Winter 12-15-2012

CollabSec: A Multi-Player Game for Researching and Teaching Information System Risk Assessment

Douglas Twitchell
Illinois State University

Christie M. Fuller
Louisiana Tech University

David Biros
Oklahoma State University

Kent Marett
Mississippi State University, kent.marett@msstate.edu

CollabSec: A Multi-Player Game for Researching and Teaching Information System Risk Assessment

Douglas Twitchell
School of Information Technology, Illinois State University,
Normal, IL, USA

Christie M. Fuller
College of Business, Louisiana Tech University,
Ruston, LA, USA

David Biros
Spears School of Business, Oklahoma State University,
Stillwater, OK, USA

Kent Marett[1]
College of Business, Mississippi State University,
Mississippi State, MS, USA

ABSTRACT

This paper introduces CollabSec, a new tool for studying risk assessment in a collaborative online environment. Players decide how to allocate limited resources to apply controls to various assets to mitigate threats and protect a network. A set of rules determines the impact of these decisions on a variety of risk outcomes in an organization. The game will be used to teach and train students and employees, as well as perform empirical research.

Keywords: Information Security Education, Games, Collaboration, Risk Management, Virtual Teams

INTRODUCTION

Information security is a critical and costly issue for managers in business organizations. It has been estimated that the cost to reconstitute a single lost or damaged record after a security breach is between $90 and $205 (Kouns and Minoli 2010). Security-related activities like risk assessment and policy implementation are highly complex and require collaboration between all affected stakeholders. Given the limited availability of time, financial resources, and employee-power, information security

[1] Corresponding author. kent.marett@msstate.edu. +1 662 325 7001

planning and execution demands coordination and collaboration with specialists within the IT domain (Werlinger et al. 2009). An earlier series of interviews with security specialists showed that security assessments are high in task interdependence with others and often require a daily exchange of information between decision makers (Knapp et al. 2005).

Previous research has examined learning principles designed for educating end users on security policies and procedures (e.g. Puhakainen and Siponen 2010), but to our knowledge, there have been no studies that investigate collaborative information technology risk management and the complexities of making necessary decisions required to implement countermeasures necessary for protecting information in such an environment. There have been a few previous games developed for studying network security and risk assessment principles (Irvine et al. 2005; Surdu et al. 2003; Uiterwijk 1999). CyberProtect was one of the first and won several awards. However, CyberProtect was a single-player game and is not adaptable to different scenarios (Uiterwijk 1999). MAADNET is also a single-player game, though different scenarios can be incorporated (Surdu et al. 2003). CyberCIEGE does allow some customization and multiple players, but is rather complex and therefore has limited potential for the limited time-span of most educational exercises and research experiments (Irvine et al. 2005). StrikeCOM (Twitchell et al. 2005) allowed groups and had some capabilities for customization; however it is based on a military scenario. Our aim with this research effort is to move towards a more general information security platform that allows for collaboration and customization.

This paper describes the development of an online game that simulates a typical local area network found in business organizations, the assets residing on the network, the threats that potentially exploit those assets, and a series of controls that could be used to protect the assets. In addition to reinforcing concepts on risk assessment, the game also requires the collaboration of players seeking to implement a rigorous security program with limited resources. We describe the main aspects of the game and briefly discuss future research to be conducted using the game.

COLLABSEC DESCRIPTION

CollabSec is a web-based multiplayer security strategy game created using Ruby on Rails, an open-source web framework for application development. It is designed for scenario flexibility and multiplayer collaboration. Through an administrative interface, shown in **Figure A.1**, a scenario designer can create an information security scenario for one or more players. To allow for many scenarios, the game board, which players use for reference, is a simple image. The scenario designer places *positions* on this image, which represent organizational assets on which players will place controls. For each position, the designer chooses possible security controls (e.g., firewall, intrusion detection, training, etc.) that the players can choose to purchase during the game. The designer also chooses the number of players, their names or roles, starting instructions for each player, the number of turns, and the amount of initial resources for the group and other features (see Table 1 for customizable features). For research purposes, additional manipulations may take place outside of the game itself, such as group member familiarity and proximity.

Table 1. CollabSec Customizable Features

Number of Players	Number of Turns
Starting Resource Levels	Number and Type of Assets
Number and Type of Controls	Number, Type and Likelihood of Attacks
Number and Type of Outcomes or Goals	Player Roles
Player instructions	End of Turn Feedback

Finally, the designer will create a set of probability-based rules that determine what happens after each round. A rule has several components: an attack, an asset, a control, outcomes, and two probabilities (See Appendix B for rule template). A repository of these rules and components (defined below) is currently under development based on previous works and industry materials (Kouns and Minoli 2010; Microsoft 2006; Richardson 2011; Stoneburner et al. 2002; Uiterwijk, 1999).

