Broadening Information Assurance Awareness by Gaming

Hongmei Chi[1] **and Edward L. Jones**[1]
[1]Department of Computer & Information Sciences, Florida A&M University, Tallahassee, FL, USA

Abstract - *Preparing students for future information assurance careers is critical for national security. A related challenge is to teach non-CS majors security issues and practical consumer skills. This paper attempts to address these challenges by inspiring the interest of students, preparing students to accede seamlessly into the future high-quality workforce via designing game-like hands-on labs. In addition, we present a pragmatic approach of teaching information assurance designed particularly in response to the demand for professional workforce in the digital world. In this paper, we focus on integration of information assurance concepts into a set of hands-on labs via playing games*

Keywords: Information Security, active learning, social networks, CyberCIEGE, game-based labs

1 Introduction

Today's students are tomorrow's workforce. Properly training our students is critical for our future workforce. Because of the pervasiveness of digital commerce and the increasing vulnerability of our society to cyber attacks, aspects of information assurance (IA) need to be included in the educational experience of all university students.

The United States is an increasingly digital nation where the strength and vitality of our economy, infrastructure, public safety, and national security have been built on the foundation of cyberspace [12, 13].

The President's National Strategy to Secure Cyberspace refers to cyberspace as the "nervous system" of our nation's critical infrastructures, and recognizes that the healthy functioning of cyberspace is essential to our economy and national security. Securing cyberspace [4] is a difficult strategic challenge, and information assurance (IA) education is critical to meeting this challenge successfully IA education has to be given to everyone.

For most of college students, social networks are very popular forums that connect communities of people together. User privacy protection is a major issue in social networks. The State of the Internet 2009 report [20], found that the most notable online threat was rogue/fake security software, major search engines, social networks and Web 2.0 threats. Cyber-criminals have made a business out of attacking popular online sites. Search engines like Google and Yahoo, or social networking sites like Twitter or Facebook appeal to these criminals. Educating college students to protect their privacy in social networking poses a new challenge—making all students IA-aware, regardless of their field of study. This challenge reflects the reality that IA is interdisciplinary, drawing from multiple fields, such as computer science, criminal justice, engineering, management science, systems engineering, accounting, public administration, criminology and security engineering.

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 grasp quickly core content and topics [1]. Games are familiar to everyone [6]. The number of people who never played a video game, from first graders to retirees, seems to be declining, especially for high school students. Games offer potentially active learning environments [11]. It is a safe assumption that most college students have experience playing computer-based games.

With the skill of playing game, students do not have to spend time to become familiar with new tools and are straightforward to accept the new IA concepts that are conveyed and reinforced in game-based labs.

We will leverage students' gaming skills to introduce information assurance to non-CS majors and impart skills to CS majors [5]. In this paper, we will show examples of games that support incremental mastery of IA concepts.

2 Motivation

Our department has a positive track record in information assurance education. Since its introduction in our department, the IA track has enjoyed the demand and throughput shown in Table 1. Additional IA courses have been introduced to meet growing demand for digital forensics and for elective courses suitable for other majors such as criminal justice. This paper reports on our efforts to increase the capacity of the IA program to meet the demand from CIS majors, and to move towards cross-disciplinary programs with STEM and other disciplines.

Our department has an opportunity to expand to meet the needs of the university. Because computing is so pervasive, the university has the obligation to educate its faculty, its students, and the public about the risks of information technology as it relates to privacy and rights. IA is one of the first aspects of computing that impacts directly on the average U.S. citizen. The mandate to serve the community is compelling.

Table 1. Demand for IA Courses at FAMU

IA Courses	2005	2006	2007	2008	2009
Intro to Computer Security	30	24	30	18	27
Network Security & Cryptography	17	22	11	16	11
Applied Security	38	21	40	17	15
Digital Forensics	N/A	N/A	12	16	17
#Certificates	5	10	29	7	6

We are experiencing increasing demand from non-CS students who want to earn an IA certificate. Because these students do not have the full complement of IT courses that CS students bring to the IA courses, we face the challenge of providing these students a meaningful course experience, without first requiring them to complete a long sequence of preparatory courses. The two strategies we currently employ are collaborative learning activities involving mixed teams of CS and non-CS students, and the use of game-based labs lab exercises.

2.1 IA Education for CS Majors

In August 2003, NSF awarded our department an Information Assurance (IA) capacity building grant. This project resulted in a comprehensive three-course undergraduate information assurance and security (IAS) curriculum track that was certified by NSA and CNSS in November 2004 as having implemented two CNSS training standards, NSTISSI 4011 (Information Assurance Professional) and NSTISSI 4014 (Information Systems Security Officer – Entry Level). As shown in Table 1, the IAS track is in great demand by students and, to date, nearly 60 students have earned certificates.

