Active Learning with the CyberCIEGE Video Game

Michael Thompson, Dr. Cynthia Irvine
{mfthomps, Irvine}@nps.edu
Naval Postgraduate School

Abstract

Hands-on exercises promote active learning where student experience reinforces material presented in lectures or reading assignments [1]. Drawing the student into a meaningful context where student decisions have clear consequences strengthens the learning experience and thus improves the potential for internalization of knowledge. The CyberCIEGE video game was designed to confront students with computer security decision points within an environment that encourages experimentation, failure and reflection. The game includes over twenty scenarios that address a range of computer and network security concepts. CyberCIEGE is extensible through use of a scenario development language that allows instructors to create and customize game scenarios. The Naval Postgraduate School uses the game in our Introduction to Computer Security course, and it has been used by hundreds of educational institutions worldwide. The game's tools allow ongoing experimentation with the student's learning experience. Student assessment is facilitated by log generation, collection and analysis. These logs help the game's developers identify areas within scenarios that may be confusing or may require additional player feedback. Ongoing development is focused on ultimately adapting the game and its student assessment functions for deployment in a broader range of formal education environments.

1 Introduction

When beginning physics students learn the rudiments of mechanics, they do so in a simplified context, unencumbered by the details of harsh reality that include complicating factors such as imperfectly shaped objects and friction. Laboratory exercises are used to reinforce students' understanding of the overarching physical laws and principles that we use to model the macroscopic natural world.

When teaching computer and network security, educators are faced with the problem of creating environments that simplify the network sufficiently so that students can experiment with major abstractions, yet are faithful to our notions of the concrete, real network. To enhance learning about security concepts, students need to have the freedom to fail and try further experiments.

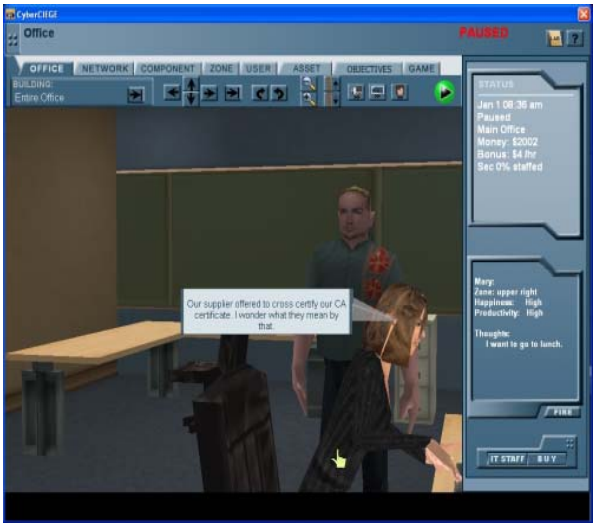

Figure 1: CyberCIEGE screen shot

The objective of the CyberCIEGE video game is to enhance computer security education by demonstrating the abstract functions and limitations of security mechanisms [2]. CyberCIEGE is a construction and management resource simulation somewhat like the Tycoon series of video games [3]. Students play the role of a decision maker for some enterprise such as a small business or military command. The game includes over twenty scenarios that confront students with a series of choices that potentially affect the security of enterprise assets. Figure 1 is a screen shot from one scenario. Students make decisions within a three-dimensional office environment populated by game characters who need to access enterprise assets to achieve goals and thus advance the student through the scenario. Sometimes these goals require the purchase of servers or workstations, other situations require network interconnections to permit sharing of assets between virtual users. An in-game economy rewards the student when users achieve goals and the economy suffers when users fail their goals. The virtual assets have associated motives whose values drive the game's attacks which may include Trojan horses, trap doors, insiders, configuration errors, un-patched software flaws, weak procedural policies and poorly trained users. Students identify vulnerabilities and

mitigate them via deployment and configuration of simulated protection mechanisms including firewalls, user authentication mechanisms, operating system access controls, biometric devices, VPNs and PKI based application security such as email encryption. Some scenarios also require choices related to physical security (e.g., hiring guards), procedural policies and user training.

