THE JOURNAL OF
DIGITAL FORENSICS,
SECURITY AND LAW

Journal of Digital Forensics,
Security and Law

Volume 2 | Number 4 Article 1

2007

SecurityCom: A Multi-Player Game for Researching and Teaching Information Security Teams

Douglas P. Twitchell
Illinois State University

Recommended Citation

Twitchell, Douglas P. (2007) "SecurityCom: A Multi-Player Game for Researching and Teaching Information Security Teams," *Journal of Digital Forensics, Security and Law*: Vol. 2 : No. 4 , Article 1.
DOI: https://doi.org/10.15394/jdfsl.2007.1029
Available at: https://commons.erau.edu/jdfsl/vol2/iss4/1

SecurityCom: A Multi-Player Game for Researching and Teaching Information Security Teams

Douglas P. Twitchell
Illinois State University
Campus Box 5150
Normal, Illinois 61790
dtwitch@ilstu.edu

ABSTRACT

A major portion of government and business organizations' attempts to counteract information security threats is teams of security personnel. These teams often consist of personnel of diverse backgrounds in specific specialties such as network administration, application development, and business administration, resulting in possible conflicts between security, functionality, and availability. This paper discusses the use of games to teach and research information security teams and outlines research to design and build a simple, team-oriented, configurable, information security game. It will be used to study how information security teams work together to defend against attacks using a multi-player game, and to study the use of games in training security teams. Studying how information security teams work, especially considering the topic of shared-situational awareness, could lead to better ways of forming, managing, and training teams. Studying the effectiveness of the game as a training tool could lead to better training for security teams.

Keywords: Experiential Learning, Security Education, Gaming

1. INTRODUCTION

With the rise of information technology and information availability has come the inevitable rise of information theft as well as other threats to security that are specific to information technology. Some of the threats familiar today include viruses, spyware, phishing, identity theft, and corporate espionage. Information security, a field of study that originated in the military's need for secrecy, has now evolved into a multi-faceted research area with immediate implications in today's world. Research into information security has resulted in many valuable technologies such as firewalls and anti-virus software, yet has also called attention to the need for education and training for both general computer users and information security specialists. Games and other simulations are beginning to be a part of this education and training and research.

The use of games for teaching or research is not new. Games and other simulations have been used for business training and research since the 1960s (Kolb & Wolfe, 1990). The main reasoning for using games and simulations for training and education is that there is a body of evidence suggesting that experiential learning creates superior learning outcomes in the learner than lecture-style learning does (Kolb, 1984). Experiential learning is learning that involves some degree of applying concepts by performing tasks that relate to the concepts. Often experiential learning is meant to give the learner an opportunity to make decisions in a low-risk environment while at the same time giving the learner an emotional appreciation for how the concepts work in the "real world." Experiential learning with games has also been extensively and successfully used in teaching and learning in teams (Kayes, Kayes, & Kolb, 2005).

The use of games in security education and training is also not new. Several games have been developed over the years to help end users understand the need for security and to help security professionals become better at making decisions concerning security (Saunders, 2002). Among them are CyberProtect from the Defense Information Systems Agency, and CyberCIEGE from the Naval Postgraduate School. However, in these and other information security games, the emphasis has not been on learning as teams, and although these games include monetary trade-offs, they don't include the political trade-offs and negotiations between security and availability—at least those that include negotiations between real people.

To evaluate these games and guide the development of a new information security game that involves teams, we can use Demsey, Haynes, Lucassen, and Casey (2002) who listed the following Criteria on which to evaluate a game for learning:

1. The game must be relatively simple to play.
2. The game can be adapted and reprogrammed inexpensively.
3. The game must have some identifiable potential for educational use, if adapted.
4. The game must be different from the other games in its category.
5. The game must be designed so that it can be played by a single player.

For games created for information security education, Criterion 3 is given, and since we are emphasizing team performance, Criterion 5 is less important. Therefore, we will evaluate CyberProtect, CyberCIEGE, StrikeCom, and the proposed game using Criteria 1, 2, and 4.

