportunities to enhance their education.

The incorporation of a preparatory class leading up to the competition is being considered by several universities that participated in this inaugural event.

0-7695-2507-5/06/$20.00 (C) 2006 IEEE

Faculty sponsors from several attending institutions recognized the value of active learning in a cooperative team based environment, coupled with the required active decision making necessary to succeed. This competition is a free form business environment event, requiring both simple decision making and execution as well as complex collaborative decision making based on team determined priorities. Performing in real time, the students had the opportunity to integrate their classroom learning, their previous experiences as well as those of others on the team to determine their activities in their quest to maintain an operational business environment in the face of common security threats that face e-businesses everyday.

2. Active and Collaborative Learning

A Chinese philosopher, Lao Tzu (6th Century BC), said: "If you tell me, I will listen. If you show me, I will see. If you let me experience, I will learn." This is the basis for active learning. Active learning is an interactive process where the student participates in the learning process. In a standard lecture class, where the professor lectures and then the student goes home and does homework, the active part of the learning is isolated, without the benefits of interaction with the faculty member. Likewise, having the student perform a laboratory exercise, where the exercise is a series of steps with defined outcomes is also interaction free. Higher levels of student involvement over time in the learning process yields greater skill building achievement. Studies have shown that including an interactive component that forces interaction with others as part of the learning experience increases the effectiveness of the class in developing student skills.[6]

As much of today's working environment is based around team activities and collaborative working environments, the use of collaborative methods in instruction seem appropriate. Building a team from members of differing skills, who are working together towards a common cause, utilizing each member's strengths and mitigating individual weaknesses has proven very successful in many business environments. When the tasks are complex and difficult, when it is impossible for a single person to possess the information needed to span the problem and solution, teams are attractive options. Effective teams require efforts in team building and skill development to work not in isolation, but together towards the common overall objective. The challenge of multiple paths and contradictory included objectives make team based management a challenge.

Computer security management is an ideal place to practice team based management, for in the business world collaborative efforts will be a reality. One of the keys to developing the proper skill sets in collaborative work is the concept of active decision making. Frequently decisions will be required when the participants will possess insufficient information to make a completely rational choice. Additionally, many times the outcome of a choice will have impacts on others in the organization, parties that are not part of the decision making process. Learning to make decisions on imperfect information and to prioritize and justify impacts is a necessary skill to be an effective professional in computer security. Designing learning environments to involve students directly in this form of active decision making is a valuable experience.

With respect to information security education, active learning could be undertaken in the classroom, through the use of laboratory exercise, team assignments or large events such as the cyber defense competition. The best answer is a blend of all of these, each where each is appropriate. The value is in having a mixture of education styles, each aimed at achieving an appropriate goal. Lecture based material is probably the best answer for many principles and fundamentals classes, where as laboratory exercises work very well in classes such as forensics and assessments.

The primary opportunity for active and collaborative learning is in the cyber defense competition. This opportunity is not just in the competition itself, but also in the preparatory phases the teams go through to get ready for the event. Preparing a team for an event of this magnitude is a large scale learning exercise in its own right. Faculty members need to engage the students in self driven learning, for it is the student teams that will be tested, the advisors are not an active part of the competition. This makes the preparation phase an ideal time to exercise both active learning and collaborative learning principles.

3. Information Security Education

Information security education is a wide ranging subject, with specifics in network security, secure coding principles, security management and other realms. When developing a curriculum in this realm, the developer must decide on the scope of coverage and depth. Attempting to cover all aspects would lead to shallow depth, and focusing on a specific aspect would achieve depth at the expense of breadth. A common curriculum used in business schools and

information systems departments is one based on the management of the information security function.

A management based curriculum will typically have a broad based introduction class to cover the breadth of the issues at a limited depth. Then electives are offered to achieve a deeper understanding of a limited set of issues. It is common to have a final capstone class to pull all the learning together into some project based event to facilitate the assimilation of knowledge by the students.

At our university, the curriculum includes an introductory level class to cover the broad aspects. After this class, a series of student chosen electives form the technical content of the program. Classes such as Incident Response, Digital Forensics, Security Policies, Access Controls and Security Assessments are among the electives being offered. With respect to a capstone class, currently the Security Assessments class offers the most comprehensive opportunity. A future opportunity built around a cyber defense competition is being explored, not only at our university, but at several others as well. The opportunity afforded students to put it all together and see where theory meets reality has drawn significant interest from both students and faculty.