CyberCIEGE has been in use for six years and has been requested by over four hundred educational institutions worldwide. This paper describes the game from the perspective of computer security educators, and includes overviews of several game scenarios and a summary of the game's use within formal education environments. We describe lessons learned and conclusions based on informal observations, ad-hock student feedback and reviews of game logs. Future work is described, including the need to apply the formal methodology of education research to measure the efficacy of the game in teaching cyber security.

2 Deployment and Support Tools

CyberCIEGE can be played by any student with access to a Windows operating system, which may be a guest on a virtual machine. The game requires the 3D graphics hardware acceleration typical in most laptop and desktop computers. The game runs as a stand-alone application with a single player. It can be installed on a network share and accessed via mapped network drives. The game creates logs of player choices that are consumed by a student assessment tool, which instructors may use to view summaries of student progress and details of individual play. Deploying the game on a shared server inherently centralizes these logs for easy review. The game also includes a simple interface for collecting player logs that can then be emailed to instructors for review.

CyberCIEGE scenarios are organized into "campaigns" which each address different computer security topics, e.g., an "encryption" campaign that includes scenarios that cover VPNs, email encryption and SSL. CyberCIEGE includes a tool that lets instructors organize scenarios into campaigns of their choosing. Additionally, instructors can customize existing scenarios and create new scenarios using the Scenario Development Kit that includes a forms based integrated development environment [4].

The game distribution includes an on-line help facility called the "encyclopedia". This includes descriptions of security concepts from the perspective of the CyberCIEGE game. The encyclopedia also includes a dozen animated tutorial videos that cover security topics such as malicious software, assurance and PKI.

The CyberCIEGE scenarios each include a student lab manual that describes the concepts covered by the scenario and instructions to guide the student through the scenario. There are also instructor notes for the scenarios that are separately provided to instructors.

3 Levels of Abstraction

Relative to traditional hands-on computer security education, CyberCIEGE is more abstract in its representations of computing and protection mechanisms and less abstract in depicting the environments in which those elements operate. The fidelity of computing and protection mechanisms is high enough to require students to make decisions that have observable consequences while not overwhelming them with syntax and interface details. Student observation and appreciation of cause and effect is enhanced through the use of concrete (but often fanciful) scenarios whose outcomes depend on student decisions.

The primary purpose of the game is to bring context to computer security concepts by creating a personalized learning environment where an engaging virtual world helps the player bridge the gap between terminology (e.g., "a firewall") and abstract functions and effects. For example, while a simple lab can illustrate the mechanics and effects of an Access Control List (ACL), the experience is strengthened when authorized users bitterly complain about lack of access, or an attacker compromises assets due to loose ACLs resulting in loss of virtual money that the student worked to earn for the enterprise.

Providing the student with an interactive context also helps illustrate limitations of security mechanisms. For example, a traditional computer vulnerability (hacking) lab can show students how to use a Trojan horse to get around ACLs. CyberCIEGE brings added appreciation of the threats of a Trojan horse by putting the student at the receiving end of such attacks, perhaps resulting from poorly trained users who introduce unauthorized software into the workstation. The concept can then be further illustrated through a different scenario in which an attacker's motive is so high that even well-trained users and strict procedures are unable to keep a Trojan horse from compromising a valuable asset.

