CyberCIEGE: A Video Game for Constructive Cyber Security Education

MICHAEL F. THOMPSON & CYNTHIA E. IRVINE, NAVAL POSTGRADUATE SCHOOL

Knowledge must come through action; you have no test which is not fanciful, save by trial.
--Sophocles, Women of Trachis, 450 B.C.

Estimates of the demand for cyber security professionals are as high as 1,000,000 new personnel needed in the global cyber workforce (Cisco, 2014), yet there are insufficient qualified personnel to fill the new positions. Like other organizations, the Navy is also feeling this demand signal. Unless more young people become interested in pursuing cyber security careers, there will be a woeful shortfall of talent.

Can a video game help?

Great technology transitions have changed the way information is conveyed and the way we learn. Just as the printing press transformed information transfer, literacy, and education, thus allowing a student to be absorbed in a book, so has digital technology revolutionized the way we interact with the world and learn. Now, it is common to be absorbed in digital activities.

For decades, educators have suggested that students' attention spans are considerably shorter than the duration of a typical high school or university lecture; and, for decades, creative teachers have used active learning techniques to engage students (e.g. Bonwell and Eison, 1991). Actually, the value of experiential learning has been recognized for millennia.

Role playing, simulations and games are now widely accepted vehicles for active learning (Davison, 1984). Simulations, for example the table-top exercises used at the Naval War College, provide focus to role playing activities and enhance critical thinking. Constructive computer games combine role playing, simulation and gaming to create virtual worlds in which each player can experiment with various methods to achieve focused objectives.

Whereas other constructive video games might have the player build the infrastructure and elements of a town, city, farm, or an amusement park, CyberCIEGE presents a virtual world where computers and networks are required to achieve game objectives. The player's role is to provide a secure infrastructure for that enabling digital technology. Driven by the objectives of the virtual enterprise and its policy for access to and protection of information, the player can choose from a combination of physical, personnel and technical methods to prevent cyber attacks and achieve those goals. The choices available can range from guards at the door and background checks for the virtual world's personnel, to network configuration and monitoring devices.

Although packaged as a video game, CyberCIEGE is a technologically sophisticated network security simulation. It contains many distinct scenarios, each designed to teach selected computer and network security concepts (Irvine, Thompson, & Allen, 2005). The high level objective of CyberCIEGE is to teach students how to build systems less vulnerable to and more resilient to attacks. While cyber exercises, e.g., "capture the flag", have been successfully employed to test operational and exploitation skills, the challenge for CyberCIEGE was to create a game that