Based on the positive results from the cyber defense competition, minor changes throughout the existing course offerings are being prepared. Targeted guest lecturers from industry to shore up critical points are being added, as are new modules to attempt to integrate student knowledge across the classes in a real world setting. Although major changes to curricula, such as adding courses, can take years for approvals, much can be done within the current existing structure based on the lessons learned from the competition, and these are being pursued.

4. Cyber Defense Competitions

Competition has been a part of university life for decades. Sporting events and rivalries have galvanized institutions and alumni into alliances benefiting both parties. Pride and honor drive many in the pursuit of winning, a task requiring much preparation and training. Using this same model to promote learning, the engineering community has produced competitions for concrete canoe races, robots and software programming challenges to name a few. Other curriculums have similar academic competitions specific to their fields of interest. The development of competitions surrounding cyber security is not new, with a history of capture the flag activities dating back many years at the annual DEFCON convention. The appearance of cyber defense competitions at universities is merely an extension of a proven learning model in other curricula.

4.1. Existing Competitions

The use of cyber defense competitions in an educational setting can be traced to the United States Military Academy sponsored Cyber Defense Exercise (CDX). CDX was created in 2001 to serve as the capstone course in their information assurance program.[7, 8] The emphasis of this event is on being able to maintain an operational military network in the face of a hostile force attempting to breach the security of the network. As part of the educational experience, each team designs, implements, and maintains an operational network consisting of a variety of platforms to meet requirements laid out in the CDX objectives. This event is heavily driven by military network requirements and testing is done using military information warfare units. Each year the US service academies compete with the objective of bringing home the trophy.

A product of the CDX was an NSF sponsored workshop to explore the opportunities to migrate a CDX type event to information security programs in the university environment.[9] One of the products of this workshop was a comparison of several formats for conducting cyber defense competitions. There are numerous activities of this nature across the university programs with several different objectives and outcomes. The events have ranged from single institution events like competitions at The University of Texas at Austin, and Texas A&M University, to international events such as the one at the University of California at Santa Barbara.[9]

These competitions ranged from student led activities to faculty led activities based on coursework requirements. Some were based on the military CDX concept, while others were attack and defend activities like DEFCON's capture the flag event. Based on inputs from these events and the workshop, The University of Texas at San Antonio embarked on developing a competition based on operational business and computer security principles. The inaugural event was conducted in the spring of 2005 with five schools attending the event over a weekend in April.

4.2. Cyber Defense and Business

A key decision in developing a comprehensive event based educational class is the scope of operations associated with the event. There have been numerous debates within the information security community about the value of offensive computer

security operations. One camp argues that learning how attackers think and attack is essential in learning how to defend. The other camp focuses on the fact that students are being prepared for careers that by and large will not include offensive tasks and that teaching hacking only opens the community up to criticism and liability.

Information warfare and the offensive aspects of attackers, both techniques and mindset are an important part of a complete information security education. A subset of these skills is used in the penetration testing portion of the assessment class, where student teams perform actual penetration testing, both internal and external, against a client network. [4] Although offensive games and capture the flag type events are very attractive to students, to use them for the focal point of a capstone level class is not appropriate.

Designing a realistic event driven scenario to test student abilities and provide an educational test-bed to encourage growth and collaborative teamwork dictates the use of a business scenario. Business will employ the vast majority of our graduates and they will be operating and defending operational business networks, not playing capture the flag. Using this as a rational, an operational business environment was chosen.

There is still the need to have an offensive activity element in the scenario for the students to practice defensive skills. For this element, a corporate red team was used for several reasons. First and foremost was a matter of control. The red team element in the competition is an integral part of the competition and it needs to be applied equally across all teams in a measured fashion. The competition is about defending, and maintaining a network, in an educational setting. Permitting a red team to erase a server, just to show they can, serves little purpose in the time based element of the competition. If the objective of the competition is to allow the teams a chance to learn, then destroying them serves no educational purpose.

From a standpoint of competitive propriety, neutral parties did all aspects of the scoring. This means that the members of the red team (attackers) and the white team (judges) were independent of the teams in the competition. Managing this aspect when the red team came from students could present a conflict of interest or at least be perceived as one by the teams. Service uptime scoring and traffic generation were also neutral, being performed by automated services.