The context provided by scenarios helps students understand how abstract information security policies might be implemented through a combination of logical protection mechanisms, physical security and procedural policies. And the scenarios help students understand how security decisions might affect a user's ability to achieve goals. The game does not purport to identify the best solutions to security

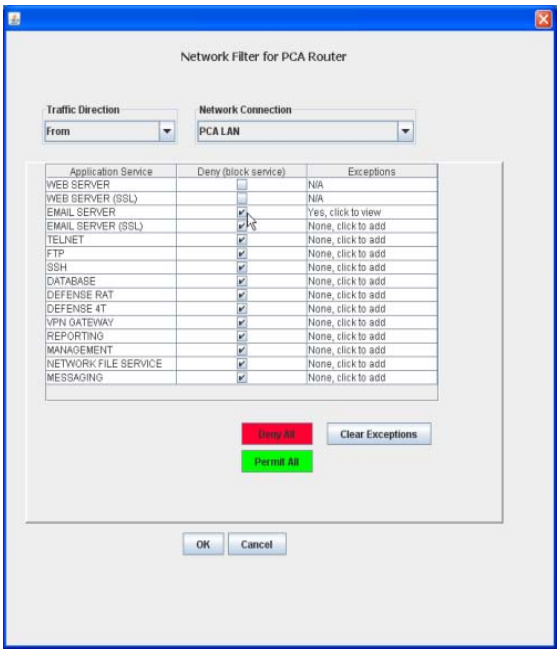

Figure 2: Network filter interface

problems nor does it strive to faithfully represent the security of specific networks. Rather, it gives students an environment in which they can learn through experimentation about the security and productivity issues that may arise in various circumstances.

A student's prospects for actively learning from the environment contrived by CyberCIEGE scenarios is improved if the game maintains "flow" [5] in the student's progress through the scenarios. Maintaining flow requires that the student have a general understanding of what is going on in the virtual environment with just enough lurking threat and problem solving to keep it challenging. If the configuration of security mechanisms requires too much syntax and training, the flow may be interrupted. Obviously, creating a network simulation having enough fidelity to represent actual devices (e.g., a Cisco router) would have required a substantially greater amount of effort than was needed to implement the game's current levels of abstraction. But it also would have made it much more difficult to construct scenarios that provide enough flow to enhance active learning through trial and error and deliberate exploration of "wrong" choices. Figure 2 shows a CyberCIEGE network filter interface, which illustrates the typical level of abstraction incorporated into the game components.

4 Scenario Definition Language

CyberCIEGE is built around a scenario definition language that describes scenarios in terms of users, information, user goals, attacker motives and initial security settings [6]. The CyberCIEGE game engine consumes this language and presents the player with the resulting scenario. The game engine assesses network topologies, security settings and attacker motives and it determines whether a given type of attack will be successful. The economy and attacks are managed by the game engine and thus need not be managed within the scenario definition language. The scenario designer must provide the story line, and the designer must define the scenario objectives and phases such that students can proceed through a coherent sequence of challenges.

The language lets scenario designers make a variety of computers, network devices and security mechanisms available for use within scenarios. Routers interconnect networks and include filters to block or permit selected application service types (e.g., FTP). VPN gateways and clients authenticate and/or encrypt network traffic between selected end-points. The scenario language lets designers choose whether VPN key management will occur via "magic", or whether students must select between shared secrets and PKI, with the latter requiring assignment of CA's, installation of trusted roots and selection of certificate policies. Computer operating systems include ACL enforcement and scenarios can be structured such that students must constrain read and/or modify to assets via ACLs. Other computer operating systems enforce mandatory access control policies, requiring students to assign security labels to network interfaces. Identity management devices such as card readers and retina scanners can be deployed to control access to workstations or to physical zones.

A rich set of in-game triggered events lets the scenario designer provide players with feedback (e.g., characters "speaking" via cartoon text, message tickers, videos, etc.). Designers also use triggers to define the criteria for completing the objectives of a phase and for moving on to the next phase in a scenario. Triggers can also be used to alter the game environment, e.g., to introduce a new set of users and/or goals.

5 Scenarios

This section describes a sample of the CyberCIEGE scenarios that are designed for use within computer security courses. Details of scenarios are included within lab manuals and instructor notes. The simulation of PKI and VPN mechanisms has been described previously [7].

