EFFECTIVENESS OF USING CARD GAMES TO TEACH THREAT MODELING FOR SECURE WEB APPLICATION DEVELOPMENTS

Mark Thompson, University of North Texas, mark.thompson2@unt.edu
Hassan Takabi, University of North Texas, takabi@unt.edu

ABSTRACT

Gamification of classroom assignments and online tools has grown significantly in recent years. There have been a number of card games designed for teaching various cybersecurity concepts. However, effectiveness of these card games is unknown for the most part and there is no study on evaluating their effectiveness. In this paper, we evaluate effectiveness of one such game, namely the OWASP Cornucopia card game which is designed to assist software development teams identify security requirements in Agile, conventional and formal development processes. We performed an experiment where sections of graduate students and undergraduate students in a security related course at our university were split into two groups, one of which played the Cornucopia card game, and one of which did not. Quizzes were administered both before and after the activity, and a survey was taken to measure student attitudes toward the exercise. The results show that while students found the activity useful and would like to see this activity and more similar exercises integrated into the classroom, the game was not easy to understand. We need to spend enough time to familiarize the students with the game and prepare them for the exercises using the game to get the best results.

Keywords: Cybersecurity, Gamification, Threat Modeling, Web Application, and Card games

INTRODUCTION

Gamification is a significant and emerging topic in pedagogical research. In the last three decades, learning games have stormed the world. Games of all kinds, from digital to face-to-face, have become an alternative means of delivering academic content. Through games, teaching and learning take new forms and engage students in subject areas to which they may traditionally be resistant. They can be fun and entertaining, improve leaner engagement with content, and may allow students to explore ideas and ask questions.

Educational games have been used to teach a variety of topics beyond computer science or computer security, such as mathematical fractions (Popović et al., 2013) or algebra (Dragonbox, 2016). Educational research communities have explored using of games in various aspects of computer science education such as using game for programming assignments (Seaborn et al., 2012), teaching specific topics such as computer ethics (Brinkman, 2009), and adapting to skill level (Andersen, 2012).

In the context of cybersecurity, both serious games including full simulation and partial simulation, informal games have been used to raise awareness and teach cybersecurity concepts. *Gondree et al.* give an overview of the benefits of using casual games to impart modest security information (Gondree et al., 2013). They reference *Klopfer et al.*'s five freedoms essential to play, namely the freedom to experiment, the freedom to fail, the freedom to fashion identities, the freedom of interpretation, and the freedom of autonomous effort, and reinterpret them as mapping to various aspects of computer security (Klopfer et al., 2009). They argue that tabletop games including card and board games have a few advantages over their digital counterparts: they are accessible, social, unobtrusive, modest, and modifiable (Gondree et al., 2013).

While there have been some examples of informal games in cybersecurity awareness (Denning et al., 2013; Gondree & Peterson, 2013; Olano et al., 2014), for the most part using informal games in security has been relatively unexplored. Furthermore, the assessment of informal games appears to be complicated. The questions remain as to how they translate into real-world knowledge and skills, how they affect lesson retention, etc.

In this paper, we aim to evaluate effectiveness of one such game, namely the OWASP Cornucopia card game (OWASP Cornucopia, 2016). OWASP Cornucopia is a card game designed to assist software development teams identify security requirements in Agile, conventional and formal development processes. It is language, platform and technology agnostic. Cornucopia Ecommerce Website Edition (OWASP Cornucopia Ecommerce, 2016) is based on the concepts and game ideas in EoP, but those have been modified to be more relevant to the types of issues ecommerce website developers encounter. It attempts to introduce threat modeling ideas into development teams that use Agile methodologies, or are more focused on web application weaknesses than other types of software vulnerabilities.

The rest of this paper is organized as follows. Section 2 discusses the related work. In Section 3, we describe the experiment methodology followed by experimental results in Section 4. Finally, Section 5 concludes the paper.

