Active Learning Approaches to Teaching Information Assurance

Christy Chatmon
Dept. of Comp. & Info. Sciences
Florida A&M University
Tallahassee FL, 32307
chhatmon@cis.famu.edu

Hongmei Chi
Dept. of Comp. & Info. Sciences
Florida A&M University
Tallahassee FL, 32307
hchi@cis.famu.edu

Will Davis
Dept. of Comp. & Info. Sciences
Florida A&M University
Tallahassee FL, 32307
will3davis@yahoo.com

ABSTRACT
This paper presents several active learning strategies to engage students in Information Assurance (IA) concepts and to enhance their learning experience. Simply listening to a lecture or attending a physical computing laboratory to explore IA concepts for numerous reasons, may not be ideal. Passive involvement of students in their learning process generally leads to a limited retention of knowledge. Students today have excellent visuospatial reasoning skills and the instructional methods chosen should be visual and require active participation. We are exploring several active learning pedagogies in hopes of increasing IA awareness amongst undergraduate computer science majors and non-majors.

Categories and Subject Descriptors
K.3.2 [Computer and Information Science Education]: Computer science education.

General Terms
Management and Security

Keywords
Information Assurance, Hands-on lab, Active Learning, Virtual Labs, E-Learning

1. INTRODUCTION

Information Assurance (IA) is one of the fastest growing areas of the information economy, addressing concerns ranging from matters of national security to individual privacy and information protection in the conduct of commerce, entertainment and social interaction. At Florida A&M University (FAMU), the information assurance track has become one of the most popular tracks of study in the Department of Computer and Information Sciences.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

Copyright 2009 ACM 978-1-60558-661-8/09/0004...$5.00.

Our goal is to strengthen the existing IA program and increase IA awareness to other disciplines by integrating IA modules into courses taught to non-majors.

The variety of IA curricula and diverse educational models at universities has not provided their graduates with skills demanded by employers. The levels of skills expected by employers and those graduates have acquired after completing their studies suggests a discrepancy. Organizations employing IA professionals emphasize problem solving, creativity, and interdisciplinary collaborative work while exhibiting effective communication and teamwork skills.

It is our view that instruction must adapt to these demands. The traditional passive learning approach (reading, hearing, looking and watching) should be adapted to create an environment in which knowledge retention is significantly increased. [9, 15, 20] suggests that an increase in students’ retention of information is gained by not simply receiving information verbally and visually, students must be receiving and participating and doing.

Reaching today’s students can be a challenge when using primarily lecture-based instructional methods. Today’s youth are visuospatially intelligent and talented [7] and may need to experience instruction that is visual and that requires active participation. Many research studies [3, 5] show that by applying active and collaborative learning there will be improvements in:

- Information retention,
- Student-faculty interaction,
- Student-student interaction,
- Academic achievements (i.e., grades),
- Higher-level thinking skills,
- Teamwork,
- Attitude towards the subject and motivation to learn.

These observations motivate a rethinking in how IA education instruction is delivered. To that end, we explore the potential for active learning instructional methods to focus IA program and modules more intently on problem solving, design, communication and teamwork. The planning and preparation of active learning activities we have implemented, such as virtual labs and web-based activities, are fundamental to the future of e-learning in IA education at FAMU.

In this paper, we introduce active learning as a pedagogical approach for IA education and provide several case studies to demonstrate its usefulness.
2. ACTIVE LEARNING

The “talk and chalk” or “sit and get” approach using a power point presentation combined with lecture is not alone effective to teaching IA concepts. The increase popularity of active learning methods in computer science curricula is due to the growing awareness that it is no longer possible to train computer scientists for a life long career within a comparatively short period. A computer scientist needs competencies in problem solving, teamwork, and communication skills to be able to apply technical knowledge in various circumstances. The origin of learning is rooted in activity, doing something to find out about the world [9].