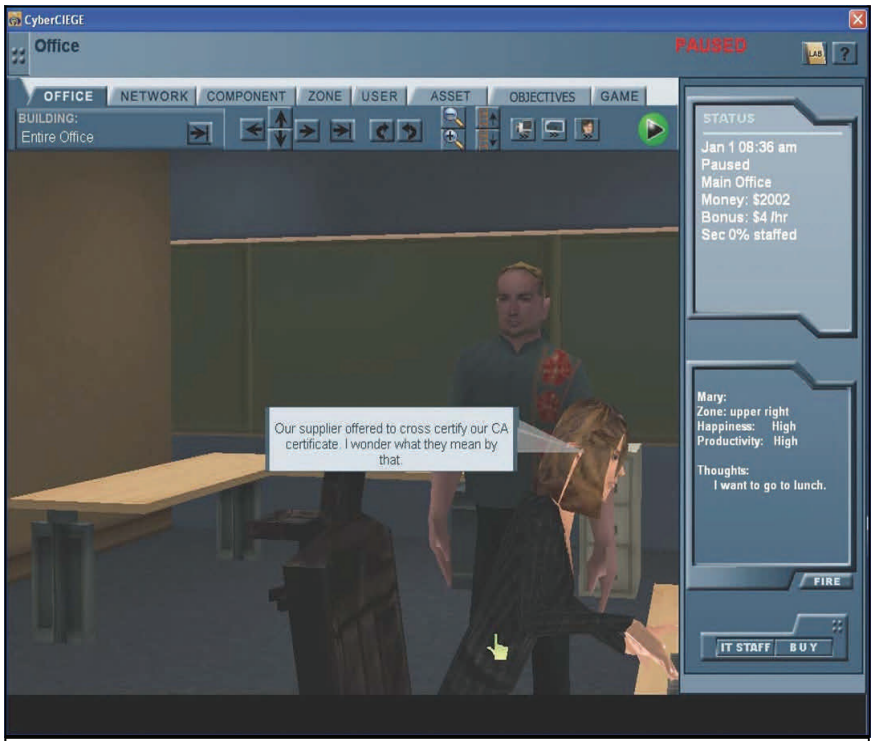

Figure 1: Screen shot of 3D CyberCIEGE environment

could help teach constructive security concepts, some of which can be rather subtle. We have found that, when the game provides a compelling environment in which students can explore, experiment, fail, reflect, and succeed, students do learn these challenging concepts. To build CyberCIEGE, we utilized modern 3D computer gaming graphics, created a network security simulation engine, and developed a suite of tools to design and build game scenarios and monitor student achievement.

Approach to Education

CyberCIEGE uses a variety of constructive resource management techniques (Thompson and Irvine, 2011). Students spend virtual money to build, operate and defend networks, and can watch the consequences of their choices while under cyber-attack. They purchase and configure workstations, servers, operating systems, applications, and network devices. Students make decisions within a three-dimensional environment populated by game characters (AKA *users*) who need to access enterprise assets to achieve goals and thus advance the student through the scenario. An example screen shot of a game underway is shown in Figure 1. An in-game economy rewards the student when game characters achieve goals. Conversely, the economy suffers when characters fail to meet their goals. The virtual assets have associated multi-factored values that motivate and drive the game's attacks, the vectors for 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 by 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's custom game engine uses a scenario definition language for the creation of new scenarios and for tailoring of existing scenarios (Thompson, 2012). Detailed in-game condition assessment and player feedback mechanisms let scenario designers integrate formative assessments into the instructional modules. The Scenario Development Kit (SDK) includes a forms-based integrated development environment (IDE) with which scenario designers express the initial game state, enterprise users and assets, and game phases and objectives. The game engine uses the resulting scenario definition to create the interactive environment. Scenario designers can deploy multiple choice and true/false questions to both test student understanding and help ensure that students remain focused on the scenario's learning objectives (Thompson and Irvine, 2014.) Student choices are logged and these logs are input to a student assessment tool that allows instructors and learning science researchers to monitor student progress.