RELATED WORK

Many games have been used for raising security awareness and teaching cybersecurity concepts. Examples of digital games include the *Anti-Phishing Phil* (Sheng et al., 2007), *CyberCiege* (Irvine at al., 2005), *CyberProtect* (CyberProtect, 2016) and *MAADNET* (Hill et al., 2003). There are also a variety of simulation based cybersecurity games such as Capture-the-Flag competitions (e.g., (DEF CON CTF (Dark Tangent, 2016); PlaidCTF (PlaidCTF, 2013), NSA's *Cyber Defense Exercise* (CDX) (Cyber Defense Exercise, 2016), and the Collegiate Cyber Defense Competition (CCDC, 2016) which try to simulate real world attack and defense mechanisms and engage players in a competitive environment. Examples of non-digital games are *Protection Poker* (Williams et al., 2010), *Elevation of Privilege* (Shostack, 2012), and *OWASP Snakes and Ladders* (OWASP Snakes and Ladders, 2016), and VOME's privacy game (Privacy Game, 2012).

Protection Poker, is an agile development game designed to elicit accurate estimates of the cost of developing software features. It is intended to structure discussion about security risks. A customer representative explains each requirement followed by a discussion of threats, each of which is assessed on the basis of ease and asset value. Ease and asset values are then combined into an assessment of security risk. *Elevation of Privilege* is a game designed to draw people who are not security practitioners into threat modeling (Shostack, 2012). The game uses a variety of techniques to do so in an enticing, supportive and non-threatening way. It was inspired by Protection Poker and its cards are ordered more like a traditional card deck, and the rules provide a very different structure for play. EoP is designed for 3-5 players and consists of 84 cards. The cards are in six suits: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. Each suit consists of cards numbered much like normal playing cards, 2-10, Jack, Queen, King, and Ace. Each playing card shows a suit, a number, and a threat of the type exemplified by the suit. These threats, or hints, help non-security-experts find problems.

OWASP Snakes and Ladders is an educational game that promotes awareness of application security controls and risks, and in particular knowledge of other OWASP documents and tools (OWASP Snakes and Ladders, 2016). "This board game was created to use as an ice-breaker in application security training, but it potentially has wider appeal simply as a promotional hand-out, and maybe also more usefully as learning materials for younger coders." (OWASP Snakes and Ladders, 2016). The game is quite lightweight, and has two editions for Web Applications and Mobile Apps. In the web applications edition, the virtuous behaviors (ladders) are secure coding practices and the vices (snakes) are application security risks whereas the mobile apps edition uses mobile controls as the virtuous behaviors and mobile risks as the vices (OWASP Snakes and Ladders, 2016).

The *VOME's privacy game* is developed to help people who are designing new products and services to understand privacy issues and make better decisions about architecture (Privacy Game, 2012). Players work to build a database of personal information and make decisions about what information characters might reveal to others and what they keep to themselves. In doing so, they explore the tensions between public and private, and have to make active decisions as well as negotiate with other players. For each character personal information is a valuable commodity. The game is designed to highlight the differing values of personal information as players work their way through a number of scenarios. The online version of the game is designed for 3-5 players who can assume various identities: hacker, bank manager, advertiser, health service worker, employer and community reporter (Privacy Game, 2012).

As they play the game, the characters are invited to reveal social, digital, financial, biographical, security and health information. The way to win is to keep the most valuable information to themselves while trying to find out what information others have.

The Fantasy Flight Games' *Android: Netrunner*, published in 2012, is a commercial tabletop card game that deals with cybersecurity (Netrunner, 2012). It is two-player game set in a dystopian, cyberpunk future where monolithic megacorps own and control the vast majority of human interests. While corporation players try to score points by advancing their agendas, they have to guard their intellectual properties from the elite and subversive hackers known as netrunners. A digital version of the parlor game *Werewolf* has been used to explore information flow policy in class (Ensafi et al., 2012). *Werewolves* is an online version of the game Werewolves of Miller's Hollow that was developed to help teach information flow. The game pits werewolves against townspeople in a shared Linux system, where students must use the command line environment to find information flow leaks in the form of side channels that reveal the werewolves' identities. Werewolves has many desirable traits, such as the ability to make learning about information flow fun and the fact that the kinds of attacks students can carry out to gain an advantage in the game are open ended, which leads to self-guided learning" (Ensafi et al., 2012).