Active learning refers to developing and implementing planned activities to engage the participant as a “partner” in the activity. In short, students are learning by doing. That means that while students are doing an active learning exercise (such as hands-on lab), 90% of the students are actively engaged with the material and getting practice in the skills an instructor is trying to teach them. Active learning results in a deeper and more integrated understanding of concepts, as well as significant improvement in student retention in degree programs. Engaged students remember concepts longer, enjoy the learning process more, and are more likely to continue.

Active learning techniques can help students to increase mastery of foundational skills, improve technical communication skills, and enhance critical thinking. [5, 8] describes several case studies demonstrating this approach, in this paper we explore our implementation of integrating active learning strategies into the IA courses illustrated by several case studies.

2.1 Various Active Learning Techniques

In comparing the effectiveness of lectures and group discussions, research suggest that both are useful for knowledge-level learning, group discussion methods are more favorable for problem-solving, transfer of knowledge to new situations, and motivation for further learning [2]. [10] found that cooperation improved learning outcomes relative to individual work across the board. The primary goal of small group techniques is to get students to really think about the material so they can state their own views, to hear others, to hone their argumentative skills, and vocalize what it is they are thinking about. This approach makes it difficult for students to avoid participating thus making each person accountable. [19]

Collaborative Learning refers to any instructional method in which students work together in small groups toward a common goal [17, 22]. The emphasis of this approach is on student interaction rather than on learning as a solitary activity. An example of this approach is a “think/write/pair-share” method. The instructor begins by posing an issue or problem to the class and then allowing the students to reflect and write out their response. Students then pair up and explain their responses to one another for a set time. Lastly, as a class, the issue or problem is discussed. The instructor may record each group’s main point on the board and incorporate the material into a future lecture.

Cooperative Learning is defined as a structured form of group work where students pursue common goals while being assessed individually. The emphasis of this approach is a focus on cooperative incentives rather than competition to promote learning [12]. An example of this approach is cooperative groups, which are useful for more complex projects. This approach is encouraged discussion of problem solving techniques and avoid the embarrassment of students who have not mastered all the skills yet [19]. Examples of this approach include cooperative groups, concept mapping, and debates.

Problem-Based Learning can refer to as an instructional method where relative problems are introduced at the beginning of the instructional cycle to which is used to provide the context and motivation for the learning that follows. This approach involves considerable self-directed learning on the students’ part. Learning becomes active as the students discover and work with content that they determine to be necessary to solve the problem. Problem-based learning as experienced by the student is when a student: 1.) explores the issues 2.) lists what is known 3.) develops, and writes out, the problem statement in own words 4.) lists out possible solutions 5.) lists actions to be taken with a timeline 6.) lists what needs to be known 7.) writes up solutions with its supporting documentation and 8.) debriefing exercise is administered individually and as a group.

Learning by Doing is best described by a Chinese famous educator Confucius who said two thousand years ago, “tell me and I will forget, show me and I may remember, involve me and I’ll understand.” When students with limited computing background enter the IA field, they face a steep learning curve. Hands-on labs that employ game playing help students to quickly grasp core content and topics.

2.2 The Learning Process

Learning begins at the initial exposure of the content, where the student witnesses the use of new concepts to explain or explore an IA issue in a virtual/physical environment. During the exposure stage, the learner is exposed to the new concept from the instructor/peer or by their own experiences. Students are afforded additional opportunities to learn as they apply IA concepts to solve a real-world problem or do an experiment. This is considered learning by doing, where one has become familiar enough with IA concepts/measures to find solutions to the real-world specific security problems. The adaptation and creativity stages mark the onset of research.

Our motivation for designing the various learning activities was to create a unique environment to allow students to incorporate what they have been exposed to into applications. As an example, in several of our security courses, students are required to create and design their own labs to be administered to their peers. The student in this activity is given guidance by the instructor, but is allowed the freedom to explore the security tools. We examine this idea further later in the paper. This type of experience encourages the student to move from the exposure stage to a higher level of learning. With guidance and similar activities, the student gains mastery of the concepts as shown in Figure 1. This is the ultimate achievement and core of the learning process.
3.1 Virtual Laboratory Exercises

Education in IA is better served by a laboratory component that reinforces IA concepts while providing exposure to current tools. It is always important to show students how to apply the theory in practical situations [18]. Hence, it is our view that a good part of an IA course should focus on applications and operational concerns. In order to support our security track, a combination of physical and virtual laboratory exercises are conducted. However recently we are primarily offering laboratory exercises virtually.