2.2 IA Awareness

The current direction of our IA program is to offer a certificate in digital forensics, as a first step towards cross-disciplinary programs with sociology and criminal justice and other disciplines. The criminal justice program at our university enrolls nearly 600 students; their graduates have been placed in major corporate and leading government agencies such as the FBI, CIA, U.S. Department of State, and U.S. Customs. Criminal justice has four substantive areas from which all majors are required to select one: juvenile justice, minority and gender, or corrections. The students are also required to have a minor area. The CIS and Criminal Justice departments are working to define digital forensics as a new minor option for Criminal Justice majors.

3 Active Learning

Active learning refers to techniques where students do more than simply listen to a lecture. 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. Gaming technology, which emphasizes engagement, provides an additional tool for implementing active learning.

The "learning tree" shown in Figure 1 begins with the initial *exposure*, where the student witnesses the use of new concepts to explain or explore an IA issue in a virtual/game environment. Interested students will be afforded additional opportunities to learn to *apply* IA concepts to solve a real-world problem or do an experiment. The next level of learning is *adaptation*, where one has become familiar enough with IA concepts/measures to find solutions for their real-world specific security problems. The application and adaptation stages mark the onset of *research*. Advanced research involves *creating* new IA technology, e.g., creating new IA models or new IA measures.

In this paper, active learning is achieved by playing games. Non-major students will learn IA easily by exploring the games [9]. Gaming applied to anti-phishing, quickly show scenarios for which poor user choices lead to disastrous results.

4 Game-Based Lab Design

One of the critical steps to train students to be professionals in the digital world lies in creating a comprehensive approach to computer security education [1, 2]. In this section, we address how to create labs that help the students better understand IA concepts through progressive, incremental experiences.

4.1 Framework

Our academic department has embarked on a project to expand the capacity of the IA program to include non-CS majors, to meet the demand for IA education from other majors, and to move towards cross-disciplinary programs with other disciplines.

We are planning to achieve three goals: (1) create game-based labs for CS majors so that students can do some labs without limiting resources; (2) design various game-based IA labs for non-CS majors so that we expand IA education to every student on campus; and (3) make sure that faculty can borrow and adapt existing labs and for their classes.

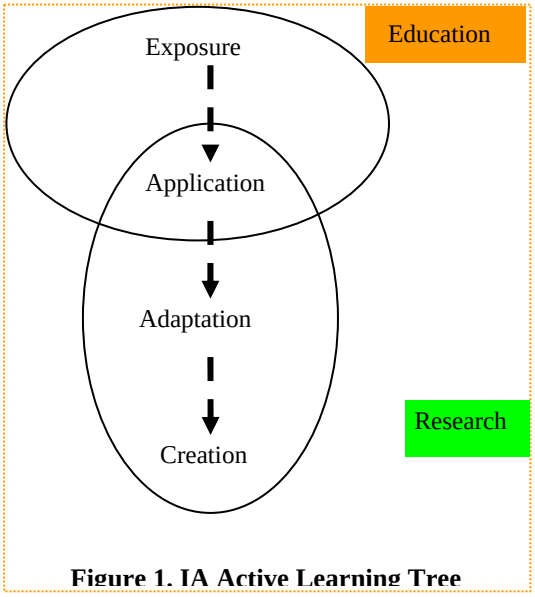

Figure 1. IA Active Learning Tree

The first such course, Cyberlaw & Cyber Crime, will be offered by the department of sociology and criminal justice at our university. The instructor wishes to make students aware the consequences of cyber crimes. Of course, there many current events reported in the news, such as the waves of July 2009 cyber attacks targeting a number of major websites in South Korea and the United States [14]. The attacker used *botnets* and file updates to rapidly spread the attack. Getting students to understand the full complexity of the bot infection life cycle is an important challenge for teaching network security. It is hard for students to visualize the process by which the attack spreads and the potential destructive consequences of botnet attacks. Game-based labs help students to see the cost of *distributed* denial-of-service (DDoS) attacks.

4.2 CyberCIEGE

The tool that we use to create labs is the CyberCIEGE Scenario Development Toolkit (SDK) [19]. CyberCIEGE is an IA training tool that illustrates computer and network security principles through simulation and resource management trade-offs. In the CyberCIEGE virtual world, users spend virtual money to operate and defend their networks, and can watch the consequences of their choices, while under attack.

CyberCIEGE has several predefined labs, each called a *scenario*. Examples include the "Stop Worms and Viruses" scenario, which is an extremely simple security awareness training scenario. Also, this scenario provides first time players with an introduction to the CyberCIEGE game interfaces and features.