CyberProtect, created for the Defense Information Security Administration in 1999, won several awards for gaming in general. In this game, the player represents a network administrator with a budget who must buy equipment and training to defend the network against attack. The game is played in rounds during which the player must buy and install assets with varying degrees of effectiveness and in various locations on the network. When a round is complete, random attacks are attempted on the network, and their efficacy reported. When finished the game gives the player an overall report of preparedness. CyberProtect's user interface and game-play are relatively easy with only two screens (the network, shown in Figure 1, and the budget) to navigate during play, therefore, CyberProtect meets Criterion 1. However, the game source code and configuration are hidden, so Criterion 2 is not met. Finally, CyberProtect was one of the first computer games produced for information security education and therefore meets Criterion 4.

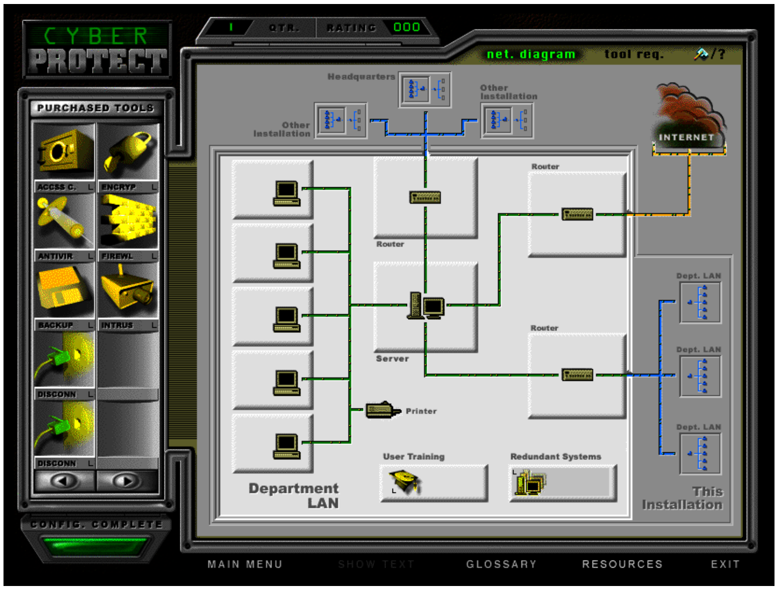
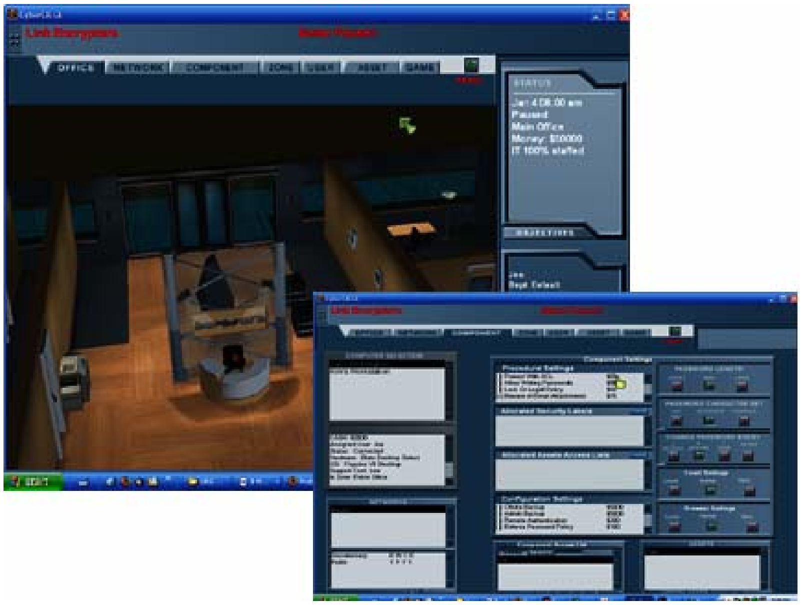