Picking a defensive competition in an operation business setting is designed to serve the largest number of students in their future career endeavors. Developing a competition that had conflicting requirements, forcing decisions by the teams without complete knowledge of scoring was purposeful to simulate the real world business environment where outcomes are frequently not fully understood ahead of time. Using this competition as an active and collaborative learning environment allows all the previous coursework and theories to be put to the test of reality. Having a large enough event, with business related aspects changes the focus from a technical computer security exercise to a learning laboratory where team work is needed for success.

4.3. Collegiate Cyber Defense Competition in Detail

Based on the NSF workshop, members from the Center for Infrastructure Assurance and Security (CIAS) at The University of Texas at San Antonio joined forces with representatives from The University of Texas at Austin and Texas A&M University. The objective of this steering committee was to design and develop a cyber defense competition embodying the principles laid out at the NSF workshop.

One of the overriding concerns was to develop what was perceived to be a fair and level playing field for all of the participants in the competition. For this reason, a common setup was developed, one that would be used by all teams. This setup was designed to mimic a small business entity, with file server, web server, e-commerce site, employee portal, mail server, domain server and database server. A mixed environment of Linux and Microsoft platforms acted as the backbone with networking equipment provided by Cisco.

Each team was scored on three elements – their ability to keep required services up and running, their ability to react to business generated injects and their ability to keep hostile elements at bay. At the beginning of the competition, all the networks were fully functioning, although not at any given patch state. The teams were told they had bid and won the contract to run the company network, and that the previous firm was fired due to non-performance. Although the teams were free to reorganize the equipment in any fashion they chose, any service outages would be counted against them.

To give the teams a chance to minimally patch their systems, the red team did not begin operations until two hours into the competition. The student teams were aware they had a quiet period, but they did not know the true length. Each team was allowed to bring a box to the event preloaded with patches and

freeware tools to assist them in this aspect in a timely fashion.

Business function injects were periodically provided to the teams and scored in a timed fashion. An example of a business inject would be the addition and or deletion of people, and their access, the movement of people and permissions between departments, the addition or removal of network equipment (day 2 saw a new PIX firewall arrive, on another occasion a server "suffered a power supply failure"). Some of these events were designed to create busy system administration work, others were designed to force the students to change plans and make decisions. Teams were required to produce management reports detailing their "billable" activities. Tasks assigned in day one (permission changes) had impacts on day 2 and 3, so even if they were not done on time, if the team ignored them, they were continually penalized. The overall objective of the competition was one of balance.

A complete description of the event is beyond the scope of this article, but can be found in White, et. al.[5]

5. Conclusion

When we embarked on the journey to develop and deploy a cyber defense competition, the focus was on providing a learning opportunity for the students. At the conclusion of the event, we surveyed faculty and student participants as to the level of preparedness they felt they had, the level of reality simulated by the environment and solicited inputs for future events. After conducting the event and reading the surveys, several factors came to our attention.

First and foremost, none of the teams felt adequately prepared for the event. Part of this was due to the inaugural nature of the event and no past knowledge, and part was by design – the event was specifically designed to be overwhelming to any single individual. Each team had its own specific weaknesses and each team went home determined to correct them. From an outsider's point of view, the red team, led by professionals from the defense industry, were impressed with the ability of the teams. The red team rated them all as competent and well within expected capabilities of industry. This was a very positive result for all of the attendees.

Second, each school went home with thoughts on how to improve their performance. And these thoughts were aimed at curriculum changes to better prepare them and fill missing elements uncovered during the competition. Student chapters of ISSA were formed at a couple of schools, aimed at better connecting students, academia and industry around a common objective. These dynamic, yet focused changes will improve each institution's offering and better prepare students for future careers.

Industry involvement in the competition is leading to further industry involvement in the academic programs, providing key speakers for targeted classes and other opportunities to work together for the students benefit. Industry sponsors provided key funding, without which this event would not have been able to occur.

Observing the interactions of the teams during the event, the judges noticed the value of team work and how different teams struggled to work together. Some were more organized than others, but the competition and its events forced all teams to depart from their pre-event plan and make decisions and change during the event. Watching the students learn as they interacted with the events being presented to them was a case study in team building. Each night, while going to their rooms to rest, teams held meetings with their faculty advisors, drafted new game plans and alternates for the coming day's events. This type of learning environment can not be duplicated in an ordinary classroom and surprisingly proved to be one of the most popular aspects of the event based on student responses.