In addition, the CyberCIEGE SDK includes tools for developing our own games for specific training or education purposes. CyberCIEGE is intended to teach IA concepts to students within information assurance or computer science curricula. Unfortunately, CyberCIEGE provides only a few "training and awareness" scenarios targeted toward general computer users.

4.3 Sample Labs

Case I Description

The CyberCIEGE "Stop Worms and Viruses" scenario is an example of an extremely simple security awareness training scenario. Also, this scenario provides first time players with an introduction to CyberCIEGE, including several of the game interfaces and features.

You work for the BorSoft company. It seems that whenever a new employee joins BorSoft, there is an outbreak of viruses and worms, resulting in a lot of lost productivity. The boss puts you in charge of preventing the new employee spreading email viruses and worms. Your tasks are to play the "Stop Worm and Viruses" Scenario and prevent new employee, named Joe, from spreading email viruses and worms throughout BorSoft.

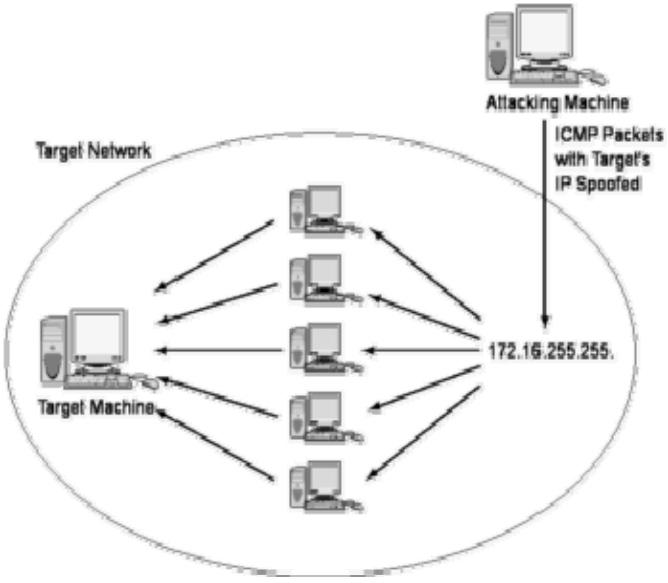

Figure 2. A DDoS (Smurf) attack.

Case II Description

The purpose of this lab is to test the different applications for the use of IP scanners. IP and port scanners are used very often by network administrators to verify security issues on their network and to check to see if computers are alive (connected to the network). We will test some of the uses of IP/port scanners in this lab and perform a DDoS attack. Figure 2 shows a DDoS attack [15]. DDoS attacks are hard to track back because of use botnets. Students completing this lab will see the consequences of a DDoS and the difficulty of mitigating it.

After each lab, the student will be required to answer four to seven questions related the lab. The conclusion may be a

report summarizing findings and their relevance along with the report generated by the software if it has that function.

4.4 Feedback

Anecdotal feedback from students is very positive. In our network security course, students are given four labs: two of them use free resources and the others are created by CyberCIEGE. The last question in the midterm exam for this class is "Compare the four labs you did, and write down the interesting topics that you have learned from these labs." Several responses are presented next:

> "I like all those labs and the most interesting lab is that I can see [the] consequences of DDoS by playing games."
>
> "[The] most interested labs are to make use of CyberCIEGE and password cracking. It is surpris[ing] to know how easy to crack my own password and see how the worm/virus are spread. I would like to work as [in a] network security related job"

The main finding so far is that the learning curve for CyberCIEGE labs is smaller than for other labs that use different tools. We conjecture that when new tools such as, nmap, Cain Abel, or FTK, are used to perform certain labs, students have to be familiar with the interfaces of tools first. Game-based labs minimize this hurdle, since most students already know how to play games.

We will test those labs for non-majors and conduct pre/post-survey and report the responses in future papers. Also, our students will have chances to do hands-on labs in both virtual environments [16,17] and game-based. It is interesting to compare those two methods and investigate advantages of both types of labs. It is likely that these two methods will remain popular options for future IA education.

5 Conclusions

We have discussed our principles and ideas of creating game-based labs for non-CS majors and CS majors in IA education, given the constraint that the labs are designed from free sources such as CyberCIEGE. In the future, we will continue to work with most popular IA topics and create additional labs that exploit the design variations we want students to experience [3]. In addition, we will improve existing labs and continuously retrieve student feedback to make labs better learning tools and more student-friendly.