Figure 1 A screenshot of CyberProtect showing the view of the network

Another, CyberCIEGE (Irvine, Thompson & Allen, 2005), was recently created and was developed using the same kind of interface as the popular game *The Sims*. Players in this game are immersed in a three-dimensional office where they can be confronted with a number of different information security scenarios. These scenarios are configurable through a language developed for the game itself allowing a high level of configurability and handily meeting Criterion 2. However, the ability to adapt and configure the game to complex situations and scenarios seems to make the game more difficult to use. The player's interface includes seven panels, which include the main 3D interface and six other panels with various options for the user (see Figure 2). While such complexity may allow for more realistic scenarios and may be appropriate for longer courses where learning the interface can take place, it doesn't seem that the game meets Criterion 1 and may not be appropriate for shorter training courses. Since, however, CyberCIEGE is highly configurable, it may be possible to design scenarios with simple, easy-to-learn interfaces. CyberCIEGE does, however, meet Criterion 4.



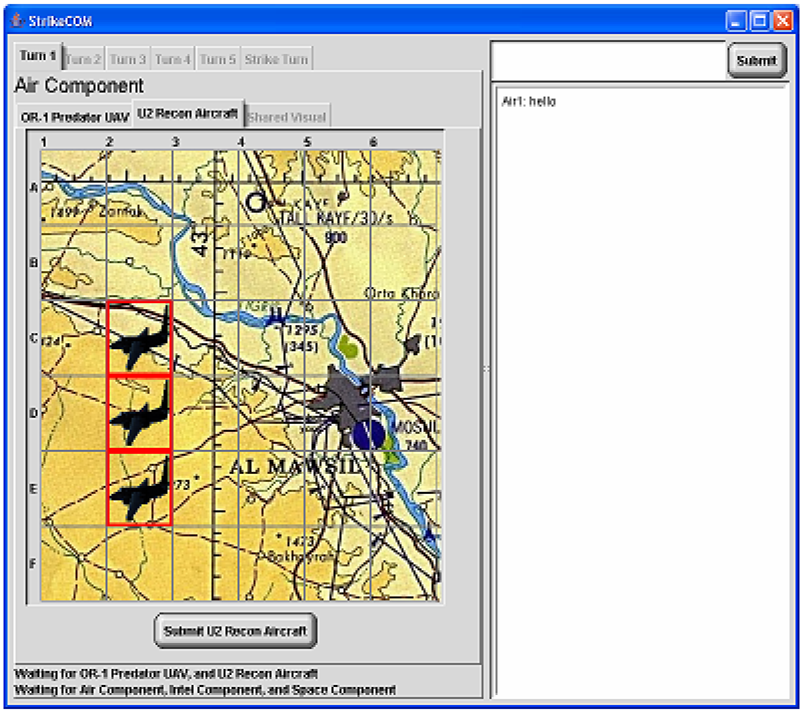
Jan 4 08:00 am
Paused
Main Office
Money: $10000
IT 100% staffed

Figure 2: Screenshots from CyberCIEGE showing the 3D office view (upper left) and a detail panel (lower right)

Finally, StrikeCom (Twitchell, *et. al.*, 2005) was originally created to support deception detection research, and was later used by the Department of Defense's Office of Force Transformation during short course seminars to teach some of the tenets of Network Centric Warfare (NCW) including shared situational awareness. The game requires teams to search a grid-based game board for enemy camps. In the most commonly used configuration, each player had two assets with which to search the board. During each of five turns, the players search the board and submit their search. At the end of each turn, the game returned one of three results: likely nothing found, uncertain, or likely something found. After the end of the five searching turns, the teams use the information acquired in the previous rounds to place bombs for destroying the enemy camps.