The rising interest in the use of virtual laboratories is due to several reasons including interest in supporting distance education, potential for resource sharing and cost savings, and potential for improved educational outcomes [3]. IA e-learning opportunities at FAMU are currently being developed which makes the need to transition from physical to virtual laboratories even greater. Another compelling reason is that our physical IA laboratory consists of 15 desktop workstations which support four courses and research activities. With a growing interest in our IA security track, the enrollment has soared and has caused a significant strain not only on the physical workstations, but also on faculty/staff that continuously reconfigured the workstations for classroom experimentations. The implementation of the virtual environment (VMware Server) allows for an enriched laboratory experience for the students and an easier setup and implementation for faculty/staff. Students are now able to access their experiments from remote locations (with Microsoft Terminal Server Connection) and are accessible at all times.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Description:</th>
<th>Special Software Needed:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virus Removal</td>
<td>Explore the process of virus removal &amp; vulnerability identification (see Figure 2)</td>
<td>Avira AntiVir Personal; Trojan Horse application</td>
</tr>
<tr>
<td>Password Policy</td>
<td>Modification of local security policies</td>
<td></td>
</tr>
<tr>
<td>Enumeration</td>
<td>Identification of resources available on the network</td>
<td>LANguard Network Scanner</td>
</tr>
<tr>
<td>Host-based Firewall/IDS</td>
<td>Detection of system-level attacks</td>
<td>Sygate Personal Firewall</td>
</tr>
<tr>
<td>Packet Analyzer</td>
<td>Protocol observation using a packet sniffing tool</td>
<td>Ethereal</td>
</tr>
<tr>
<td>System Vulnerabilities</td>
<td>Determination of security state of a system</td>
<td>Microsoft Baseline Security Analyzer</td>
</tr>
<tr>
<td>Web Browser Security</td>
<td>Investigate the flaws and vulnerabilities of Web browser software</td>
<td></td>
</tr>
</tbody>
</table>

The exercises engage students in an active learning way and more importantly allow students to gain a deeper understanding of how the security tools work and explore their limitations and advantages.
capabilities. It also exposes students to the activities of designing secure systems and policy implementation.

Initially students are provided video tutorials to foster an understanding of proper use and access (remotely) to the virtual machine and its resources before conducting their first laboratory assignment. Video tutorials are also provided for later labs to offer explanation of laboratory experiences and to reinforce concepts. Table 1 demonstrates examples of virtual laboratory exercises conducted in our various security courses.

![Figure 2: Virus Removal Exercise](image)

### 3.2 Online Cooperative Group Discussion Activities

Socratic questioning techniques are a useful active learning tool to encourage effective class discussion and interaction. Students in our security courses enjoy a good classroom discussion/debate about IA related current events and security concepts such as computer viruses, privacy issues and hacker activities just to name a few. Our class time is limited and valuable. To ensure that we cover as many security concepts as we can during the semester, we use online group discussion activities via Blackboard to investigate and reinforce IA concepts.

The benefits to using online discussion boards to facilitate active learning pedagogy are abundant [1]:

- Students utilize critical thinking skills
- Students participate more regularly and more thoughtfully than they would in a face-to-face instructional setting, especially in large classes
- Students develop a stronger class community
- Students are more likely to cite research and class readings
- Students achieve greater cognitive and exploratory learning
- Faculty members spend less time answering questions (students often answer each others questions with little or no prompting from the instructor)
- Students have a greater sense of race and gender-based equality

Students are given one or more topics to select from. The student must then read 2–4 pieces of literature associated with their topic. Each student is then required to participate in two online group discussions biweekly – one group discussion and one pair discussion. After posting their initial response to the question, the student must read their groupmates posts and post at least one reply/follow up.

