

# Active Learning in the Security Classroom

## Abstract

*Information assurance is a critical topic in undergraduate education and has received a lot of attention in recent literature. At our institution, we have taught multiple security courses for several years and have tried different approaches to make the material interesting and meaningful to the students. One approach that has proven effective is the application of active learning techniques. We have developed interactive visualization tools for in-class use, designed hands-on laboratories, created an inter-school assessment competition, and employed active learning activities in the classroom. All of these techniques are designed to engage the student in the learning process; to develop a deeper understanding of security concepts; and to act as a motivational tool. This paper will describe the different tools and techniques used and how they fit into an active learning approach. We will present our experience with using the tools, their effectiveness, and student reactions. Finally, we will describe our future plans for the security courses.*

## 1. Introduction

There has been a great deal of emphasis over the past decade on the importance of information security in higher education. This emphasis is a result of an increased awareness of security issues and vulnerabilities, expanded resources for security research, an increasing number of highly publicized attacks, and an increasing awareness of computer-related legal issues. Along with this increased awareness comes the demand for more effective means to teach the fundamental concepts of security.

The application of active learning techniques is one means of motivating and engaging students in the learning process. In its simplest form, active learning has been described as involving students in the classroom in activities other than listening that are meaningful and make them think about what they are doing [3]. This paper will describe means that our institution has taken to incorporate active learning into the security curriculum.

Many institutions have made great strides in developing active Information Assurance curriculum at all levels. Purdue's Center for Education and Research in Information Assurance and Security

(CERIAS), in particular, has even produced lesson plans and other materials for K-12 education. Every one of their lessons for the K-12 audience is based on some form of active learning. At the collegiate level, some of the most highly noted methods include regional and national level cyber defense and offense competitions. At our school, we have incorporated the preparation for such exercises as part of a course in order to allow students to actively reinforce the core security education objectives that they are expected to meet. MIT offers a free security camp as one means of providing awareness and education to the general public. The camp is very similar in venue to that of a conference or workshop and the degree of active learning will likely vary as it does from conference to conference.

Institutions also fuel interest and motivation by involving students in research projects. While research clearly provides a student with hands-on active learning, such projects at the undergraduate level require faculty supervision and focus in order to ensure security concepts are learned beyond the research skills acquired.

All of these practices speak to the importance of keeping the target audience and the educational objectives at the forefront of the curriculum. Information assurance education offers unique challenges to instructors from this perspective, including the multi-disciplinary nature of the subject and the draw of mass appeal from movies, novels, and spy stories which may include preconceived notions of security concepts. At a senior undergraduate level, critical and skeptical thinking are often key over-arching objectives. In security education, it can be challenging to enable students to be able to evaluate the strength and weaknesses of a security system if all they are interested in is a checklist on how to configure a system or use a tool.

The Department of Computer Science at our institution has been teaching Information Assurance since 1996. Over the past 12 years, it has developed a variety of IA curriculum, tried numerous approaches to teaching specific concepts, developed IA labs for education, and participated in Information Assurance competitions. In 2005, our institution pursued and was recognized as one of only two undergraduate-only institutions to achieve the status of a Center of Academic Excellence in Information Assurance Education.

This paper will relate some of our lessons learned and some of our current successes in focusing on critical thinking and fundamental security concepts through active learning techniques. This paper first describes recent advances in education based on active learning and recent studies related to active learning. We will then show how these concepts have been applied in the context of information assurance education at our institution with specific emphasis on techniques targeting more complex and abstract security concepts. We end by summarizing our experience and ideas for future investigation.

## 2. Active learning

The term “active learning” was popularized in the 1990s to refer to teaching techniques which seek to actively engage students in the learning process in the classroom [3]. Many educators advocate active learning techniques as contrasted to traditional lecture-based teaching in which the primary student role in the classroom is passive listening. Ideally, active learning techniques supplement rather than replace lecturing.

Examples of active learning techniques include student discussions, student presentations, in-class exercises, student role playing, and game-based learning. Paulson provides a list of 29 active learning techniques which can be applied to classrooms for any academic discipline [6].