There are also some games used for cybersecurity awareness such as the *Control-Alt-Hack* game (Denning et al., 2013) and the *[d0x3d!]* game (Gondree & Peterson, 2013). The former is a card game based on Steve Jackson's *Ninja Burger,* but designed for the context of a security consulting firm. It is designed to expose the player to a variety of cybersecurity terminology, applications, and careers. The latter is a board game designed to casually introduce the players to some of the terminology and adversarial thinking related to network security. Another card game is the *Exploit!* that was primarily designed for entertainment of the security audience, not education (Core Impact. Exploit, 2013). SecurityEmpire is a multiplayer computer game to teach cybersecurity concepts to high school students (Olano et al., 2014). It challenges the users to build a green energy company while engaging in sound information assurance practices such as not clicking on unsafe links, encrypting auction bids, authenticating software downloads, performing integrity checks of system software, keeping antivirus protection up-to-date, and choosing strong passwords.

RESEARCH METHODOLOGY

In the actual game scenario, before the OWASP Cornucopia card game commences, an application or application process that needs to be reviewed from a security requirements perspective is identified. This may be a concept, design, or an actual implementation. Once identified, a data flow diagram is created to provide a visual overview of the system in question. Then, anywhere from three to six key business stakeholders from a group of architects, developers, testers, and support personnel, are invited to take part in the card game, where at least one person should be somewhat familiar with application security. The end goal of the OWASP Cornucopia card game, and in particular, the Ecommerce Website Edition, is to provide a medium by which to help these stakeholders identify security requirements from the OWASP Secure Coding Practices – Quick Reference Guide. In fact, the Cornucopia suits are based on the on this reference guide, with additional consideration from the OWASP Application Security Verification Standard, the OWASP Testing Guide, and Principles of Secure Development by David Rook [OCEW]. Similar to poker-playing cards, the six Cornucopia suits, or areas of security focus, include data validation and encoding, authentication, session management, authorization, cryptography, and cornucopia, which serves as a trump suit and includes areas not specifically targeted in the prior suits. Each card has a suit and value, attack description, and cross-references to help create the security requirements.

Now before the game is started, the Jokers and a few of the low-score cards from the Cornucopia suit are removed to ensure that each player will have the same number of cards. Then, the cards are shuffled and all the cards are dealt. A player will be chosen at random to play the first card, which cannot be initially from the Cornucopia suit, by reading the card aloud and explain how the threat could or could not apply to the application or application process. Players may earn points in two ways: (1) the group concurs that the threat is an actionable bug to their system, and (2) the highest card of the same suit of all the cards played, or if Cornucopia cards are played, the highest card from the Cornucopia suit. The attack would be documented so that security requirements specific to this application or application process can be identified and addressed. This process would continue in a clockwise fashion until all the cards are played.

For our purposes, the focus of the study was to answer simple questions - what is the impact on student learning of using the OWASP Cornucopia card game, and do students enjoy the process and view it as a worthwhile exercise.

In order to do this, we designed an experiment for a security related course that is taught at both undergraduate and graduate levels at our university. The students, both graduate and undergraduate, were tasked with reading the OWASP Ten Most Critical Web Application Security Risks (1) and the OWASP Secure Coding Practices Quick Reference Guide (2). One week after the readings were assigned, and just prior to the exercise, all students were given a multiple choice 16 question quiz over related security topics. All students were then given an e-commerce case study to read, along with copies of the OWASP Top 10 and the OWASP Secure Coding Practices Quick Reference as guides.

Students (both graduate and undergraduate) were randomly divided into a group that played the OWASP Cornucopia card game (hereafter the Cornucopia group) and a group that simply discussed the case study among themselves without playing the card game. The randomness was chosen in an effort to simulate members of different groups (i.e., architects, developers, testers, and support personnel) coming together to work on a common problem, that is, our given case study. Both groups were asked to elicit a requirements list for the case study either using the card game or the discussion group. Both groups were given the same amount of time for their respective activity. One week after either playing the game or discussing the topic, all students were given the same 16 question quiz with questions and answers in a different order. Both groups also were surveyed using a common form to elicit their reactions to the exercise. On the survey, questions were asked to rate statements such as “The exercise was worthwhile”, rather than “the card game was worthwhile” to allow for a common survey. It is worth to note that majority of undergraduate students enrolled in this course are senior students. We performed the experiments in two consecutive years, 2015 and 2016, in the same course. Most of the experiment procedure were kept the same. The only difference was that in second year we allowed more time to complete the experiment: two class sessions instead of one session of class we used in 2015, since many students during the first year indicated that it took a significant amount of startup time to properly comprehend the task and therefore not enough time was given to sufficiently explore the activity. In the graduate course during the second year, groups were also organized according to the group projects, i.e., e-commerce web sites, which were being developed as the final project in the class to see if a common focus (i.e., their group project) would somehow improve each group’s effectiveness in the activity.