5.1 Tutorial Scenario

An introductory scenario walks students through some of the game mechanics such as purchasing computers and connecting them to networks. Extensive pop-up help guides students to the proper game screens and interfaces to configure policies, train users and adjust physical security. The scenario covers basic security awareness issues including risks of email attachments, installation of unauthorized software and leaving unattended workstations logged in.

The introductory scenario also gives students an opportunity to navigate around the 3D office and explore the online encyclopedia help features. Because it is intended to introduce the game, student choices are constrained and little experimentation is possible in the tutorial scenario.

5.2 Network Filters, Patches and DMZ

Examining these three scenarios helps illustrate the levels of abstraction within CyberCIEGE. The network filters scenario starts with a small company in which the boss's son Larry requires Internet access to perform "research". The company has a small internal LAN and Larry has a workstation but no external link to the Internet. The 3D office view shows the users, their computers. Selecting Larry displays his complaints. A separate screen depicts the network topology and the student can see the offsite "web" resources that Larry has a goal to reach. Starting the simulation results in a loss of cash resulting from the penalty for Larry failing his goal to reach the web asset.

The student must purchase a router (using the in-game catalog of products available for purchase) and connect the router to the company LAN and to the Internet. Doing this pleases Larry and puts the game economy into a surplus instead of a deficit. But the student soon sees that children on the Internet are attacking the company computers because the router's network filters are all very loose by default. As illustrated in Figure 2, the router's network filter interface lets the student selectively close ports, i.e., block application service requests coming from or going to selected networks. The student can experiment with different "correct" configurations, i.e., blocking requests from the Internet or block requests to the internal LAN. And the student can experiment with blocking web service requests from the internal LAN, thereby angering Larry.

The network filters scenario goes on to confront the student with the inability of a network filter to prevent a well motivated attacker from using a Trojan horse to exfiltrate secrets. And the scenario completes with an external user who is authorized to access a company database via SSH. The player has to open an SSH port in the network filter to permit this.

The next scenario in the sequence highlights the need to deploy a patch management system. This scenario directs students to use a simple in-game network scanning tool that reports on outwardly visible software services, e.g., an un-patched web server. The scenario also introduces challenges associated with patching user workstations and ends by requiring the student to purchase a test server so that the onslaught of patches are not first tested on the production server.

The next scenario combines concepts covered in the network filters and patches scenarios and requires that the student deploy a DMZ. The scenario starts with a small company whose internal email is managed on a local server. The company has an Internet connection that provides web access but the initial router filter blocks all application service requests from the Internet. The boss then wants to be able to receive email from her daughter. Since the router is blocking email traffic, the daughter complains and the player starts losing money. If the player opens the email port on the router, attackers exploit a flaw in the email server application, which is also visible to the player via a network scan. If the player deploys patch management for the server then the network scan reports the application has up-to-date patches, but is frequently subject to zero-day exploits.

The solution to the DMZ scenario is to purchase a second email server and deploy it as a proxy for the internal server. A second router is then deployed between the email proxy and the internal LAN. The student must open the email port between the two networks – but only for email traffic originating at the proxy. Students may experiment with solutions that do not involve a DMZ, e.g., if they make filter exceptions for the daughter's remote mail server, the game switches out that mail server. Similarly, if the student protects email via encryption without

deploying a proxy, the email server is brought down via denial of service attacks.

5.3 Email Protection and PKI

CyberCIEGE includes several scenarios designed to illustrate the use and limitations of PKI for managing cryptographic keys [7]. The "Hard Rain" scenario introduces the use of email encryption and signing to protect email, and the scenario reflects the role of PKI in that process. Student choices related to email protection include: which CA will issue a certificate for a given email client; which root certificates will be recognized by the client; and, instructing the user to encrypt or sign email when achieving selected goals.

The scenario opens with a company undergoing an "efficiency improvement", which the employees see as a round of layoffs. The company has an internal server that hosts email services. The employees have administrative access to this server and there is nothing the student can do about that. Two efficiency experts have joined the company and they must exchange email using this server.