### 2.1 Advantages of active learning

Advocates of active learning approaches cite several advantages of using active learning techniques in the classroom. One advantage of well-designed active learning activities is that they may be more motivational to students and thus hold student attention longer than lecturing alone [3]. When used at periodic intervals during a lecture, short active learning activities may also be useful in breaking up the lecture and regaining lost student attention [6]. Because many active learning techniques require students to solve problems and reflect upon what they have done, these techniques may lead to a deeper level of student understanding and better retention of the concepts being taught. Finally, active learning techniques are likely to be well-suited to kinesthetic learners who are most effective at learning by doing as opposed to learning by listening [2].

Prince also points out that assessing the benefits of active learning in general is very difficult. Still, a number of studies conclude that the use of active

learning techniques increases student learning and retention.

### 2.2 Objections to active learning

Despite the cited benefits of active learning, not all faculty members are eager to introduce active learning techniques into their instruction. First, incorporating active learning activities into classroom teaching represents a change to how many instructors themselves learned. If listening attentively to the instructor and taking notes while in class worked well for me, why should that not work well for my students?

As with any newly adopted technique, there is an inherent risk. An active learning activity may fail to adequately engage student interest or foster learning of the desired concepts. Planning, and preparing active learning activities takes time which may be a significant addition to normal lecture preparation. Also, developing or purchasing materials in support of active learning activities may require additional resources. Finally, spending valuable class time on active learning activities is likely to reduce the number of topics that can be covered during a scheduled class time.

### 2.3 Overcoming objections to active learning

All of these potential objections to active learning are easily overcome as long as the instructor is willing to try new strategies in an effort to increase student learning. Most of today’s students have grown up actively engaged with video games, cell phones, and the internet. Active engagement is a familiar and preferred way of learning for many of them.

Instructors seldom need to develop active learning activities from scratch since countless examples are easily available on the internet and in educational literature for a wide variety of disciplines. While finding an appropriate active learning activity and adopting it to a specific course will take time, if the activity is successful, that time should be amortized over many uses.

Dedicating class time to active learning activities at the expense of covering additional content can be a difficult choice. The justification for doing so clearly depends on the effectiveness of the activity relative to the alternative, usually lecturing. For well-planned and executed activities, the time required can be kept relatively short. Some active learning advocates recommend keeping these activities as short as a few minutes [7]. However, with set up and activity-specific instruction, some active learning activities

may require substantial class time. In that case, the depth of learning and retention fostered by the active learning activity must exceed the benefits of delivering additional content in the classroom.

In the next section we present our experiences applying active learning techniques in computer security courses.

### 3. Applying active learning in security

Students in our security courses enjoy classroom discussions about computer viruses, spreading worms, malicious attacks, and vulnerabilities. They are intrigued by popular press articles regarding privacy issues, denial of service attacks, and hacker activities. However, a large part of security education is understanding the concepts and theory behind these more visible end results. Students become less excited in the classroom when formally proving theorems about safety or studying an abstract formal model of access control. Instructors have reportedly heard students groan when told they would be reviewing Turing machines in preparation for formal reasoning about security provability. Relegating these important topics to dry lecture or long readings can de-motivate students resulting in lower levels of understanding and knowledge retention.

To maintain student interest in security concepts while covering more complex topics, our institution has made a concerted effort to incorporate motivational active learning techniques in our security classrooms. An example of a traditional active learning type activity can be found in our Information Warfare class. In an introductory lecture on threats and vulnerabilities, combination padlocks are passed out and students are asked to attempt to open them. A discussion follows as to how secure the padlock needs to be, what is the threat, and what is the risk (e.g., what is the impact if it is compromised?). The instructor concludes the discussion by demonstrating a method for opening the padlock without the combination. This activity generates a lot of interest and discussion – the key ideas behind active learning. In addition to the more traditional active learning approaches, such as role playing and classroom activities, we have developed a series of interactive classroom visualizations, participated in a cyber-defense competition and an inter-school vulnerability assessment exercise, and created hands-on laboratory exercises to allow students to experiment with and experience security tools and practices in an isolated environment. Each

of these activities will be further described in the following sections.

#### 3.1 Interactive classroom visualizations

Interactive classroom visualizations (ICV's) are lecture support tools designed to provide a visual demonstration of a concept or algorithm. Visualizations have a long history in computer science with several examples in algorithms, data structures, graph theory, computer graphics, automata theory, and programming languages. Many examples abound on the web with varying levels of interactivity, formats, and complexity.