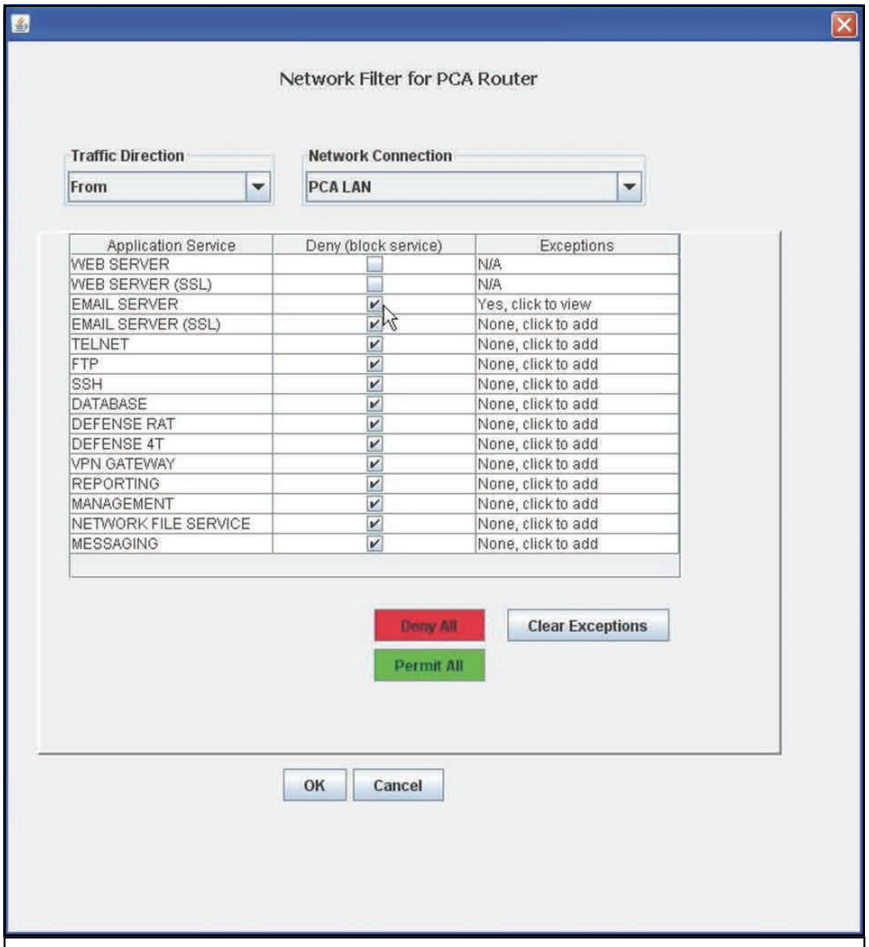

Figure 2: Network filter configuration interface

CyberCIEGE scenarios can consist of multiple phases, where each phase requires the student to achieve one or more specific objectives. Students see their progress in terms of completed objectives and phases. Other feedback includes monetary bonuses and penalties, suggestions from the game characters, pop-up messages and message tickers. Lab manuals accompany the scenarios, which are organized into *campaigns* that address different computer security topics, e.g., an "encryption" campaign that includes scenarios that cover VPNs, email encryption and SSL. A CyberCIEGE tool lets instructors organize scenarios into campaigns of their choosing.

The game includes an on-line encyclopedia that explains cyber security concepts

from the perspective of the simulation. Animated tutorial videos that explore various cyber security topics (e.g., policy, malicious software, assurance, etc.) supplement both the encyclopedia and the scenarios, and can be used separately for classroom instruction.

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 sufficiently high to require students to make decisions that have observable consequences, while not overwhelming them with syntax and interface details. The virtual worlds presented in the scenarios, are typical of those students might encounter in the workplace or at home. Student observation and appreciation of cause and effect is enhanced through the use of concrete (but often fanciful) scenarios the outcomes of which depend on student decisions. The game brings 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., "firewall") and abstract functions and effects. For example, while a simple lab can illustrate the mechanics and effects of an Access Control List (ACL) associated with a file containing personally identifiable information, the experience is heightened when authorized users within CyberCIEGE's virtual world bitterly complain about lack of access, or when an attacker compromises assets due to loose ACLs, with consequent loss of protected information and virtual money that the student worked to earn for the enterprise.

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. Furthermore, 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 problems nor does it strive to faithfully represent the security of specific networks. Rather, it gives students an environment in which they can learn about the security and productivity issues that may arise in various circumstances. CyberCIEGE is an example of an epistemic game (Shaffer et al., 2013) in which students are immersed in environments that matter to them and are encouraged to think like subject matter experts.

CyberCIEGE is designed to encourage each student to play the role of and think like a network security analyst. The immersive simulation allows the player to explore sophisticated networks and attack strategies without requiring access to elaborate configurations of lab equipment. Students use domain-specific knowledge to achieve objectives. 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) to achieve objectives within some other context (e.g., strategies to address the problem of malicious software within a protection mechanism.) Experimentation is encouraged and not penalized.