The student must provide the two efficiency experts with computers, configure their email clients to support email encryption, and direct them to use email encryption for their sensitive communication (i.e., about who to lay off). The student has to choose a CA to issue the certificates for the email clients. Initially, the only available CA is the "VeriScream" pay-per-cert CA. If that is chosen, a rouge employee pays VeriScream for a misleading certificate that is then used to spoof one of the efficiency experts. The student must purchase a CA so the company has more control over the representations made by the PKI certificates. The student then must hire support staff to manage the CA.

In the final phase of the Hard Rain scenario, one of the employees must provide a remote vendor with an electronically signed purchase order. The vendor is willing to install any root certificate, however the vendor's management prohibits encrypted email because it foils their "ultra deep packet inspection" product. By experimenting in this phase, the student can observe how signing an email does not require the installation of any other root certificates, whereas encrypting the email would require local verification of the recipient's key, which implies either an added root certificate or a cross certification.

The next email protection scenario requires the deployment of smart cards and smart card readers to protect secret keys. A paramilitary group has been activated to protect an international carbon credit derivatives cartel. The group members require use of email, but management has outsourced the email server to the "cloud", which is nothing more than a contractor who has good reason to want to see the content of the emails.

6 CyberCIEGE in Formal Education

CyberCIEGE is an example of what Shaffer, Squire, Halverson and Gee refer to as an epistemic game [8]. The game is designed to encourage students to think like a network security analyst and immerses the student in activities that apply domain-specific knowledge to achieve objectives. Cyber security is a good candidate for active learning because the simulation allows the player to explore sophisticated networks and attack strategies without requiring access to elaborate configurations of lab equipment. Playing CyberCIEGE promotes active thinking by requiring students to apply concepts learned in one context (e.g., the risks of malicious software in an application program) to achieve objectives within some other context (e.g., malicious software within a protection mechanism.) Some scenarios include many ways to achieve objectives, leading to experimentation and innovation by the player.

6.1 Use of CyberCIEGE at NPS

We have successfully incorporated several CyberCIEGE scenarios into our Introduction to Computer Security course as lab exercises. Students perform the labs using shared lab computers, or on their own laptops or personal computers. The game is initially introduced to the students via a one-hour lecture within which the instructor leads group play of one of the more advanced scenarios. This lecture also includes viewing of three of the game's animated tutorial videos. Students are then assigned specific scenarios throughout the quarter. The student assessment tool provides our instructors with summary information about student progress with the labs. We are currently reviewing our network security course offering with a goal of incorporating some of the more advanced scenarios, (e.g., those include PKI deployment) as laboratory assignments.

The scenario for which we have the most experience with student interaction is the network filters scenario. We have reviewed game logs from a sample of 149 recent students. Data from the logs is illustrated in figures 3 and 4. Students spent an average of thirty minutes on this scenario and played it an average of three times, with three quarters of the students playing the scenario more than one time.

Ninety-two percent of the players "won", and about one in five students continued to experiment with the scenario after winning.