When StrikeCom was used in military officer training, the emphasis was placed on the communication among team members during the searching and striking rounds. These communications were the basis for teaching NCW. NCW (Cebrowski & Gartska, 1997) is one of the leading theories currently driving U.S. military operations. It contains five tenets: 1) Knowledge of the adversary; 2) Shared situational awareness; 3) Commanders intent; 4) Decentralized execution and 5) Self synchronization. Of these, Shared

Situational Awareness (SSA) is one of the most appropriate for implementation using information security—especially in teams. It has shown to be a valuable tenet of network-centric warfare through the use of tools such as the Blue Force Tracker used in Iraq and Afghanistan. This tool allows individuals from all levels of the military to be able to see where they are in relation to others on both sides of the battlefield. Furthermore, it gives them the information they need to make informed decisions that might affect others. Since information security (or information warfare as it has been called) is often compared to warfare, SSA could be just as important to information security as it is for military operations and should be tested as a part of an information security system.



Waiting for OR-1 Predator UAV, and U2 Recon Aircraft
Waiting for Air Component, Intel Component, and Space Component

Air1: hello

Figure 3: A screenshot from StrikeCom's Search phase.
The game board is on the left, and the chat window is on the right

StrikeCom was used during NCW short courses offered by the Department of Defense to experientially illustrate the concept of SSA and other NCW tenets. To accomplish this, the game was tuned so teams of 3 officers or civilians play using 3 communication media. The first game has players sitting next to each other and talking face-to-face, the next game is played using chat only with players who are anonymous. These two game situations are common experiences in actual tactical and operational military interactions. Hence, post-hoc analysis of game scores, communication channel, player behavior and interaction reveal a number of critical teaching points for intent, decentralized execution, self-synchronization and SSA. After these two games are played and debriefed, a third game is played with a shared visualization tool (augmented SSA) added. At the conclusion of the final game, NCW concepts are evaluated with the training group via a panel of experts. StrikeCom was, according to user feedback comments, successful at supporting these workshops for the training of NCW concepts with various military groups around the world.

Like CyberCIEGE, StrikeCom is highly configurable, but is also simple to use, as is illustrated by its wide use in short training courses where the students learned how to use and used the game for learning in a two-hour session. Therefore, StrikeCom meets Criteria 1 and 2. However, it doesn't necessarily meet Criterion 4, since other grid/turn-based games have been used in the past.

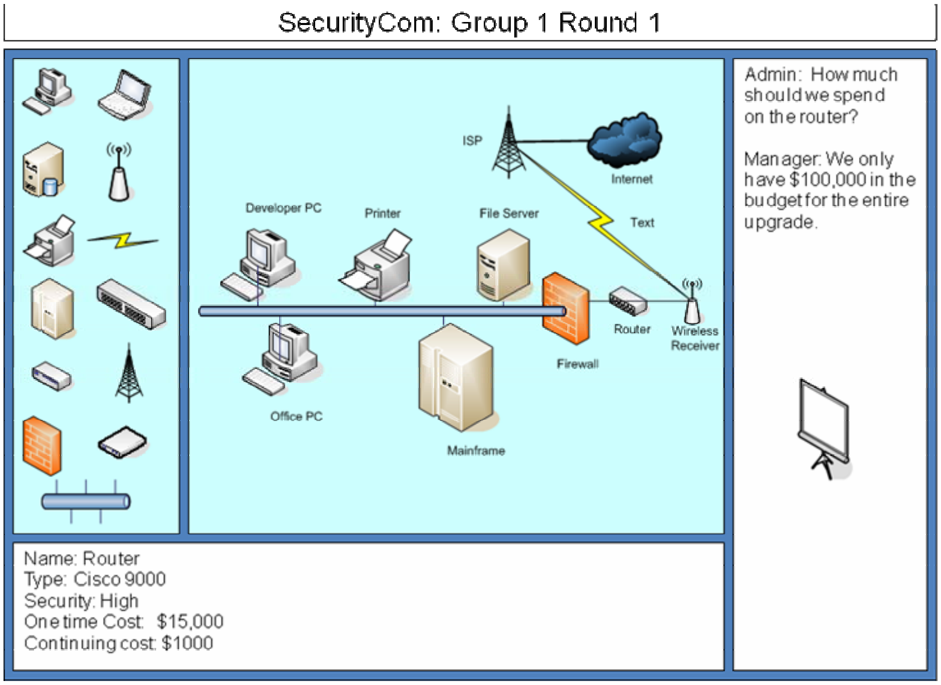
Despite its team orientation, its ease of use, and configurability, StrikeCom is not specifically built for information security education and research. Although deception detection and shared-situational analyses are well-simulated in the game, information, computer, and network security are not. Therefore, we propose modifying StrikeCom to have a simple information security interface while retaining its team orientation and configurability. The new game will be called SecurityCom.