At our institution, security ICV's have been designed specifically with active learning in mind. That is, they are designed for use in the classroom, not as standalone tutorials. Table 1 shows the specific ICV's that have been developed for security concepts. A complete description of the individual tools is not practical here, further information on specific tools can be found in the literature [5,8,9,10].

**Table 1. Security ICV's**

<b>ICV</b>	<b>Description</b>
GRASP	security protocol visualization demonstrating handshaking and attacks
Ciphers	interactive applets for seven different cipher algorithms, showing how they work, characteristics, and attacks
PKIVis	game-like environment for demonstrating how PKI works
Take-Grant	tool for demonstrating a formal access control model and its limitations
HRUVis	tool for demonstrating the Harrison Ruzzo, Ullman access control model, and using it to prove the undecidability of safety
CodeBlue	a version of Core War with small programs in memory battling each other demonstrating offensive strategies and relocatable code

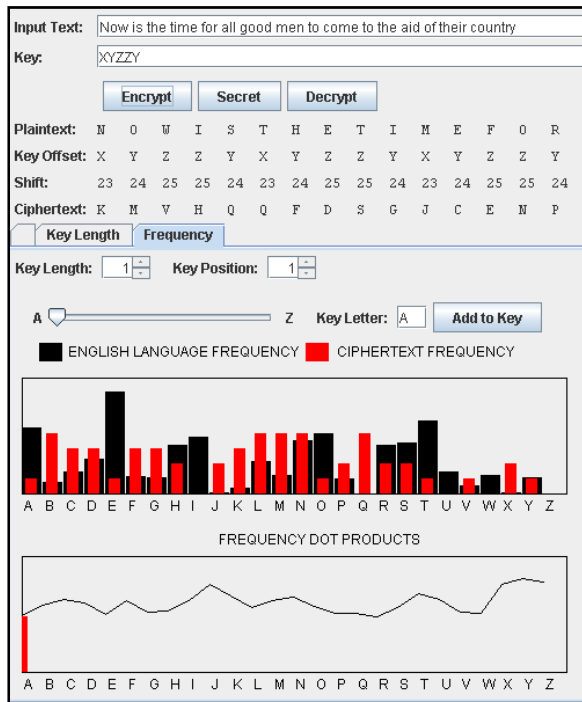
Designing ICV's for use in the classroom is different than designing visualizations for standalone use or independent study. Some of these design characteristics include:

- High level of interactivity
- Easily understood abstraction
- Limited number of concepts

- Relevance to lecture topic
- Robust user interface

Each of these will be discussed further.

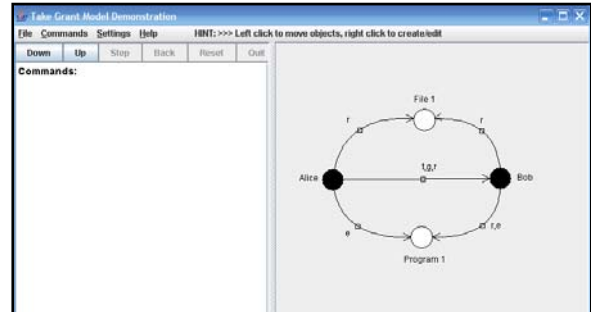
Interactivity is critical for demonstrating “cause-effect” relationships. Rather than simply visually demonstrating a concept, it is important in active learning for the student to be able to control the environment by setting parameters, specify input data values, and stepwise control the action of the ICV. By interacting with the ICV, the student participates in the demonstration and is not just an observer. An example of such interaction as part of a cipher visualization tool is shown in Figure 1. In addition to being able to set the input plaintext and key information, the student has widgets, such as the slider bar, that interactively shows changing letter frequencies and allow the student to break the cipher.



**Figure 1. Interactive cipher visualization tool**

Another design consideration is level of abstraction. Abstraction is an inherent part of any visualization. An example of an abstraction in security is representing letter digraph distributions in encrypted text with a colored 2-D heat map. When designing ICV’s for classroom use, it is important that such abstractions be quick to comprehend and easy to use. An example of a simple abstraction is the Take-Grant graph-based access control ICV shown in Figure 2. The model is a simple graph of objects and subjects connected with rights. Students

interact with the graph to set up the rights system and create commands to prove properties about the model. They are able to quickly understand the representations and actions. Consistency in abstract representation is also important when presenting different tools with similar concepts. For example, several cipher applets have the same general layout as shown in Figure 1; all follow a similar look and feel for encryption, decryption, and cipher characteristics.



