A Comparative Study of CyberCIEGE Game and Department of Defense Information Assurance Awareness Video

Jonathan Jones, Xiaohong Yuan, Edward Carr, Huiming Yu
Department of Computer Science
North Carolina A&T State University
Greensboro, North Carolina, USA
xhyuan@ncat.edu

Abstract - **A pilot study comparing the educational effectiveness of CyberCIEGE game and Department of Defense Information Assurance Awareness video was conducted in an undergraduate Introduction to Computer System Security course. The students in this class were split into two groups, with one group playing the game and the other group watching the video. The students in both groups were given a pre-test before using the training tools and were given a post-test after two weeks of using the tools. The student pre-test/post-test scores, the student answers to post-test questions and the student survey results are analyzed and discussed in this paper. Future work includes a more thorough assessment of the effectiveness of Cyber-CIEGE game compared to DoD IAA video.**

I. INTRODUCTION

Video games and interactive simulations have been developed in order to raise the students' interest in information assurance and provide them with hands on experiences. Next Generation Security (NGSEC) is an Internet based security game which has eleven levels, each requiring solving a challenge to obtain authentication credentials [1]. CyberProtect is a product launched by the Information Assurance Support Environment (IASE) [2], an organization which specializes in providing information assurance training for the Department of Defense. CyberProtect is a resource management simulation of a relatively small networked system with external connections. The players select counter measures to various security threats with a limited budget. Another game is Artificial Intelligent Wars, a three Dimensional first person online game. In the game the player interacts with human or artificial objects [3]. "Defensive applications", "offensive applications" and "information applications" are components of the game that incorporate information security concepts. The goal of this game is for entertainment though it increases the player's information security awareness.

CyberCIEGE is an interactive video game developed by the Naval Post Graduate School for information assurance awareness training [4-11]. The player plays the role of security manager and makes management decisions to ensure that the organization is properly secured. In the game, the player budgets money to operate and defend the computer networks and sees the consequences of his/her choices. The player is presented with security-related scenarios with different challenges. A game scenario includes a few characters/employees that play different roles in the virtual organization. The player needs to ensure that the characters are happy and productive in the virtual organization. The player has to balance the budget, productivity, and security in making his/her decisions.

Several studies have been conducted to investigate the suitability of security games as a pedagogical tool for teaching information security. Fung et al. [12] conducted a pilot study on the use of CyberCIEGE for raising awareness and knowledge on information security among a small group of Thai students. The students were evenly divided into two groups with one group playing the game and the other having a one-hour training session. The pilot study compares the two groups' level of awareness on information security before and after using the game or receiving a traditional classroom lecture style of training. Some of the research results include: (1) Both groups have similar level of understanding in the non-lab oriented questions, but the game players appear to have a deeper level of understanding in their answers; (2) The game players had a greater success with lab-oriented questions; (3) The game players feel that they can apply more knowledge into real life, and think it is more mentally challenging; (4) The increase of knowledge from the game players is more than those attended the class lecture. This may be due to the fact that they have spent considerably more amount of time. However, in this study strong conclusions cannot be drawn due to small number of samples.

This research was supported in part by National Science Foundation under the award number DUE – 0737304.

978-1-4244-5853-0/10/$26.00 ©2010 IEEE

Another study on the use of an information assurance simulation game was conducted in Anglia Polytechnic University. This study analyzed the suitability of using the online security game NGSEC as an alternative pedagogic tool. In this study two cohorts were compared. Both groups were given lectures. For one group conventional laboratory sessions were conducted; for the second group laboratory sessions were conducted by means of NGSEC games. This study showed that the second group produced better results in the case study than the first group as they produced an extremely technical and accurate solution for the case study. The difference between the two groups is statistically significant. The students' experiences with NGSEC were positive [13]. It was concluded that online labs based on NGSEC and the amount of research involved to solve them contributed significantly to student's understanding.

The Department of Defense Information Assurance Awareness video (DoDIAA) is a training tool for DoD employees [14]. The video introduces such security topics as physical security, social engineering, and malicious software, etc. At the end of the video various exercise scenarios are presented to the user to apply the knowledge learned from the video.

This paper reports our experiences using CyberCIEGE and DoDIAA in an undergraduate "Introduction to Computer Security Systems" course. The students in this class were divided into two groups, with one group playing the CyberCIEGE game, and the other group using the DoDIAA video. A pilot study was conducted comparing the two groups' level of awareness on information security before and after using the game or the DoDIAA video. The experiment and findings are described in the following sections.