2. OBJECTIVES OF PROPOSED RESEARCH

This research has three main objectives. First, build a research and teaching tool, SecurityCom, that can be used in this and other projects to test aspects of team interaction and education in information systems security. Second, determine how important SSA is to the effectiveness and efficiency of information systems security teams. Third, determine how effective SecurityCom is at aiding the education of security personnel compared to other learning modes.

2.1 Build SecurityCom

SecurityCom will be built using the same concepts as StrikeCom used—team interaction and simplicity. The user interface will allow for the interaction between security personnel on the team and also allow for the researcher to capture communications among team members. A chat window will be the main channel of communication, which will provide the means to communicate remotely or co-located, and it will allow capture by the researcher. The user interface will be simple and intuitive so that the user will require a minimal amount of training to complete the exercise. CyberProtect was a good example and aspects of its user interface design will be integrated into SecurityCom's user interface. The user interface itself will be built on a web-browser-based interface to allow for ease of administration and deployment. A mock-up of the user interface is shown in Figure 4.



SecurityCom: Group 1 Round 1

Admin: How much should we spend on the router?

Manager: We only have $100,000 in the budget for the entire upgrade.

Name: Router
Type: Cisco 9000
Security: High
One time Cost: $15,000
Continuing cost: $1000

Figure 4: A mock up of the SecurityCom interface
Left: a palette of network components.
Middle: the dynamic network diagram or shared situational awareness.
Right: a chat window for communication.
Bottom: network component properties

2.2 TEST SHARED-SITUATIONAL AWARENESS (SSA)

SSA is the ability of all team members to see the dynamic environment in real-time as it changes. The information SSA gives allows team members to make informed decisions on future actions. In battle, the use of SSA results in greater effectiveness at hitting targets, greater efficiency in the use of resources, and fewer friendly-fire incidents. In information security SSA should allow security teams to make quicker decisions concerning security controls and allow them to be more effective in mitigating risk. The purpose of this objective is to test whether SSA does increase efficiency and effectiveness in mitigating information security risk.

2.3 Test SecurityCom against other games and methods

As indicated above, the use of games for information security education is not new, and there are several games such as CyberProtect and CyberCIEGE that have already been developed. Therefore, SecurityCom should be compared against these other games to determine whether it is superior or inferior in its effectiveness at aiding the teaching of security concepts. Unfortunately, these and other information security games currently available are not multi-player, so the comparison will have to be done with individuals. Comparing the games not only provides evidence for which game is more effective, but it also helps inform researchers whether the theories upon which the games are built have validity. Furthermore, the purpose of this objective is to test SecurityCom's performance relative to other games, but also other modes of learning such as classroom lecture.

3. METHODOLOGY

The philosophy underlying the methodology of this research project is the information systems field's Design Science (Hevner, March, Park, & Ram, 2004). This research methodology framework is based on the idea that information systems research should be centered on an "IT artifact:" a formal method, instrumentation, computer program, or hardware that is designed, built, and tested. Theory informs the design and construction of the artifact, and the subsequent testing in the laboratory, the field, or other suitable arena. The design and testing then feed into improvement of the theory or creation of further theory.

SecurityCom is the IT artifact to be designed, built, and tested. The informing theories include experiential learning theory, the theory that educational, training, and awareness are integral to information security, and the NCW tenet of SSA. Once built, SecurityCom will be used to perform two laboratory experiments. The first experiment will test the usefulness of SSA in security teams, and the second will test the SecurityCom game against other information security games.