**Figure 2. Take-Grant ICV.**

Another feature that is important when designing ICV’s is to limit the number of concepts being demonstrated. Active learning activities are intended to be short in duration to supplement lectures, not replace them. One approach to keep the focus on a narrow concept is to use tabs, each tab focusing on a separate concept, such as the cipher ICV shown in Figure 1. Different tabs can be shown at different points in the lecture to describe features and/or vulnerabilities of the cipher being studied.

Relevancy is always important in lectures, but especially when presenting interactive activities. There is always a danger that highly interactive visualizations are seen as more “gee whiz” than meaningful to the lesson if the concept being demonstrated is not clear or the interaction is trivial. While there may be some benefit in providing a break from straight lecture, activities that are seen as trivial or irrelevant waste valuable class time and can lead to student disinterest. To ensure our security ICV’s are relevant we carefully select which concepts to represent based on topics that are difficult to grasp, benefit from a visual representation, or can be easily grouped together with similar concepts.

A final design consideration is to ensure a robust user interface. When used in the classroom, the instructor may be standing at a podium or trying to use the keyboard under less than ideal conditions. Minimizing typing and making extensive use of GUI widgets help. For tools that require text commands, such as the protocol language shown in Figure 3, the

capability to save and restore data files is incorporated allowing the instructor to pre-build demonstrations. It is also important to make sure that any erroneous input is handled gracefully. This is to avoid frustration by the student when they are using the tool, and to avoid instructor embarrassment when demonstrating the ICV in front of the class.

ICV's are designed for use in the classroom as an active learning activity. Typically, the instructor demonstrates the tool as part of introducing the concept and then lets the students use the tool in the class on their laptops, in front of the class, or as an out-of-class assignment. A common way of using the tools is to play "what-if" games in the class where the instructor sets up a scenario and asks the students to predict what will happen, or asks the students to come up with a scenario to cause a certain event. An example is the protocol visualization tool, GRASP, shown in Figure 3. Students can be asked how an eavesdropper, Eve, can attack the protocol using a man-in-the-middle attack, and how to modify the protocol to counteract the attack.

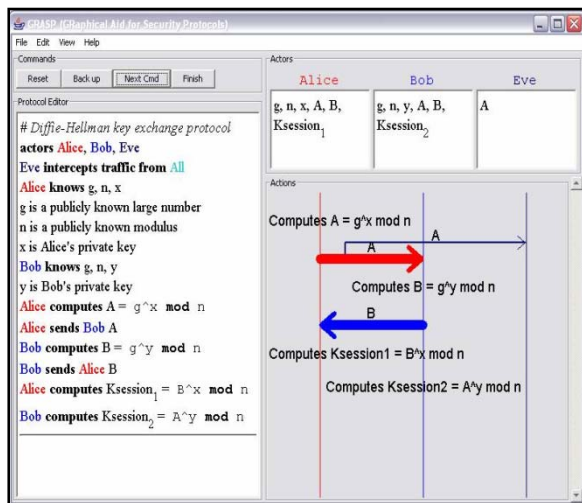


Figure 3. Security protocol visualization tool

### 3.2 Security competitions

ICV's provide one form of active learning activity for the classroom that is short, focused, and highly interactive. Another form of activity to engage students in security concepts is to make use of competitive type activities such as Capture the Flag events. While shortened forms of these can be done in the classroom or lab, a more common approach is to dedicate a day, or several days, to participating in a competition with other institutions. These types of competitions can be highly motivational to students

and reinforce critical concepts in a real-world type environment.

Traditional cyber competitions, such as the UCSB international event, involve teams composed of individual schools employing both offensive and defensive strategies to attack and defend networks. The Cyber Defense Exercise, or CDX, is a competition between the service academies that focuses on network defense [1]. The National Security Agency serves as the red team attacking the networks. A version of CDX has been created to broaden participation by more schools in an intercollegiate competition [11].

These types of competitions can engage students in an active learning manner. However, care must be taken to ensure that the focus is on the underlying concepts, and not simply the use of tools or strictly the competitive nature of the events. To address these concerns, we developed a regional assessment competition with other schools in our area known as CANVAS, the Computer and Network Vulnerability Assessment Simulation [4]. CANVAS is unique from other security competitions in its inclusion of all experience levels, team makeup, and emphasis on analysis and communication.