Cornucopia Group

The group of students participating in the Cornucopia game was 33 in number and consisted of graduate and undergraduate students (in separate teams of 4-6).

Discussion Group

The second group did not play the game, but rather discussed the case study and proceeded to write down appropriate requirements, using the OWASP Quick Reference as a guide. This group consisted of 34 undergraduate and graduate students, also in groups of 4-6. Graduate students and undergrads were not on the same teams.

RESULTS

In this section, we describe the results of the experiment which consists of the quiz results and survey results.

Pre-exercise and Post-exercise Quiz Results

Students were given a strict 10-minute time limit for the pre and post quizzes, and told that the quiz was not a factor in their course grade. The quiz covered material across many different areas from the OWASP Top 10 and related security topics (ref. to Appendix A). In particular, some questions originated from the OWASP Top 10 Threats and Mitigations Exam – Multiple Select (OWASP Top 10 Threats, 2016), with some modifications so that only one correct answer was present for each question. Since the quiz and OWASP readings covered some material that was covered only lightly in class, relative performance on the quizzes before and after the exercise is the important metric.

In the first year, the average quiz scores of the Cornucopia group increased from 8.53 in pre-exercise to 8.65 post-exercise and the average quiz scores of the discussion group increased from 9.73 in pre-exercise to 9.87 post-exercise. In the second year, the average quiz scores of the Cornucopia group increased from 9.25 in pre-exercise to 9.31 post-exercise and the average quiz scores of the discussion group increased from 9.16 in pre-exercise to 9.37 post-exercise. As we can see there were slight improvements in post-exercise quiz scores over pre-exercise quiz scores. If we look at the individual quiz questions, however, there are some interesting observations.

For example, for the questions 3 (Which attack can execute in the user's browser and is capable of hijacking user sessions, defacing websites or redirecting the user to malicious sites), 5 (An attack technique that forces a user's session credential or session ID to an explicit value), 11 (Which of the following can result in insecure cryptography), and 15 (Pick the one that is not a security misconfiguration), we observed increase in average scores in both the Cornucopia group and the discussion group.

For example, for the question 4 (What flaws can lead to exposure of resources or functionality to unintended actors) and the question 10 (Which of the following vulnerabilities are most likely to occur due to an insecure direct object reference attack), we observed 19% increase in average scores in the Cornucopia group while the average score remained the same in the discussion group.

For the question 7 (Network permissions should be established so that users can accomplish their tasks, but cannot access any system resources that are not necessary so that …), we observed 19% increase in average score in the Cornucopia group while there was 5% decrease in average scores in the discussion group. For the question 9 (Which of the following languages is the primary target of cross-site scripting), we observed 6% increase in average score in the Cornucopia group while there was 10% decrease in average scores in the discussion group. For the question 13 (Which of the following vulnerabilities are most likely to occur due to an insecure direct object reference attack), we observed 12% increase in the Cornucopia group while there was 10% decrease in average score in the discussion group.

There was only one question, the question 14, where average score remained the same for the Cornucopia group while there was 31% increase in average score in the discussion group.

These results show that the card game was effective in teaching students the OWASP security requirements and identifying them as shown by improvement for many questions in the pre-exercise and post-exercise quiz for the Cornucopia group. However, in order to be more effective, we need to spend more time than one or two class sessions to prepare students for the activity, familiarize them with the card game, and include more real world scenarios in the exercise.

Survey Responses

A common survey administered to all student participants asked for rating agreement with statements about the exercise on a scale of 1 (most disagreement) to 10 (most agreement).

The survey was as follows:

1. I enjoyed this activity
2. I learned something from this activity
3. The activity was worthwhile
4. The activity was easy to understand
5. I learned more from interacting with my group than I would have on my own
6. This activity should be a part of this class in the future
7. I felt like I was getting practice for real-world scenarios
8. I felt my group identified key security requirements for this activity
9. I have a better understanding of the OWASP Top 10 now

10. I would like to see more exercises like this in the class

Survey respondents were also asked to list any suggestions for improvement and anything they liked or didn't like about the exercise. During the exercise, the general feeling regarding this activity was that those who were in a discussion group would have rather been in a Cornucopia group playing the game.