The overall impact of this competition is wide. It spans obviously the students who directly participated, for they were exposed directly to the competition itself. It also affected the faculty advisors and other students, for although they were not allowed in the actual competition rooms, they did consult with the students each night and they were involved both in pre-event preparation and post-event analysis. The direct exposure of the students was also carried back to their representative campuses in the form of "war stories" as schools have already begun preparations for the next event. As curriculum changes and adjustments are made, the impact of the event will indirectly affect other students as well.

To prepare for future competitions, several schools have examined forming a class to allow direct instructor student interaction within the realm of a systems approach to computer security in a business environment. It became clear during the inaugural event that a cross discipline team approach was best and also necessary to be competitive. Removing the competitive aspect and focusing on the education perspective, there was a significant level of interaction between team members during the event, and this interaction was founded in part based on their differing backgrounds. Although in some circumstances, a diverse background is not a recipe for success in the classroom, in the specifics of this task, it is a key ingredient. This leads to content and

grading issues in the class because of the diverse background of students. Specific issues such as what content would be used in the class, grading criteria and how to handle the multi-disciplinary nature of the topic are being worked out by each instructor within their own institution's guidelines.

Because of the size constraint on the actual competing team, a mechanism needs to be in place to determine team membership without disrupting the rest of the people in class. Only one institution faced this in the inaugural event, and they chose members based on demonstrated skill levels throughout the class preparation time, maintaining both a drive for the best and a diverse team. In the end, the team formulation concept turned to bite them as they found through the competition that their team, although individually strong and diverse was missing technical ability in setting up firewalls. In spite of planning and best efforts, this gap in skills hurt the team throughout the competition.

The impact of organizing student groups associated with computer security, affiliated for instance with ISSA, is also a positive one. Engaging student-industry interaction exposes the students to their potential employers and opens doors through new relationships built on common objectives. Increasing faculty-industry partnership is also helpful, both in terms of connecting faculty to the current state of the industry and in the aspect of outside resources for their classes. Both of these results have already been observed in the two months after the competition.

Based on these results and encouragement by leaders in industry, UTSA announced at the 9th Colloquium for Information Systems Security Education in Atlanta, Georgia, that they were organizing additional regional events for the spring of 2006, culminating in a national event between winners in the late spring 2006.

6. References

1. *Centers of Academic Excellence*. 2005, National Security Agency. Available at: http://www.nsa.gov/ia/academia/caeiae.cfm
2. Felder, R.M. and R. Brent, *Learning by Doing.* Chem. Engr. Education, 2003. **37**(4): p. 282-283.
3. Resta, P. *Project CIRCLE: Student Mentors as a Strategy for Training and Supporting Teachers in the Use of Computer-Based Tools for Collaborative Learning*. in *Proceedings of Computer Support for Cooperative Learning 1995*. 1995. Bloomington, IN: Indiana University.
4. Conklin, A. and G. White. *A Graduate Level Assessment Course: A Model for Safe Vulnerability Assessments*. in *Proceedings of the 9th Colloquium for Information Systems Security Education*. 2005. Atlanta, GA.
5. White, G.B. and D. Williams. *The Collegiate Cyber Defense Competition*. in *Proceedings of the 9th Colloquium for Information Systems Security Education*. 2005. Atlanta, GA.
6. Bonwell, C.C. and J.A. Eison, *Active Learning: Creating Excitement in the Classroom.* ERIC Digest, 1991.
7. Schepens, W.J. and J.R. James. *Architecture of a Cyber Defense Competition*. in *2003 IEEE International Conference on Systems, Man & Cybernetics*. 2003.
8. Schepens, W.J., D.J. Ragsdale, and J.R. Surdu, *The Cyber Defense Exercise: An Evaluation of the Effectiveness of Information Assurance Education.* The Journal of Information Security, 2002. **1**(2).
9. Hoffman, L. and D. Ragsdale, *Exploring a National Cyber Security Exercise for Colleges and Universities. Report No. CSPRI-2004-08, The George Washington University, Report No. ITOC-TR-04001, United States Military Academy*. 2004.