To help maximize participation by students at all levels of experience, there is no minimum experience required to participate. Students with several security classes participate along with students having had no classes, but an interest in the topic. Some of the students have extensive network and system administrative experience and have participated in other competitions; others are only experienced as users on their own machine. When students sign up to participate in the day-long event, they self-rate their experience level.

To compensate for the wide variety in student experiences, and to mitigate any over-competitiveness associated with the event, teams are not comprised of students from individual schools, but rather teams are formed "on the fly" from a mixture of schools and experience levels. Ideally, each team has no more than a single student from a given institution. This approach serves several purposes. It eliminates the lengthy preparation time that some competitions encourage – while individual students may practice with the allowable toolset before the competition, there is no extensive strategy planning or team practicing. This approach to team structure also adds an interesting component to the competition; that of learning to work with peers that you have never met before and may have very different skills and backgrounds than you. While initially a little intimidating for some, the social aspect of meeting and working with other students

becomes a positive aspect of the event. Finally, this method of forming teams significantly reduces the pressure to win by a given school. While each team wants to outdo the other teams, there is no school pride or reputation to uphold. This allows students to participate in a more relaxed manner and learn from their peers.

The final distinction between CANVAS and other competitive events is the way in which results are conveyed and tallied for a final score. In other competitions, points are awarded for captured flags, for successfully attacking an opponent, or for successfully defending against an attack. The premise in CANVAS is that each team is evaluating a contrived system for vulnerabilities using standard offensive tools. The goal is not to attack the system, but to discover the vulnerabilities and report them, along with an analysis of the potential consequences of the vulnerability, and a recommended fix. Some flags are placed in the system so students know they are on the right track, but simply collecting flags is not the emphasis. At the end of the exercise, teams are given a period of time to write up their discoveries in a report format to submit to the CEO and CTO of the fictitious company. Faculty members from the participating schools read each of the reports and rank order them based on completeness, technical correctness, and the quality of the analysis and recommendations.

We have successfully held the CANVAS exercise for three offerings. Participation has been around 40 students from five to seven regional undergraduate institutions. Participant surveys have been highly positive on the value of the experience and over 94% of participating students would like to do it again and/or would recommend it to others. Students enjoy using the offensive tools, learning how to evaluate a system, and working with other students in a social atmosphere. They are less excited about writing up their results for final evaluation. Students give mixed reaction to the team composition strategy with some students saying they enjoy learning from their peers, while others would prefer to be teamed with their classmates. Participating faculty agree that the team make-up forces peer-level interaction and teamwork that students will find valuable in a future real-world situation. Faculty also agree on the value of the final report and getting students to see the bigger picture beyond just “hacking” to compromise a system.

### **3.2 Hands-on laboratory exercises**

The final active learning activity that we have incorporated in our security courses is an emphasis

on hands-on laboratory and project exercises. Many security programs use laboratory exercises as a motivational means to give students hands-on experience with current tools and first-hand practice with different techniques. While these exercises engage students in an active learning way, it is important to ensure the focus is on the underlying concepts and not just the tools. For example, a laboratory exercise in password cracking can be accomplished as simply running a software tool. However, a greater education benefit is achieved if the student understands how the tool works, what its capabilities and limitations are, and how to design systems and passwords policies that would defeat the tool. Having students perform an analysis on the size of password space, the theoretical amount of time needed to search the space, and proposing alternative password schemes can provide a much deeper understanding of the concepts involved.

In addition to laboratory exercises, our Information Warfare course uses hands-on final projects as a means to engage students more fully in an active learning way. For the project, the student selects a security topic of interest, such as graphical passwords, steganography, or digital camera forensics. Part of the project is the necessary background work to understand the issue, approaches that others have taken, and a proposed approach for study. Rather than simply being a research paper, each project must include some implementation associated with the topic for analysis. For example, a steganography project may include a tool for detecting the presence of it in an image. Another example is the creation of “gummy bear” fingers to try and defeat a fingerprint scanner. The major emphasis in the project is not the implementation itself, but rather the analysis of the implementation. For example, how successful is the steganography detector, what types of images does it not work well on, and why. The implementation phase of the project engages the students while the analysis portion requires them to examine the underlying concepts.