Attack. The attack specifies the name of the attack and the plain language description displayed to players when a successful attack occurs. There may be many rules for a single attack since the same attack may happen on multiple assets or may be controlled by multiple controls. There would be no rule for illogical asset-attack combinations such as a social engineering attack on a router.

Asset. The assets are the potential targets of the attacks. There will be assets representing people, data, information systems, hardware, and network components.

Control. In each rule, the control specifies what control must be in place on the specified asset for vulnerability to be mitigated and an attack to be thwarted. Players may choose different quality levels (e.g., high or low) for some controls.

Outcomes. The outcomes are the impacts to the system and various aspects of the organization if an attack is not stopped by the control. There may be multiple outcomes. The outcomes may be related to player roles in such a way that players either compete or cooperate. Each outcome is represented by a score, when a successful attack occurs, the score is decremented by the outcome.

Probabilities. There are two probabilities associated with the rule: the probability of the attack being successful given that the appropriate control *is not* in place, and the probability of the attack being successful given that the control *is* in place (i.e. residual risk). For each rule, the game will determine if the rule applies to any of the current assets, and if the appropriate control is in place. The rules then The probabilities are then used to determine if the attack is successful, and scores for the outcomes will be adjusted accordingly.

Playing the game

Currently, **Figure A.2** depicts CollabSec configured as a three-person game although multiple configurations are possible. The players include a *security manager*, an *operations manager*, and an *accountant*. Each of these players is given instructions specific to his or her assigned role. The accountant is instructed to minimize the financial impact of the purchase of controls and any successful attacks, while the operations manager must minimize the impact of controls and attacks on business operations. The security manager, on the other hand, must maintain the security of the system by maximizing controls given the allotted resources.

After logging in, the players are presented with the board and a chat window as shown in **Figure A.2**. For each of the positions on the board, representing assets, players must collaboratively decide which controls to place on which positions. Each control they place uses part of a finite set of resources, restricting the number and quality of controls that can be used. Once finished with their choices, they submit their choices and the game, using the rules described above, evaluates their decisions and gives feedback based on which attacks were successful. The players may use this feedback in successive turns of the game in order to meet the objective as outlined by a particular scenario. For example, in the scenario described above, the objective of the security manager is to minimize risk to an acceptable level while maximizing the protection to the assets at the least cost. The rules provide the descriptions that comprise the feedback. An example feedback might say the following:

> "Using social engineering an attacker successfully convinced your helpdesk agent to reset a password. The attacker was then able to obtain credit card numbers for 500 customers. You lose X financial points for the money required to send notices to those customers, provide them with fraud protection and reimburse the credit card company for the replacement of cards. You lose Y security points your company's security posture has been seriously

> degraded. You lose Z operations points because until you install new controls you have to issue your customers telephone passwords they will use when calling the helpdesk and your customer service times skyrocket."

The players then see the board for a second turn in which they can make changes based on the feedback. This cycle continues for as many turns as specified in the game scenario.

FUTURE DIRECTIONS AND PLANNED RESEARCH

CollabSec can be used in a variety of Information Systems and Information Assurance courses. It will also be appropriate for use for training employees in a corporate environment. However, CollabSec is expected to provide more than educational value; it is also planned to be used as a tool for conducting research on a range of different topics. One potential research question involves transactive memory and security planning. When individuals interact in groups and work toward a common goal, they likely draw upon transactive memory resources, which refers to the domain-specific knowledge allocated across members of a group and a shared awareness of who knows what (Wegner 1986). The group benefits from transactive memory when members' knowledge sets are complementary, able to be retrieved, and communicated in a fashion that is relatable to other group members. The end result is that group members are able to supplement their own limited memories and experiences with external information provided by (presumably) trusted others. The use of transactive memory resources would seem to be beneficial within the context of security planning and implementation. For instance, it is unlikely that a single manager will be knowledgeable about all potential security threats, so carrying out risk assessment activities should be undertaken with a team of security professionals and end users with complementary knowledge bases (Straub and Welke 1998). We intend to investigate this possibility.

Similarly, we intend to compare performance across group environments, particularly between collocated and dispersed groups. Any process gains and process losses due to the communicative environment could have undue influence on group collaboration, especially when the group is faced with a resource allocation task (Qureshi and Vogel 2001). Like most other business functions, information security planning is increasingly being coordinated across computer-mediated means, so CollabSec provides an opportunity to test existing computer-mediated communication and group collaboration theories within the InfoSec context.

REFERENCES

Irvine, C., Thompson, M., and Allen, K. "CyberCIEGE: Gaming for Information Assurance," *IEEE Security & Privacy* (3:3) 2005, pp. 61-64.