It is important to provide adequate time between the deadlines for the initial response and the reply/follow up responses to allow students to read each other’s posts and allow the instructor to respond to posts as well. Also, students are explained the value of participation on the discussion board and provided online discussion guidelines/tips prior to discussion activities beginning. This is essential to stimulating a healthy academic debate on IA issues. The instructors spend time explaining to students how to listen to others, how to validate others’ opinions and beliefs, the usefulness of paraphrasing to clarify understanding, the importance of summarizing, and how to encourage others to participate in the discussion. It is not assumed that students have these skills and taking time to emphasize them may facilitate a more successful experience for the student.

### 3.3 Think-Pair-Share Activities

Another cooperative learning technique we use is the think, pair, share strategy which encourages individual participation. Students think through questions posed to them using three distinct steps [10, 19]:

1. **Think** – Students think independently about the question posed in class forming their own ideas.
2. **Pair** – Students are grouped in pairs to discuss their thoughts which allow students to articulate their ideas and to consider those of others.
3. **Share** – Students pairs share their ideas with the class. Students tend to be more comfortable sharing their ideas with the support of a partner. During this step students’ ideas become more refined.

Research suggests that students’ learning is enhanced when they are given opportunities to elaborate on ideas through talk. It is through this method that students increase the kinds of personal communications that are necessary to internally process, organize, and retain ideas [21].

Students are given guidelines outlining the procedures when the “think-pair-share” activity is first introduced. They are then presented a challenging or open-ended question either prior to class time or during class depending on its level of complexity. If the question or issue is presented during class the students are given a period of time to “think” and consider their thoughts about the question. It is helpful to set time limits on the “think” and “pair” activities. Also, if the “think” step is outside of class encourage students to write down their thoughts.
In the “pair” step, the students are paired with a collaborative group member to discuss their ideas. It is during this step that students begin to construct their knowledge in these discussions and discover what they do know and what they do not know, which is not normally available to them during traditional lectures.

We use various approaches to address the “share” step of the strategy. After a set period of time, the instructor randomly solicits student comments or takes a classroom vote/poll. The random calls are important to ensure that students are individually accountable for participating. The responses are often more intellectually concise since students are given a chance to reflect on their ideas. Also, this approach enhances the student’s oral communication skills as they are given an opportunity to discuss their ideas with their peers. Another variation is to require students to write down their thoughts and collect them for later review and discussion. The instructor is then given an opportunity to see whether there are problems in comprehension [19, 20, 22].

Below are examples of the type of discussion questions posed to students during a “think-pair-share” activity:

- What would you recommend as a punishment for a policy violation involving removal of confidential records for a “harmless” reason like catching up on reading them at home? Would your recommended punishment be different if the violator used them for a different purpose, perhaps using them to perform identity theft? [24]:
  - Get into the mindset of a truly determined hacker. Why would someone devote tremendous time and energy to trying to break into an information system? What could the reward be?
  - Once managers have gone to the trouble of creating a security policy, how can they ensure that all personnel read and understand it?
  - Most security policies recommend the following:
    - Personnel must never use a password that is the same as or similar to one they are using on any corporate system and on the Internet site.
    - Company personnel must never use the same or a similar password in more than one system. This policy pertains to various types of devices (computers or voice mail), various locations of devices (home or business), and various type of systems, devices (router or firewall), or programs (database or application) [14].

Do you agree or disagree with these recommendations. Discuss the feasibility of following these recommendations.

Research tells us that we need time to mentally chew over new ideas in order to store them in memory. If we allow students to “think-pair-share” throughout the lesson, more of the critical information is retained [19]. Students are given an opportunity to talk over new ideas and their misunderstandings about the topic are often revealed and resolved during this discussion stage. This approach is useful beyond discussion questions. We also use this approach informally for lecture check and current events opinion.