To test the usefulness of SSA in information security, groups of three subjects will be randomly assigned to one of two treatments. In the first treatment the groups will not have a SSA displays during the first half of the game, but it will be given to them during the second half. In the second treatment, the opposite will be done: the groups will have the SSA during the first half, but will not have it during the second. Effectiveness at mitigating risk to information security on the given network will be the dependent variables that will be measured at half way through the game and at the end of the game. Differences between the treatments will be compared using repeated-measures ANOVA.

In the second experiment, SecurityCom with full SSA will be compared to two (or one depending on the availability of subjects) other information security experiential learning games. This time, because the other games are not yet capable of multi-player play, individuals will be randomly assigned to one of four (or three) treatments: SecurityCom with SSA, CyberProtect, CyberCIEGE, or classroom lecture. The dependent variable to measure is the individual's grasp of a specific information security concept. The learning will be measured by comparing a pre- and post-test. Again, repeated-measures ANOVA will be used to assess the differences among the treatments.

Together these experiments using SecurityCom will provide evidence on the usefulness of SecurityCom specifically and gaming generally in information security education and shared-situational awareness in information security team effectiveness. The evidence can then be used to further update the informing theories.

4. CONCLUSION

It is encouraging to see the advances being made in using experiential learning in information security education. In addition to the games mentioned in this paper, the Collegiate Cyber Defense Competition (CCDC) run yearly around the U.S. provides an immersive, semi-real-world environment where students can apply what they have learned while under pressure. Since the CCDC requires numerous resources and is therefore only run once each year, the games mentioned and proposed in this paper provide a means for continuous experiential learning with little investment in resources.

SecurityCom, based on CyberProtect and StrikeCom, will provide an experiential learning platform for teaching team concepts in information security, especially those involving the allocation of scarce resources and the tension between security and availability. Learners using SecurityCom will get a taste of how security is implemented in the context of organizational resources and politics, and they will gain some experiences advocating for security. SecurityCom should also be valuable to information security researchers hoping to gain insight into the behavior of information security professionals that work in teams, especially shared-situational awareness.

ACKNOWLEDGEMENTS

This paper was originally presented at the 2007 Information Security Curriculum Development Conference, September 28-29, 2007, Kennesaw, Georgia, USA.

AUTHOR BIOGRAPHY

Douglas P. Twitchell, PhD is an assistant professor of information systems in the School of Information Technology at Illinois State University. He is the author of several articles and conference proceedings on behavioral issues in information security. His other research interests include online conversations, text mining, and deception detection.

REFERENCES

Cebrowski, A. K., & Garstka, J. (1997). “Network centric warfare: Its origin and future. Naval Institute Proceedings,” 124(1), 28-36.

Dempsey, J. V., Haynes, L. L., Lucassen, B. A., & Casey, M. S. (2002). “Forty simple computer games and what they could mean to educators.” Simulation & Gaming, 33(2), 157-168.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). "Design science in information systems research." MIS Quarterly, 28(1), 75-105.

Irvine, C. E., Thompson, M. F., & Allen, K. (2005). "CyberCIEGE: Gaming for information assurance." Security & Privacy Magazine, 3(3), 61-64.

Kayes, A. B., Kayes, C. D., & Kolb, D. A. (2005). "Experiential learning in teams." Simulation & Gaming, 36(3), 303-329.

Keys, B., & Wolfe, J. (1990). "The role of management games and simulations in education and research." Journal of Management, 16(2), 307-337.

Kolb, D. A. (1984). Experiential learning: experience as the source of learning and development. Englewood Cliffs, N.J.: Prentice-Hall.

Saunders, J. H. (2002). "Simulation approaches in information security education." Journal of Information Security, 1(2).

Twitchell, D. P., Wiers, K., Adkins, M., Burgoon, J. K., & Nunamaker, J., Jay F. (2005). 'StrikeCOM: A multi-player online strategy game for researching and teaching group dynamics.' Paper presented at the Thirty-Eighth Hawaii International Conference on System Sciences (CD/ROM), Big Island, Hawaii