Knapp, K.J., Marshall, T., Rainer, K., and Ford, F. "Managerial Dimensions in Information Security: A Theoretical Model of Organizational Effectiveness," Report for (ISC)^2 Inc., 2005.

Kouns, J., and Minoli, D. *Information Technology Risk Management in Enterprise Environments*, Wiley, Hoboken, NJ, 2010.

Microsoft "The Security Risk Management Guide", 2006.

Puhakainen, P., and Siponen, M. "Improving Employees' Compliance through Information Systems Security Training: An Action Research Study," *MIS Quarterly* (34:4) 2010, pp. 757-778.

Qureshi, S., and Vogel, D. "Adaptiveness in Virtual Teams: Organizational Challenges and Research Directions," *Group Decision and Negotiation* (10:1) 2001, pp. 27-46.

Richardson, R. "2010/2011 Computer Crime and Security Survey" Computer Security Institute, 2011.

Stoneburner, G., Goguen, A. and Feringa, A. " NIST Special Publication 800-30: Risk Management Guide for Information Technology Systems," National Institute of Standards and Technology, 2002.

Straub, D.W., and Welke, R.J. "Coping with Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly* (22:4) 1998, pp. 441-469.

Surdu, J.R., Hill, J., Dodge, R., Lathrop, S., and Carver, C. "Military Academy Attack/Defense Network Simulation," Advanced Simulation Technology Conference Symposium on Military, Government, and Aerospace, Orlando, FL, 2003, pp. 57-63.

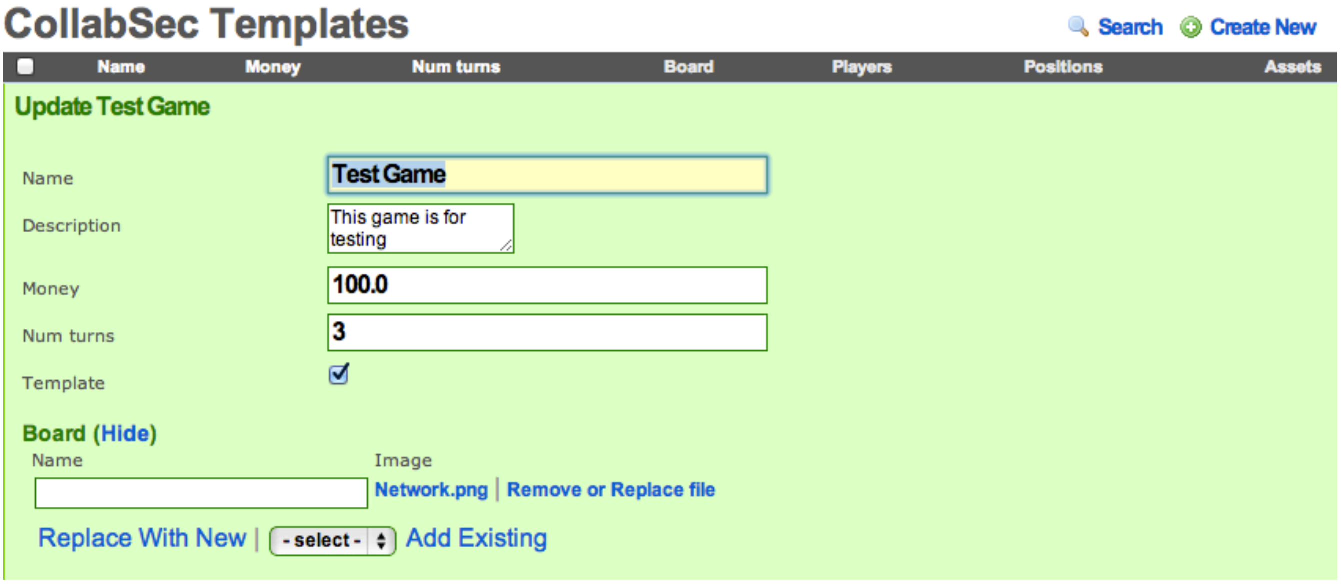
Twitchell, D.P, Wiers, K., Adkins, M., Burgoon, J.K and Nunamaker, J.F. "StrikeCOM: A multi-player online strategy game for researching and teaching group dynamics," Thirty-Eigth Hawaii International Conference on System Sciences, 2005

Uiterwijk, A. "Security Game: Playing for Keeps," *Federal Computer Week,* 1999.

Wegner, D.M. "Transactive Memory: A Contemporary Analysis of the Group Mind," in: *Theories of Group Behavior,* B. Mullen and G.R. Goethals (eds.), Springer, New York, NY, 1986, pp. 185-208.