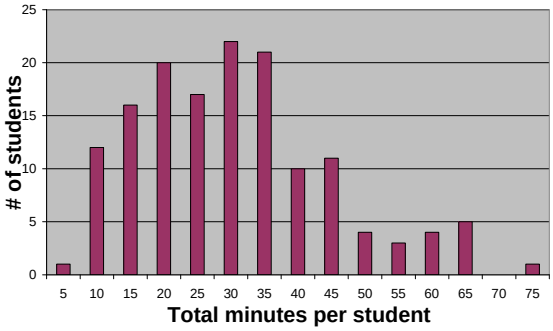

Figure 3: Time spent on network filters scenario

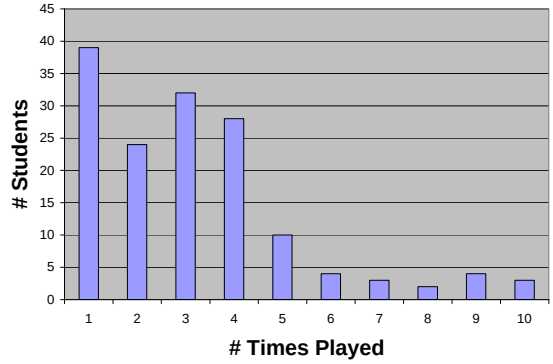

Figure 4: Replaying the network filters scenario

Although we've not performed formal research to assess the effectiveness of the game, our conclusion from ad-hoc student interaction and review of the logs is that the game is effective. As one of our network security instructors observed, "If I see that a student has interacted with a reasonable simulation of a network filter for twenty minutes, and figured out how to win the scenario, I believe the student has probably learned something."

6.2 Use of CyberCIEGE Elsewhere

CyberCIEGE has been incorporated into a range of different curriculums at different levels of education. The Virginia Tech Pamplin College of Business includes the game in their "IS Security and Assurance" course. Students are required to play a large selection of scenarios and create reports on their solutions including discussions of what worked and what did not work. Penn State campuses include the game in their "Introduction to Security and Risk Analysis" courses, and at least one Penn State campus includes several scenarios as labs in their Network Security course. Weber State uses CyberCIEGE as lab exercises in their "Computer and Network Security" class to reinforce security principles taught in the class. Recently, the National Defense University of Taiwan has included CyberCIEGE scenarios as lab assignments in their "Information Security" course.

CyberCIEGE is used by several on-line universities, due in part to its providing hands-on exercises without requiring access to lab systems. For example, TUI University includes it within their IT Security course for undergraduates and graduate students. Technical and vocational schools such as the ITT Technical Institute have used the game as part of network security training for several years.

Researchers have conducted a two limited studies of the effectiveness of CyberCIEGE. Jones, et al. [9] compared CyberCIEGE with a DoD information assurance awareness video in an undergraduate computer security course at North Carolina A&T State University. They found that the students who used the game were more enthusiastic about the game than the other group was about the video. And they found the game group provided more detailed answers to test questions, though that may have been due to the game group investing more time than did the video group. Fung et al. [10] conducted a pilot study on the use of CyberCIEGE for raising awareness and knowledge on information security among a small group of Thai students, comparing the game with a traditional classroom lecture. Both studies were encouraging, though not definitive due to small sample sizes.

7 Lessons Learned

Based on informal interactions with students and ad-hoc written feedback, we have found that students approach games in a variety of different ways, and overall, they approach games differently than they approach other lab assignments. While traditional labs typically require students to reference lab manuals that explain the lab purpose and desired outcomes, students often approach a game expecting to discern its purpose via interaction with a minimum of reading. So while the CyberCIEGE scenarios include detailed lab manuals and on-line help, many students jump into the game without reading anything. This has led us to rework several of the scenarios to provide additional feedback and in-game explanations. We have also been transitioning toward the additional use of multiple choice questions within the game since so many students never see questions embedded in lab manuals.

Some students spend a lot of time on scenarios. Others solve them quickly and move on. Some give up quickly. Most play each scenario multiple times, and eventually complete the scenarios. The ability to run the game on their own computers gives some students the ability to explore the game at their own pace, and informal feedback indicates that this substantially improves the educational experience for some students. Overall, the game works best when the student gets comfortable enough with the tool to explore decision paths without fear of failing. This comfort with failing requires that students are able to grasp the cause of asset compromises, traced back to one or more student decisions. The game facilitates this kind of exploration by letting students save game state that can be returned to after disaster strikes.

Younger students in general seem comfortable with the video game nature of the tool. However some serious gamers who primarily play first person shooter or adventure games find this kind of construction and management simulation genre somewhat disorienting. On the other hand, students who grew up playing sims-type games quickly recognize the intended functions. One of our early concerns was gender differences in video game experience and acceptance, but we've not found that to be an issue.