The results of the survey are shown in Figure 1.

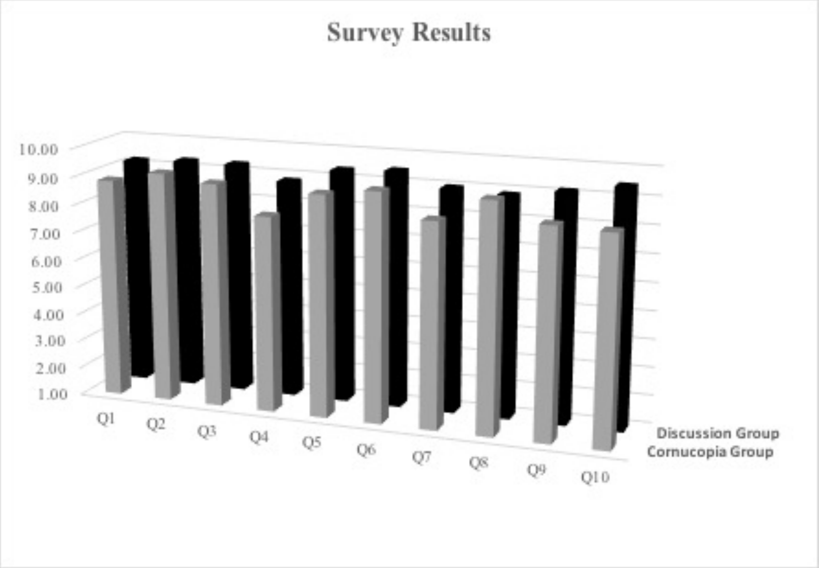

Figure 1. Survey Results

One thing that was pretty obvious in the survey was that both groups did not feel the activity; both the Cornucopia and discussion groups stated that the activity was not easy to understand (question 4 of the survey had the lowest ranking in both groups). All groups were observed to be very slow to get started with the activity, and adding to this, the Cornucopia group took even longer as there was an added component of the game to understand. Additionally, students had questions about understanding the threats and vulnerabilities listed in the game. This was also apparent from students' comment where they noted that the activity was "time consuming" and "better introduction about the activity in advance".

As we can see in Figure 1, for majority of the questions the discussion group has higher ratings compared to the Cornucopia group. We believe the main reason for this is the short period of time the activity was conducted in. Since the time was limited, the participants weren't able to get a feel of the game and how to play it; this is also shown in students' comment where they stated that "If this activity was conducted in lab, we might have more time to understand and go with the game. Half of one class, we took to understand the game." And "provide a presentation to explain how the game should be played rather than relying on handout …". Another important reason we believe is cultural factors as majority of graduate students were international students and not familiar with card games in general; this made it more difficult for them to get a grasp of the game in the short amount of time they had.

Although students felt the activity tended to be more difficult, both groups indicated that this activity should be part of the class, ranking question 6 as the highest or second highest of the survey questions. Similarly, question 10 (I would like to see more exercises like this in the class) scored very well for both groups.

An interesting observation was the question 8 of the survey (I felt my group identified key security requirements for this activity) which was rated higher by the Cornucopia group compared to the discussion group. This shows that the exercise was effective in improving the students' ability to identify security requirements which was the main goal of the activity. To make it more effective, however, we need to make some changes to the exercise as it was also stated by students' where they noted that "more discussion about the real-world scenarios" and "In-depth examples of attacks" should be included in the activity.

SUMMARY

Although a number of informal games in cybersecurity education exist, using informal games has been relatively unexplored in cybersecurity. Furthermore, there is no assessment of effectiveness of these games. In this paper, we performed an experiment to evaluate effectiveness of one such game, namely the OWASP Cornucopia card game. Both undergraduate and graduate students enrolled in for a security related course at our university participated in the experiment where they were randomly divided into a group that played the OWASP Cornucopia card game and a group that did not. They were given an e-commerce case study and were asked to elicit a requirements list for the case study. Their knowledge was tested using pre-exercise and post-exercise quizzes and a survey was performed to elicit their reactions to the exercise. The results show that the card game is effective in improving students' skills in identifying security requirements but the classroom activities need to prepared in advance and enough time should be assigned to the exercises in the classroom to achieve goals of using card games in teaching cybersecurity concepts. For future work, we plan to perform the experiment with larger groups in a longer time period and examine how the results might change if we remove limitations of this study.