II. CYBERCIEGE AND DODIAA VIDEO

This section provides some background information on CyberCIEGE and DoDIAA video based on which the experiment was conducted.

A. CyberCIEGE

The goal of CyberCIEGE is to create an extensible Information Assurance teaching and learning laboratory. CyberCIEGE includes several different scenarios, each of which can be run separately. Each scenario consists of predefined users, assets, user goals and an enterprise security policy. The elements of CyberCIEGE are: a simulation engine, a scenario definition language, a scenario development tool, student assessment logs and a video-enhanced encyclopedia. New scenarios tailored to specific audiences and topics can be created to extend CyberCIEGE [7].

CyberCIEGE introduces the player to the need for well formed information security policies, allowing the player to deploy a variety of means to enforce security policies, including authentication, audit and access controls [4]. In a scenario, a player engages in such activities as configuring existing computer components, making physical and procedural security choices, hiring IT support staff, purchasing specific components and connecting them to networks [7].

The Starting Scenarios in CyberCIEGE include the following: Introduction Scenario, Physical Security, TirePly Filter Scenario, Patches and GenesRus Biotech. The Introduction Scenario walks the player through the mechanics of the game and introduces the player to a number of the CyberCIEGE security concepts. The Physical Security Scenario introduces CyberCIEGE zones and methods of physically protecting assets. The TirePly Filter Scenario explores issues arising from connecting networks to the Internet and the use of filters to protect assets. The Patches Scenario explores the need to apply software patches to applications and operating systems. In GenesRus Biotech Scenario, the player helps a biotech company secure their valuable trade secrets while developing revolutionary products [11].

B. DoDIAA Video

The Federal Information Security Management Act (FISMA), and the Office of Management and Budget (OMB) Circular A-130 require that all users of Federal computer systems be trained in information system security concerns. The DoDIAA video was designed as a course to fulfill that requirement. The learning objectives are that, upon completing the course, the user should be able to:

- Identify what information assurance is and its importance
- Recognize vulnerabilities of and threats to DoD information systems
- Identify how to protect DoD information systems from threats
- Identify best practices to secure home computer

DoDIAA Video first presents some introductory concepts and information, then ask the user to complete scenario-based exercises.

III. COMPARATIVE STUDY

The "Introduction to Computer Systems Security" course is a junior/senior level elective course in the Department of Computer Science at this university. In Spring 2009, twenty students were enrolled in the class. In this class we conducted a pilot study comparing the educational effectiveness of CyberCIEGE game and DoD video.

First the students were given a twenty-minute pre-test on information security. Then the instructor gave a brief introduction to the game, the video and the purpose of the study. Based on the introduction the students chose which tool they would use in this study. Fourteen students were present in the class with eight students choosing the game and the other six using the video. The students who chose the video could watch it online, but the students who chose the game had to download the tool onto their personal computer. Of the fourteen students, only two had taken an information security related course before this course.

The two groups were given two weeks using the tools without any help on the material. Only guidance on how to use the tools was provided. After two weeks both groups were given the same post-test. The post-test had the same questions as the pre-test but the order of questions was rearranged. We chose topics that are covered by both the video and the game. These topics had not been taught in this class. The students were also given a questionnaire survey.

In what follows, the student pre-test/post-test scores, the student answers to post-test questions and the student survey results are analyzed and discussed.

IV. STUDENT PRE-TEST/POST-TEST SCORES

All students improved their scores from pre-test to post-test. General high-level answers were acceptable. The average percentage of improvement of the game group (40.1%) is higher than that of the video group (33%). The highest percentage improvement for game group was 95.1% and the lowest was 4.4%. The highest percentage improvement for video group was 76.6% and the lowest was 7%. The percentage of improvement is calculated as below:

Percentage Improvement = ((Post-Test – Pre-Test)/Pre-Test) * 100%

However, on average the game group spent much more time (6.15hrs) on the game than the video group (1.75hrs) spent on the DoD IAA Training video. This may be because the game is more interactive, and the students had to play multiple times in order to understand the game.

V. ANALYSIS OF STUDENT ANSWERS TO POST–TEST QUESTIONS

Comparing the student answers to post-test questions from the two groups will give us insight on whether the tools caused different levels of learning. In what follows, the questions on the post-test and answers from both groups of students are listed. For each question we list the answers both groups gave, and the answers only the game group gave and the answers only the video group gave respectively.