A student's prospects for actively learning from the environment presented by CyberCIEGE scenarios depends, in part, on maintaining game "flow" (Sweetser and Wyeth, 2005) as the student progresses 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. Hence the level of abstraction presented to the student must be sufficient to convey the concepts, but not so complex that it would bog the student down with details best learned in product-specific activities. Figure 2 shows a CyberCIEGE network filter configuration screen: this illustrates the typical level of abstraction implemented in the simulation. A network filter might be a firewall or part of a router. The objective of CyberCIEGE is to teach students why network filters are important and the types of choices that may be made when configuring such filters: not all connections into the enterprise network should be permitted, neither should all possible outgoing connections be allowed. The arcane details of firewall or router configuration syntax are absent.

Discussion

CyberCIEGE's simplicity can be a boon to instructors beleaguered with many demands in the classroom. First, many schools today, whether K-12 or at the university level, offer little or no cyber security instruction. This is

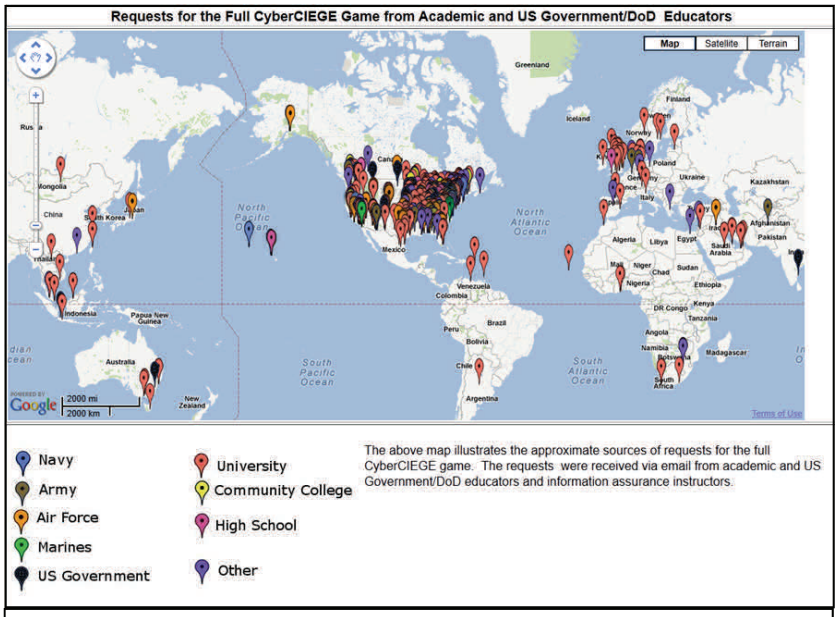

Figure 3: Requests for CyberCIEGE from educators

especially the case when instructors have limited experience in digital technology and cyber security, and lack resources to construct and utilize elaborate infrastructures. Second, because it does not require special laboratory resources, CyberCIEGE affords students an independent study tool. Often instructors use the evaluation version of the game with an entire class and then obtain the full version for students who want to explore more. In addition, many active duty military who wish to improve their knowledge and skills use CyberCIEGE for independent study. Finally, in-game formative assessment shortens and improves the typical cycle required for an instructor to detect and mitigate student confusion; more timely intervention guides the student back toward the intended learning objectives.

Although CyberCIEGE has been very popular, it would be naïve to expect it to be embraced by all students; some enjoy games and are fully engaged, whereas others do not like games and consider it drudgery. As is the case for most video games, the overwhelming majority of CyberCIEGE's development has been by males, thus the game may reflect unintended gender biases. We do not know if the game is equally appealing to both male and female players, or how subtle gender-related issues could be addressed through changes to scenarios, artwork, and other elements of the overall CyberCIEGE package.