8 Conclusions and Future Work

CyberCIEGE enhances computer security education through hands-on interaction with a network simulation that lets students experiment with various choices and experience the consequences of those choices. The game illustrates concepts and helps students understand relationships between policy, mechanism and the need for an enterprise to be productive. The student assessment tool helps instructors track student progress through scenarios and identify potential problem areas. The scenario development kit lets instructors customize scenarios and create new scenarios.

As a hands-on educational tool, CyberCIEGE differs substantially from competition-based exercises in that it works best when students knowingly fail. We have considered creating multiplayer versions of the game, however a drawback might be a loss of the student's comfort with failing.

We are working under NSF sponsorship to further align CyberCIEGE with standard computer and network security textbooks and adapt the game for use in formal educational settings in a manner that supports assessment of its effectiveness as an educational tool. This work will also improve and expand the student assessment tool to aid instructors and to aid independent evaluation of the game.

Assessing the efficacy of CyberCIEGE is a challenge that we think would greatly benefit from participation of education researchers versed in formal methodologies for measuring the contribution of the hands-on activities to student understanding. Given that many different organizations use the game, there is potential to obtain log and survey data from a range of environments. Research goals would include an understanding of what motivates students to deliberately explore wrong choices and how much time students are willing to engage in such exploration.

CyberCIEGE creates detailed data sets of player actions. An experienced scenario designer can review these data sets and draw conclusions about where students have problems with scenarios. A future area of investigation will be toward creation of tools that allow scenario designers to correlate game log entry attributes with student choices. The resulting tool could be used by instructors to highlight areas where students appear to have difficulty with the subject matter or the course content, without requiring the instructor to have detailed knowledge of the scenario structure. Similar strategies for mapping log attributes to specific scenario properties can potentially help to quantify the effectiveness of scenarios in teaching selected topics.

References

[1] Bransford, J. D., Brown, A. L., and Cocking, R. R. (eds.). How People Learn: Brain, Mind, Experience, and School. National Research Council, National Academy Press, 2000.

[2] C.E. Irvine, M.F. Thompson, and K. Allen, "CyberCIEGE: gaming for information assurance", Security & Privacy Magazine, IEEE, May-June 2005, Volume: 3, Issue: 3, page(s): 61- 64, ISSN: 1540-7993

[3] A. Rollings and E. Adams, Fundamentals of Game Design. Prentice Hall, 2006.

[4] Naval Postgraduate School, The Center for Information Systems Security Studies and Research, "CyberCIEGE Scenario Development Tool User's Guide", http://cisr.nps.edu/cyberciege/downloads/sdt.pdf. Last accessed 17 April 2010.

[5] Sweetser, P. and Wyeth, P. GameFlow: A model for evaluating player enjoyment in games. Computers In Entertainment 3, 3 (July 2005), http://portal.acm.org/ft_gateway.cfm?id=1077253&type=pdf&CFID=15529450&CFTOKEN=70343664 Last accessed 8 April 2011.

[6] C.E. Irvine, and M.F. Thompson, "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

[7] C.E Irvine, and M.F. Thompson, "Simulation of PKI-Enabled Communication for Identity Management Using CyberCIEGE", The 2010 Military Communications Conference, pp. 1758-1763.

[8] D.W. Shaffer, K.R. Squire, K. R., R. Halverson, and J.P. Gee, Video Games and the Future of Learning, Phi Delta Kappan, Vol. 87, No. 02 (October 2005): pp. 104-111. (http://website.education.wisc.edu/kdsquire/tenure-files/23-pdk-VideoGamesAndFutureOfLearning.pdf)

[9] J. Jones., X. Yuan; E. Carr, H. Yu, "A comparative study of CyberCIEGE game and Department of Defense Information Assurance Awareness video," IEEE SoutheastCon 2010 (SoutheastCon), Proceedings of the, vol., no., pp.176-180, 18-21 March 2010

[10] Fung, C. C. et al., C.C. Fung1, V. Khera, P. Tantatsanawong, P. Boonbrahm "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