1. *Tom is working on a secret design project on his computer. The project is so important that no one except Tom should have access to it. Otherwise it could bankrupt the company. Tom will also require an Internet connection to do web search for information. What would you do to ensure maximum security for the designed project in Tom's computer?*
   - Answers that both groups gave: *Tom's computer should not be connected to the Internet, setup firewalls, and provide Tom with training in security.*
   - Answers only game group gave: *lock Tom's computer every time he leaves his desk, setup strong passwords, Isolate Tom's workspace from the rest of employees, implement high levels of physical security, implement access control lists, and avoid post-its with passwords.*
   - Answers that only the video game gave: *None*
2. *How would you advise your employees regarding the use of email, web site, external media, etc. to minimize the risk of infecting their computer systems with malicious code?*
   - Answers that both groups gave: *Do not allow external media, only use trusted sites, do not open email attachments that could be malicious, install antivirus, install firewall and perform virus scans on external media.*
   - Answers that only the game group gave: *use encryption.*
3. *How could you provide maximum physical security for your top secret department within organization?*
   - Answers that both groups gave: *hire security guards, hire receptionist, log all visitors, require employees to uses badges, use card readers, lock the computers when unattended, and use fingerprint readers.*
   - Answers that only the game group gave: *have physical key locks for doors, use hand scanners, install cameras, install iris scanners, install biometric readers, use encrypted locks, do not allow public access, install steel walls, and alarm system.*
   - Answers that only the video group gave: *Secure all systems in a safe place, Allow authorized personal to enter secure zones, and lock the building at night.*
4. *How would you advise your employees regarding preventing secret information from being stolen (e.g., preventing identity theft)?*
   - Answers that both groups gave: *Be aware of social engineering, use encryption, and lock or log off computers and shred documents.*
   - Answers that only the game group gave: *use ACLs, use strong passwords, Keep passwords secure, and secure secret information.*
   - Answers that only the video group gave: *train the employees on security, use approved company devices, secure all company devices, and report all stolen items.*
5. *What must a security manager/IT manager do to prevent and recover the computer systems from being infected with malicious code?*
   - Answers that both groups gave: *train their staff on computer use, monitor systems, update computers, periodic backups, setup anti-virus, and setup firewall.*
   - Answers that only the game group gave: *none*
   - Answers that only the video group gave: *none*
6. *What are some examples of insider threats?*
   - Answers that both groups gave: *password spoofing, someone within the company who is a threat, and employees with illegal access.*

- Answers that only the game group gave: *social engineering, identity theft, a gruntle employee, an employee who works as a spy, malicious code, ARP cache poisoning and insider phishing.*

- Answers that only the video group gave: *an employee who steals from the company and employee who plants viruses within the company.*

7. *What is social engineering attack (or provide an example)?*

- Answers that both groups gave: *a person who uses trickery to extract information, and phishing.*

- Answers that only the game group gave: *none*

- Answers that only the video group gave: *someone who acquires your personal information.*

The above listing shows the CyberCIEGE video game group provides much more detailed and in-depth answers than the DoD IAA video group for questions 1, 3, and 6. It seems that the game group learned more than the DoD IAA video group.

VI. STUDENT SURVEY RESULTS

The students took a survey after taking the post-test. The students from the game group overall enjoyed the game and agreed that it increased their knowledge of cyber security. The students liked that they were able to apply their knowledge to solve real world problems. However, the students felt that the game was not completely clear on how to complete the objectives. Also some students encountered difficulties because the graphics of the game was not compatible with the graphics cards of their computers. Though some students felt that the CyberCIEGE game was sometimes difficult to understand, they still liked the interactive feature of the game.

The students from the video group overall agreed that they enjoyed the video and their IA knowledge increased. Half of the students thought that video was challenging and the others thought it was not. The students liked the scenarios of the video and the information that was obtained from the video. However, some felt the video had too much clicking and narration was long and boring.

Overall the CyberCIEGE game group was more enthusiastic about the game than the DoD IAA video group was with the video.

VII. CONCLUSION

A pilot study comparing the educational effectiveness of CyberCIEGE game and DoD Information Assurance Awareness video was conducted in an undergraduate “Introduction to Computer System Security” course. The students in this class were split into two groups, with one group playing the game and the other group watching the video. The students in both groups were given a pre-test before using the training tools and were given a post-test after two weeks of using the tools.