Future work will also be focused on making certain that the labs are adaptable to different levels of student expertise and ambition. Open-ended labs provide rich experiences for motivated students, and the results of out-of-the-box explorations extend the depth of future lab assignments. We will focus on how to permeate our security education into a set of hands-on labs playing games, such as phishing education [3], botnet, and other active attacks [18]. We will create more network/computer security labs using CyberCIEGE SDK, and other games such as Second Life [10]. As for our IA certificates, the future plan is to make some of our hands-on labs are game-based. This plan will be helpful to students to conduct the set of hands-on labs that include a number of attacks that are too dangerous to perform on a real system or too expensive to set up in real laboratory. In addition, we will design and develop various in-house game-based labs for IA education and awareness [7].

Acknowledgments

The authors recognize the contribution of graduate students Jude Desti and Kevin Lawrence in implementing many of the hands-on labs. This work has been supported in part by U.S. Department of Education grant P120A080094 and P120A090122.

References

[1] Anewalt, K. 2008. Making CS0 fun: an active learning approach using toys, games and Alice. *J. Computing in. Small Colleges* 23, 3 (Jan. 2008), 98-105.

[2] Cone, B. D., Irvine, C. E., Thompson, M. F., Nguyen, T. D. A video game for cyber security training and awareness. *Computers & Security 26*, 1 (February 2007), 63-72.

[3] A., Cranor, L. F., Hong, J., and Nunge, E. 2007. Anti-Phishing Phil: the design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 3rd Symposium on Usable Privacy and Security, SOUPS '07, vol. 229*. ACM, New York, NY, 88-99

[4] Dodge, R.C. and Ferguson, A. Using phising for user email security awareness. *Proceedings of the IFIP TC-11 21st International Information Security Conference (SEC 2006)*, 22–24 May 2006, Karlstad, Sweden, 454-459.

[5] Eagle, M. and Barnes, T. 2009. Evaluation of a game-based lab assignment. In *Proceedings of the 4th International Conference on Foundations of Digital Games*, Orlando, Florida, April 26 - 30, 2009, 64-70.

[6] Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., and Pham, T. 2009. School of phish: a real-world evaluation of anti-phishing training. In *Proceedings of the 5th Symposium on Usable Privacy and Security* (Mountain View, California, July 15 - 17, 2009). SOUPS '09. ACM, New York, NY, 1-12.

[7] Morrison, B. B. and Preston, J. A. 2009. Engagement: gaming throughout the curriculum. In *Proceedings of the 40th ACM Technical Symposium on Computer Science Education* (Chattanooga, TN, USA, March 04 - 07, 2009). SIGCSE '09. ACM, New York, NY, 342-346

[8] Nielsen,S. E., Smith, J. H. and Tosca, S. P., *Understanding Video Games*, Routledge, February 2008, ISBN: 978-0-415-97721-0.

[9] Oblinger, D.G. The next generation of educational engagement, *J. Interactive Media in Education*, vol. 8 (2004), [Online] at http://www-jime.open.ac.uk/2004/8/

[10] Ryoo, J., Techatassanasoontorn, A., and Lee, D. 2009. Security education using Second Life. *Computing in Science and Eng.* 7, 2 (Mar. 2009), 71-74.

[11] Wolz, U., Barnes, T., Parberry, I., and Wick, M. 2006. Digital gaming as a vehicle for learning. *SIGCSE Bulletin* 38, 1 (Mar. 2006), 394-395.

[12] Brian Krebs. Cyber security is a national priority. Washington Post (online, May 29, 2009),visited 10/15/2009, http://voices.washingtonpost.com/securityfix/2009/05/obama_cybersecurity_is_a_natio.html

[13] Homeland security, visited 10/15/2009, http://www.whitehouse.gov/issues/homeland_security/]

[14] U.S., South Korea Targeted in Swarn of Internet Attacks Washington Post (online, July 9, 2009), visited 11/3/2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/07/08/AR2009070800066.html

[15] Easttom, C., *Network Defense and Countermeasures*, Prentice Hall, 2005.

[16]. Li, P. 2009. Exploring virtual environments in a decentralized lab. *ACM SIGITE Newsletter* 6, 1 (Jan. 2009), 4-10.

[17] Stackpole, B. The evolution of a virtualized laboratory environment. In *Proceedings of the 9th ACM SIGITE Conference on information Technology Education*, (2008), 243-248.

[18] Schaefer, R. 2009. The epistemology of computer security. *ACM SIGSOFT Software Engineering Notes* 34, 6 (Dec. 2009), 8-10.

[19] CyberCIEGE web site (an Official U.S. Navy website), online, visited December 20, 2009 http://cisr.nps.edu/cyberciege/.

[20] Report: Fake Security Software, Search Engines, Social Networks Top Internet Threats In 2009-- http://netcentricsecurity.com/articles/2009/12/14/report-top-it-security-trends-2009.aspx