REFERENCES

Andersen, E. (2012). Optimizing Adaptivity in Educational Games. *Foundations of Digital Games*. Retrieved from http://homes.cs.washington.edu/~eland/papers/Andersen_Doctoral_Consortium.pdf

Brinkman, B. (2009). The Heart of a Whistle-blower: A Corporate Decision-Making Game for Computer Ethics Classes. In *SIGCSE Technical Symposium*. Chattanooga, TN: ACM.

Core Impact. Exploit! (n.d.). *2013*. Retrieved from http://www.coresecurity.com

CyberProtect. (n.d.). *US Department of Defense Web Page,*. Retrieved from http://iase.disa.mil/eta/cyber-protect/launchpage.htm

Denning, T., Lerner, A., Shostack, A., & Kohno, T. (2013). Control-Alt-Hack: The Design and Evaluation of a Card Game for Computer Security Awareness and Education. In *CM SIGSAC Conference on Computer & Communications Security* (pp. 915–928). Berlin, Germany: ACM.

Ensafi, R., Jacobi, M., & Crandall, J. R. (2012). Students Who Don't Understand Information Flow Should be Eaten: An Experience Paper. In *USENIX conference on Cyber Security Experimentation and Test*. Bellvue, Washington.

Fantasy Flight Games, *Android: Netrunner* Retrieved from http://www.fantasyflightgames.com

Gondree, M., & Peterson, Z. (2013). Valuing Security by Getting [d0x3d!] Experiences with a network security board game. In *Proceedings of the USENIX 6th Workshop on Cyber Security Experimentation and Test*. Washington, D.C.: USENIX.

M. Gondree, Z. N.J. Peterson, and T. Denning. Security through Play. IEEE Security & Privacy, 11(3), 2013.

Hill, J., Surdu, J., Lathrop, S., Conti, G., & Carver, C. (2003). MAADNET: Toward a Web-Distributed Tool for Teaching Networks and Information Assurance. In D. Lassner & C. McNaught (Eds.), *World Conference on Educational Multimedia, Hypermedia and Telecommunications*. Chesapeake, VA: AACE.

Irvine, C., Thompson, M., & Allen, K. (2005). Active Learning with the CyberCIEGE Video Game. In *Federal Information Systems Security Educators' Association Conference*, pp. 1–10. North Bethesda, MD.

E. Klopfer, S. Osterweil, and K. Salen, Moving Learning Games Forward: Obstacles, Opportunities, and Openness, The Education Arcade, 2009.

National Collegiate Cyber Defense Competition. (2013). Retrieved from http://www.nationalccdc.org

Marc Olano, Alan T. Sherman, Linda Oliva, Ryan Cox, Deborah Firestone, Oliver Kubik, Milind Patil, John Seymour, Isaac S. Kohane, Donna Thomas: SecurityEmpire: Development and Evaluation of a Digital Game to Promote Cybersecurity Education. 3GSE 2014

OWASP Cornucopia Ecommerce Website Edition, https://www.owasp.org/images/7/71/Owasp-cornucopia-ecommerce_website.pdf

OWASP Cornucopia, https://www.owasp.org/index.php/OWASP_Cornucopia

OWASP Snakes and Ladders, https://www.owasp.org/index.php/OWASP_Snakes_and_Ladders

OWASP Top 10 Threats and Mitigations Exam – Multiple Select, https://www.owasp.org/index.php/OWASP_Top_10_Threats_and_Mitigations_Exam_-_Multiple_Select

PlaidCTF. (2013). Retrieved from http://www.plaidctf.com

Popović, Z., Cooper, S., Burns, M., Abell, O., & Smith, A. (2013). Center for Game Science: Refraction. *Center for Game Studies @ University of Washington*. Retrieved from http://centerforgamescience.org/portfolio/refraction/

Privacy Game, The Visualisation and Other Methods of Expression (VOME project), Retrieved from http://www.vome.org.uk/privacy-game/

K. Seaborn, M. S. El-Nasr, D. Milam, and D. Y. (2012). Programming, PWNed: Using Digital Game Development to Enhance Learners' Competency and Self-Efficacy in a High School Computing Science Course. In *SIGCSE Technical Symposium*.