Overall the students from both groups improved from pre-test to post-test. The CyberCIEGE game improved slightly more than DoD IAA video group. However, due to small data set strong conclusion on which tool is more effective cannot be drawn. By comparing both groups’ answers to the post-test questions, we found that the game group provided more detailed and in-depth answers than the video group. The reasons could be that the game includes more content than the DoD video. Another reason could be the students in the game group had to spend much more time than the video group which resulted in more learning. This observation is consistent with the research results in [12].

The survey results indicate that the students from the CyberCIEGE group were more enthusiastic about the game than the DoD IAA video group.

In the future we will continue conducting studies to compare the effectiveness of CyberCIEGE with the DoD IAA video and other pedagogical tools, and investigating methods to integrate information assurance simulation games into computer science/information security curriculum.

REFERENCES

[1] Next generation security technologies”, NGSEC [Online] Available at: <http://quiz.ngsec.com> Last accessed: 17 Mar. 2009.

[2] “Information Assurance Support Environment’’, [Online] Available at: <http://iase.disa.mil/eta/index.html> Last accessed: 17 Mar. 2009.

[3] “Artificial Intelligent Wars”, AIWars, [Online] Available at: <http://www.aiwars.com/frames.htm> Last accessed: 17 Mar. 2009.

[4] Irvine, C.E., Thompson, M.F., “Teaching Objectives of a Simulation Game for Computer Security”, *Proceedings of the Informing Science and Information Technology Joint Conference*, Pori, Finland, June 24-27, 2003, [Online] Available at:
<http://cisr.nps.edu/cyberciege/downloads/CyberCiege_ISIT.pdf> Last accessed: August 12, 2009.

[5] Irvine, C.E., Thompson, M.F., Allen, K., "CyberCIEGE: An Information Assurance Teaching Tool for Training and Awareness", Federal Information Systems Security Educators' Association Conference, North Bethesda, MD, March 22-23 2005. [Online] Available at:
<http://cisr.nps.edu/cyberciege/downloads/FISSEA_CyberCIEGE_PreConf.pdf >. Last accessed: March 16, 2009.

[6] Irvine, C. E., Thompson, M. F. and Allen, K. “CyberCIEGE: Gaming for Information Assurance”, IEEE Security and Privacy, May/June 2005, pp. 61-64.

[7] Irvine, C. E., Thompson, M. F. and Allen, K. “CyberCIEGE: An Extensible Tool for Information Assurance Education”, Proceedings of the 9th Colloquium for Information Systems Security Education, June 6-9, 2005. [Online] Available at:
http://cisr.nps.edu/cyberciege/downloads/CISSE_CyberCIEGE_NPS_050305.pdf. Last accessed: August 14, 2009.

[8] Cone, B. D., Irvine, C. E., Thompson, M. F., Nguyen, T. D., "A Video Game for Cyber Security Training and Awareness", Computers & Security 26 (2007) pp. 63-72, [Online] Available at:<http://cisr.nps.edu/cyberciege/downloads/06paper_ccsec.pdf>. Last accessed: March 16, 2009.

[9] Irvine, C.E., Thompson, M.F., “Expressing an Information Security Policy Within a Security Simulation Game” Proceedings of the Sixth Workshop on Education in Computer Security (WECS6), Naval Postgraduate School, Monterey, California , July 12-16 2004, pp. 43-49, [Online] Available at:
<http://cisr.nps.edu/cyberciege/downloads/WECS6_ch08.pdf>. Last accessed: March 16, 2009.

[10] "CyberCIEGE: Can you keep your network alive", The Center for Information Systems Security Studies and Research, Naval Post Graduate School, [Online] Available:
<http://cisr.nps.edu/cyberciege/downloads/CCIEGEbrochure.pdf> Last Accessed: March 17, 2009.

[11] "CyberCiege", The Center for Information Systems Security Studies and Research, Naval Post Graduate School, [Online] Available at: <http://cisr.nps.edu/cyberciege/index.htm>. Last access: March 17, 2009.

[12] Fung, C. C. et al., "Raising Information Security Awareness in Digital Ecosystem with Games – A Pilot Study in Thailand", Proceedings of the Second IEEE International Conference of Digital Ecosystems and Technologies (IEEE DEST 2008), PP. 375 -380, 2008

[13] Ariyapperuma, S and Minhas, A., "Internet Security Games as a Pedagogic Tool for Teaching Network Security", Proceeding of the 35th ASEE/IEEE Frontiers in Education Conference, October 19-22, 2005, Indianapolis, IN.

[14] "DoD Information Assurance Awareness", [Online] Available at: <http://iase.disa.mil/eta/iaav7-3/iaa/launchpage.htm>. Last accessed: August 12, 2009.