## **4. Our experience / future plans**

It is difficult to perform a formal evaluation on the effects of these active learning approaches given the small number of classes and limited number of students per class. We have attempted to quantify some of the effects of the various ICV's with mixed results. In our large freshman course, for example, we used the PKI visualization tool in some sections, but not others. There was no measurable

improvement in performance on PKI related questions on the exams. In our Information Warfare class, we evaluated the effect of the formal model tools based on class performance on exams and found students performed better when they had experience with the tool. A related informal feedback from the instructor was that he was able to reduce class time on the concepts as students seemed to “get it” quicker. Student responses on course surveys are almost always positive about the tools.

Evaluation of the effectiveness of the security competitions comes primarily from participant surveys. Students overwhelmingly rate them as highly enjoyable, informative, and worthwhile. Surveys and student reactions to hands-on laboratories and projects are similarly popular and enjoyed by the students. Quantifying the educational benefit in terms of improved learning is difficult and has not been attempted.

Perhaps the greatest testament to these approaches is the motivational aspect. Effective use of ICV’s in the classroom has an energizing effect, is seen as a fun activity, and engages students in the topic at hand. At competitions, students get excited in the discovery process and interacting with others. In hands-on laboratories, students get a sense of accomplishment in successfully breaking something, or achieving some specific goal. In all three cases, students are active participants in the learning process and not simply passive vessels absorbing the wisdom of their professors.

In the future, we plan on continuing our active learning approach in the security curriculum. Additional ICV’s are in the planning stages, and we are continually refining existing ones based on our experience and feedback from others. We are planning on continuing the CANVAS exercise and expanding participation with more schools. Minor adjustments to the exercise are planned based on participant suggestions. Similarly, we will continue to use hands-on exercises and projects in our security courses. One area that we are investigating for improvement is the use of virtualization to expand the exercises while reducing actual hardware requirements. Another improvement we are implementing for the hands-on project is to have more “pre-defined” projects for students to select from. We found that at the undergraduate level, many students did not have a good sense of the scope and level of difficulty of self-selected projects and they spent an inordinate amount of time going in non-productive directions. Having better defined projects up front will allow them to focus on the implementation and analysis phases of the project.

Overall, our experience is that active learning is an effective way to motivate students and engage them in the learning process. Applying active learning techniques to security can improve student education in this critical field.

## 5. References

- [1] Augustine, T. and Dodge, R., “Cyber defense exercise: meeting learning objectives thru competition,” in Proceedings from the Tenth Colloquium for Information Systems Security Education, June 2006.
- [2] Begel, A., Garcia, D., and Wolfman, S., “Kinesthetic learning in the classroom,” In Proceedings of the 35th SIGCSE Technical Symposium on Computer Science Education, SIGCSE '04. pp. 183-184.
- [3] Bonwell, C., and Eison, J., “Active learning: creating excitement in the classroom. ASHE-ERIC Higher Education Report 1, 1991.
- [4] Collins, M., Schweitzer, D., and Massey, D. , “CANVAS: a regional assessment exercise for teaching security concepts,” in Proceedings from the 12th Colloquium for Information Systems Security Education, June 2008.
- [5] Ebeling, D. and Santos, R., “Public key infrastructure visualization,” J. Comput. Small Coll. October 2007.
- [6] Paulson, D. and Faust, J. “Active learning in the college classroom,” Journal on Excellence in College Teaching, vol. 9 (2), pp. 3-24, 1998.
- [7] Prince, M. ,”Does active learning work? A review of the research.,” Journal of Engineering Education, 93:3, pp. 223-231, 2004.
- [8] Schweitzer D. and Baird L., "The design and use of interactive visualization applets for teaching ciphers," Proceedings of the 7th IEEE Workshop on Information Assurance, June 2006.
- [9] Schweitzer D., Baird L., Collins M., Brown W., Sherman M., "GRASP: A visualization tool for teaching security protocols," Proceedings of the 10th Colloquium for Information Systems Security Education, June 2006.
- [10] Schweitzer D., Collins M., Baird L., "A visual approach to teaching formal access models in security," Proceedings of the 11th Colloquium for Information Systems Security Education, June 2007.
- [11] White G. and Dodge, R., “The national collegiate cyber defense competition,” in Proceedings of the Tenth Colloquium for Information Systems Security Education, June, 2006.