S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L.F. Cranor, J.Hong, and E. N. (2007). Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish. In *Symposium on Usable Privacy and Security (SOUPS)*.

Shostack, A. (n.d.). "Elevation of Privilege: Drawing Developers into Threat Modeling", Microsoft Technical Paper, pp. 1–15. Redmond, Washington, Retrieved from http://www.microsoft.com/security/sdl/adopt/eop

The Dark Tangent. (n.d.). DEF CON Hacking Conference: Capture the Flag. *Def Con Web Site*. Retrieved from http://www.defcon.org/html/links/dc-ctf.html

The Cyber Defense Exercise (CDX), https://www.iad.gov/iad/programs/cyber-defense-exercise/index.cfm

WeWantToKnow. (2013). DragonBox. Retrieved from http://www.dragonboxapp.com/

Williams, L., Meneely, A., and Shipley, G., "Protection Poker: The New Software Security Game", *IEEE Security & Privacy*, *8*(3), 2010.

APPENDIX A

QUIZ QUESTIONS

1. What is the attack technique used to exploit web sites by altering backend database queries through inputting manipulated queries?
   a. SQL Injection
   b. LDAP Injection
   c. XML Injection
   d. OS Commanding
2. What flaw arises from session tokens having poor randomness across a range of values?
   a. Insecure Direct Object References
   b. Session Hijacking
   c. Session Replay
   d. Session Fixation
3. Which attack can execute scripts in the user's browser and is capable of hijacking user sessions, defacing websites or redirecting the user to malicious sites.
   a. SQL Injection
   b. Malware Uploading
   c. Man in the middle
   d. Cross site scripting
4. What flaw can lead to exposure of resources or functionality to unintended actors?
   a. Session Fixation
   b. Insecure Cryptographic Storage
   c. Improper Authentication
   d. Unvalidated Redirects and Forwards
5. An attack technique that forces a user's session credential or session ID to an explicit value.
   a. Brute Force Attack
   b. Session Fixation
   c. Session Hijacking
   d. Dictionary Attack
6. What is the type of flaw that occurs when untrusted user entered data is sent to the interpreter as part of a query or command?
   a. Injection
   b. Insecure Direct Object References
   c. Cross Site Request Forgery
   d. Insufficient Transport Layer Protection
7. Network permissions should be established so that users can accomplish their tasks, but cannot access any syste m resources that are not necessary so that
   a. A hacker cannot steal a legitimate user's identity
   b. Users will not have access to and misuse system resources
   c. Hackers will not pose as legitimate users
   d. Only the resources authorized for that user will be at risk
8. Role-Based Access control helps prevent this OWASP top 10 weakness
   a. Unvalidated Redirect or Forward
   b. Failure to restrict URL Access
   c. Security Misconfiguration
   d. Insufficient Transport Layer Protection
9. Which of the following languages is the primary target of cross-site scripting?
   a. JSON
   b. SQL
   c. JavaScript

    d. XML

10. Which of the following vulnerabilities are most likely to occur due to an insecure direct object reference attack?
    a. Executing commands on the server
    b. Modifying data without authorization
    c. Impersonating any user on the system
    d. Modifying SQL data pointed to by the query
11. Which of the following can result in insecure cryptography?
    a. Unused services
    b. Default accounts
    c. Unsalted hash
    d. Unnecessary/unused services or features
12. Which of the following protocols is a network layer encryption protocol?
    a. EFS
    b. http
    c. Kerberos
    d. SSL
13. An IP Address is the Internet equivalent of:
    a. Your Birth Date
    b. Your modem configuration number
    c. Your mailing address
    d. Your social security number
14. http://www.example.com/redirect.jsp?url=evil.com is an example of:
    a. an unvalidated redirect
    b. insecure direct object reference
    c. sensitive data exposure
    d. SQL injection
15. Pick the one that is not a security misconfiguration
    a. Out of date software
    b. Server audits
    c. Having unnecessary features or privileges installed
    d. Error messages that may reveal information to attackers
16. The use of proper security techniques can
    a. Promote cross-site scripting
    b. Provide function level access control
    c. Allow access to unauthorized users
    d. Enable the effective use of rainbow tables