Werlinger, R., Hawkey, K., Botta, D., and Beznosov, K. "Security Practitioners in Context: Their Activities and Interactions with Other Stakeholders within Organizations," *International Journal of Human-Computer Studies* (67:7) 2009, pp. 584-606.

APPENDIX A - CollabSec SCREENSHOTS



CollabSec Templates

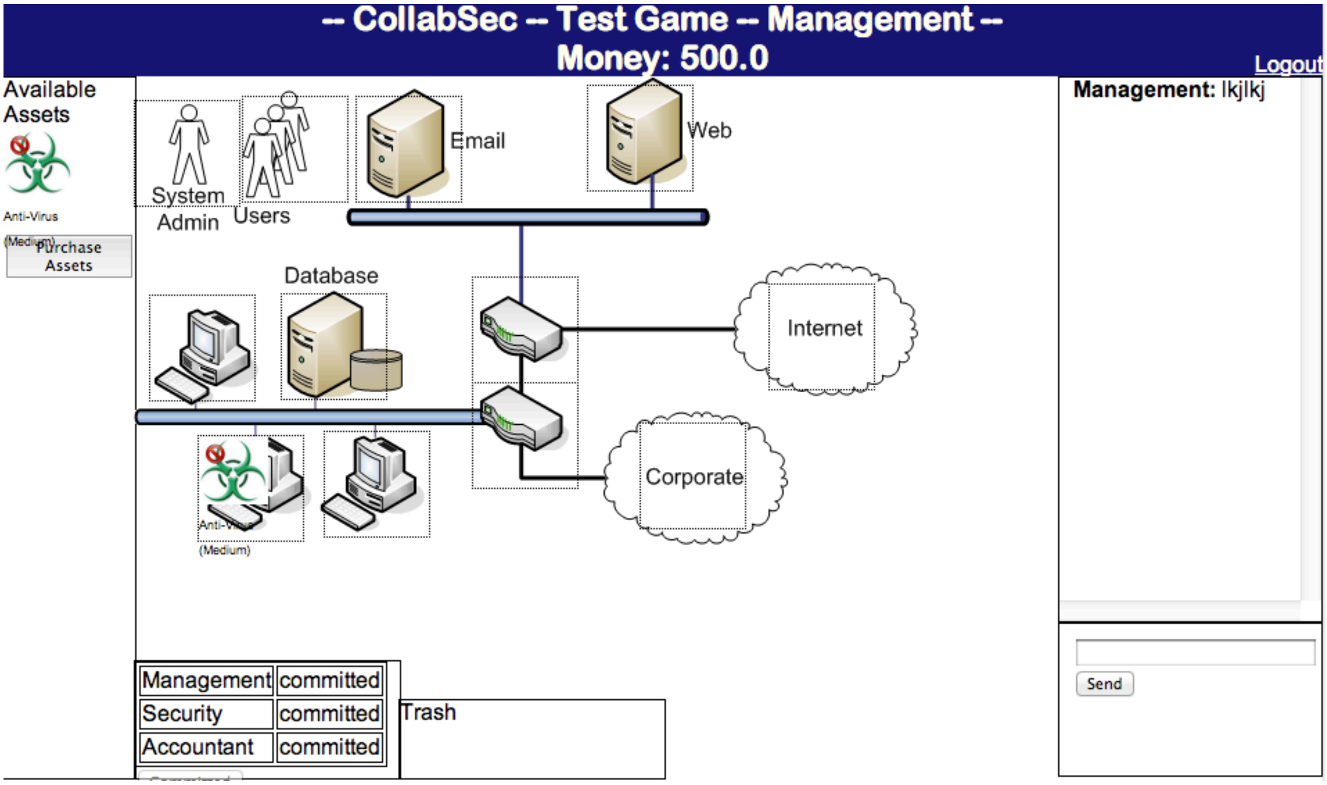
Update Test Game

Name	Test Game
Description	This game is for testing
Money	100.0
Num turns	3
Template	☑

Board (Hide)

Name	Image
	Network.png | Remove or Replace file

Figure A.1: CollabSec administration interface



-- CollabSec -- Test Game -- Management --
Money: 500.0

Management: lkjlkj

Management	committed
Security	committed
Accountant	committed

Figure A.2: CollabSec Game Board/User Interface

APPENDIX B – RULE TEMPLATE

Table B.1. Sample Rule Set.

Attack	**Asset**	**Control**	**Outcomes***			**Probabilities****	
			sec	**op**	**fin**	**control**	**no**
Social engineering	Users	Training – medium	10	3	10	.3	.7
SQL Injection	DB	Code review	10	5	10	.1	.9

*sec: security outcome; op: operation outcome; fin: financial outcome

**control: probability of successful attack given control; no: probability of successful attack given no control. The sum of control probability and no probability is 1.0.