The success of CyberCIEGE is reflected in its broad and growing use by educational institutions worldwide. The game has been informally evaluated by a variety of educators, with many integrating the no-cost educational tool into their cyber security curricula (Jones, Yuan, Carr, & Yu, 2010). With the participation of fourteen Naval Postgraduate School students, CyberCIEGE has evolved considerably since its initial release in 2005, growing from a handful of proof-of-concept scenarios to over twenty full scenarios. Through years of informal student and instructor feedback, the NPS game developers have gained considerable knowledge of strategies for immersing students into a simulated environment where they experience consequences of their choices (Thompson & Irvine, 2011).

Future Work

Over ten years after its initial release, educators worldwide continue to contact NPS several times a week to request CyberCIEGE, resulting in broad distribution of the game as illustrated in Figure 3. While this word-of-mouth marketing suggests some level of educational success, there has not yet been a formal study of the game's effectiveness. Future work to improve CyberCIEGE would greatly benefit from collaboration with experts in learning metrics and formative assessment to demonstrate its educational value and to identify strategies for improved learning outcomes.

CyberCIEGE currently requires a PC platform (or Windows in a virtual environment). Porting it to a ubiquitous gaming platform such as Unity would further broaden its potential audience, making it available on tablets and other computing platforms. Additionally, the growing proliferation of mobile computing platforms and wireless networks increases the need for innovative tools to help teach fundamental wireless security concepts. This need could be addressed by a project to extend the CyberCIEGE simulation to include wireless devices such as smartphones, tablets, laptops, and wireless access points. Such an effort would create new scenarios to illustrate wireless security risks and tradeoffs, and could also introduce wireless devices into existing scenarios. Furthermore, new scenarios reflecting emerging cyber security issues, for example in social networking and privacy, would help extend cyber security awareness to additional populations.

Summary

Games can offer great opportunities for experiential learning both in the classroom and for independent learners. With over ten years of use by the Navy, DoD, US Government, and educational institutions, CyberCIEGE offers a tool to support cyber security awareness, training and education. It is available at no cost to the Navy and can be accessed through the CyberCIEGE website at http://cisr.nps.edu/cyberciege/.

References

Bonwell, C. C. and Eison, D. (1991) Active learning: Creating excitement in the classroom. Technical report, Office of Educational Research and Improvement, Washington, DC, USA. http://files.eric.ed.gov/fulltext/ED336049.pdf

Cisco Systems. Cisco 2014 Annual Security Report. Cisco Systems, Inc., San Jose, CA, 2014.

Davison, J. G. (1984). Real tears: Using role plays and simulations. *Curriculum Review*, 23:91–94, 1984.

Irvine, C.E., Thompson, M.F., and Allen K. (2005). CyberCIEGE: gaming for information assurance. *Security & Privacy Magazine*, 3(3), 61- 64. (http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1439504) Jones, J., Xiaohong

Shaffer, D.W, 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, pp. 104-111, October 2005. (http://website.education.wisc.edu/kdsquire/tenure-files/23-pdkVideoGamesAndFutureOfLearning.pdf)

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 17, September 2012.

Thompson, M.F. and Irvine, C.E. (2011). Active Learning with the CyberCIEGE Video Game, 4th Workshop on Cyber Security Experimentation and Test, San Francisco, CA, August 8, 2011.

Thompson, M.F. (2012). CyberCIEGE Scenario Development Tool User's Guide. Monterey, CA: The Center for Information Systems Security Studies and Research. (http://www.cisr.us/cyberciege/downloads/SDT.pdf)

Thompson, M.F. and Irvine, C.E., CyberCIEGE Scenario Design and Implementation, 2014 USENIX Summit on Gaming, Games, and Gamification in Security Education, San Diego, CA, August 18, 2014.

Yuan, Carr, E., & Huiming, Yu. (2010). A comparative study of CyberCIEGE game and Department of Defense Information Assurance Awareness video. Proceedings of the IEEE SoutheastCon 2010 (SoutheastCon), pp.176-180. (http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5453895&tag=1)