### 3.4 Student Generated Labs

We have adapted the “Quiz/Test Questions” approach, which [19] is described as students becoming actively involved by constructing some (or all) of the questions for quizzes and tests, and combine it with the “Cooperative Groups” strategy. Research suggests the “Quiz/Test Questions” activity encourages students to think more deeply about the course material and explore major themes, comparison of views, applications, and higher-order thinking skills. We require student groups to create a hands-on laboratory assignment as a course project to be administered to their peers. This assignment promotes a mastery of foundational IA skills as shown in Figure 1. IA professionals must be able to learn novel technologies/skills and be self-directed.

At the beginning of the semester, student groups of size 2-3 are formed and given a project list where each project lists several free source software for consideration. They must then develop a virtual laboratory exercise including documentation to be rendered to their peers.

Here is an example of a student-generated hands-on lab which required groups to give an overview of tools for network monitoring and traffic analysis. The Netflow analyzer from SolarWinds was chosen by a group. A hands-on lab was created by students demonstrating the steps for monitoring wireless and wired network traffic. Their exercise also required customization of the NetFlow data displays to view traffic by specified time periods (up to 60 minutes) and by traffic type (see Figure 3).

![Figure 3: NetFlow data displays to view traffic](image)

These activities foster the learning by doing idea. The student groups spend numerous hours brainstorming, creating and documenting their exercises. The instructor meets with each student group periodically throughout the semester to ensure progress. Midway through the semester each group is required to...
give a presentation on the status of their project. Lastly, each group’s final laboratory exercise is critiqued by their peers after completing the exercise.

3.5 Student-Led Current Event Reviews

To motivate students’ interest and awareness in news related to information assurance, we encourage students to pay attention to press news or technology news related to IA topics. All Current event summations and presentations must respond to the following questions: (1) How does the topic you have chosen relate to Information Security? (2) How do the topics discussed in your article(s) relate to the basic computer security goals – Confidentiality, Integrity, and Availability (CIA)? (3) What is the global/societal impact of the topic(s) discussed in your article(s)?

Most students are enthused to complete those assignments. Here are examples of topics chosen by students: (1) graphics-based password research project1 (2) a report on botnet attack from Russian gangs for financial advantages2. This assignment helps to encourage our students to remain engaged in IA topics and concerns.

4. FEEDBACKS

Anecdotal feedback from students has been very positive. We collect responses for each IA course at the end of each semester. Several responses are presented below to the following question: What did you like the best about this course?

“I like all those hands-on labs and the most interesting lab is that I can design my [own] labs and learn free source tools.”

“The Current Event reports. These assignments really opened my eyes to security…”

“The current event discussions.”

“The hands on labs and the in-class discussions made me want to learn more about security.”

The main finding so far suggests that the active learning activities are welcomed by students and they have a sense of being involved in their learning experience. Of course, this survey is preliminary. We will conduct a formal questionnaire for feedback from our students. In addition, we will test various active learning activities in courses for non-CS majors and conduct a well-designed pre/post-surveys and report the responses in future papers. We also found that the student-generated labs and peer review exercises require the instructors to spend considerable outside class time with students to provide guidance on how to express their views and findings.

5. CONCLUSIONS & FUTURE PLANS

We have discussed our approaches for implementing active learning activities for CS-majors in IA education. In the future, we will continue to improve and expand the mentioned activities to include current trending topics and popular security tools. In addition, we will continuously retrieve student feedback to make activities better learning tools and more student-friendly.

In the future, we plan to develop IA active learning activities/modules to be included in courses taught to non-CS majors as a way to increase IA awareness. In addition, we are planning on expanding IA education at FAMU by offering e-learning opportunities to our students and the community; we hope to incorporate our active learning approaches to support this effort.

6. ACKNOWLEDGMENTS

This work has been supported in part by U.S. Department of Education grant P120A080094 and by NSF CPATH.

7. REFERENCES


1 http://www.darkreading.com/security/vulnerabilities/showArticle.jhtml?articleID=208804640
2 http://news.cnet.com/8301-10789_3-10086352-57.html


