Overview of Learning Cybersecurity Through Game Based Systems

Tolulope Awojana and Te-Shun Chou
Department of Technology Systems
College of Engineering and Technology
East Carolina University

Abstract

Cybersecurity awareness and skills training are very essential and challenging. Cybersecurity in itself involves the defense of systems, networks and programs from digital attacks. These attacks are capable of gaining unauthorized access to computers and networks. Game based learning allows students have fun whilst learning by actively learning and practicing the right ways things should be done. Often, the game is started on a slow pace gradually advancing gain in skill until the student is able to successfully navigate the difficult levels. There is a constant increase in cyberattacks all over the world, an estimate of $106 Billion was recorded for cyber hacks in the United States in 2016 alone. The cybersecurity skills shortage is also posing a major concern. Hence, it has become imperative to develop a learning platform for the next generation of cybersecurity professionals to learn and be further equipped by introducing cybersecurity with the concept of gaming. Some of the games developed offer some challenges and a higher level of thinking. Learning through this system introduces an immersive, learner-centered experience with effectiveness on cybersecurity awareness training and practical skill acquisition for learners from diverse backgrounds. This paper evaluates the different game based learning system in cybersecurity, identifying the various tools in existence, the benefits and shortcomings of each system and feasible ways to improve on the existing systems.

Keywords
Cybersecurity; Games; Players; Attacks; Defense; Pedagogy

1. Introduction

Game based learning has gradually become a common platform used in learning in the society today. It came into existence in the late 1970s as a collaboration between gaming and education with creative innovation from educational gaming pioneers like MEC, Davidson and the learning company and over the years there has been a tremendous increase in the user experience [1]. Eames defined this method of learning as the incorporation of games which could imply video games in instructions. There are several examples of game based learning but one of the significant ones called the Oregon Trail is one of the first and best with applicable educational standards and subject specific content giving the player a captivating game experience. Other examples of starter games include: Banished, Bridge Constructor, Gone Home, Kerbal Space Program and Myst. Games often have a fantasy element that engages players. Not only does the integration of learning with gaming make science more fun; it also motivates

students to learn, keeping them engrossed in the material so they learn more effectively and encourages them to learn from their mistakes. Games are often played for the sole purpose of fun, for taking up challenges and to outplay other opponents. It can also be used as a medium of relieving stress. Games can be played to boost a player's self-esteem and personal development. Through this method of learning, dialogues are created, and social and cultural boundaries are broken.

Learners involved in the game can evaluate how well they have performed and determine their next course of actions further sharpening their motivation and their level of engagement. It also puts forward a secure and contingent environment that encourages skill acquisition. The game based learning model has its application in various parts of the industries today particularly in areas like military, medicine, business, security, technology and physical training. The game based learning model is usually chosen depending on the learning objective. Cybersecurity has occupied a major part of the society today. According to Forbes, there should be an expected growth in the cybersecurity market to 170 billion by the year 2020 [3]. This growth stems from the increase in the trend of technology and other initiatives. There is a gap in the field of cybersecurity as reports indicates a paucity of over a million skilled cybersecurity professionals needed to deal with the current cybersecurity challenges[4][5]. There is a constant increase in the estimated losses from cyber espionage and cyber-crime which results to billions every year[6]. With the evolvement of the various disciplines over time, there is a constant shift in the view of threats and vulnerabilities in cybersecurity today. Hence, it has become important to incorporate a game based learning system into the field of cybersecurity to engage the mind of the young adults thereby establishing a foundation of the skills required in information security and creating a form of passion within them to train them to become the next generation of cybersecurity professionals while having fun alongside.

The rest of the paper includes the review of the existing systems with proper classification on the categories identified, discussion on the advantages and disadvantages, conclusion on the best system in use till date.

2. Literature Review

Several studies on the game based learning system in cybersecurity have highlighted its effectiveness and shown how skills and competencies are being improved through this learning process. Various pedagogic articles have also been published on the framework and objectives on training students in cybersecurity. However, this paper classified the different games illustrated into 3 different categories.

2.1. Category 1: Theoretical Description

This category involves only the theoretical description of themes and concepts of cybersecurity without a representation of the actual gameplay. It does not require decision making with the understanding of the concepts of cybersecurity. Control-Alt-Hack, a tabletop card game built on the Ninja Burger mechanic was developed to raise awareness in information technology and cybersecurity. The game which is majorly focused on white hat hacking was built on the basis of the gaming mechanics by gaming powerhouse Steven Jackson Games.[7] The purpose of the game is to make the young generation (fourteen years and above) familiar with terminologies in computer security. It was less focused on teaching the hands-on security skills. Denning et. al [8] conducted a research on the design and evaluation to further inform technology builders and manufacturers with a major target on the

primary and secondary education audience. It involved a competition between white hackers to become the CEO of a security company.

Stop That Post Game, an application introduced for younger players was developed by the National Center for Missing and Exploited Children on themes of safe online habits with minimum concepts on cybersecurity. "*In Stop That Post, for example, the player is told that friends or family are going to post something embarrassing online, and that they must race to stop them. The player then plays a 2D physics-based platformer, and if successful, they receive narrative feedback that the social media post was prevented*."[9]. The game gives a notion to players that through the use of this application, the social media habits of friends and families can be monitored remotely. The name Stop That Post implies that the player can stop friends and family from posting inappropriate videos, pictures and comments before it gets them in trouble. Shadowrun Returns, a pen and paper tabletop role-playing game (RPG) invented by a game developer named Jordan Weisman helped to introduce the concepts of cybersecurity by blending texts into gameplay. It involves the combination of cyberpunk aesthetic with high fantasy elements such as elves and dragons[10]. Characters of both sexes (male and female) are generated in various skin colors for any of the meta-human races. An exact gear for the character's skill set would be chosen from any of the models designed. Players are not limited to just one character development path, once a player starts with a particular character archetype they are allowed to grow their character in the path they desire. As the game progresses, abilities from any archetypes can be combined for the RPG players. While playing the game, a message is received from an old friend murdered instructing you to look for the killer with a reward of money and life insurance in return[11].

2.2. Category 2: One Player Game

This category involves the games played by one person where the individual would be tested based on the understanding of cybersecurity concepts introduced in the application. Gestwicki et. al [9] conducted a research on the observations and opportunities in Cybersecurity education game design and identified CyberProtect as a medium of learning with a very rich pedagogical content. The game developed by Carney Incorporation was created for the Defense Information Security Administration. It is usually played in rounds with the installation of assets of different levels of effectiveness on different locations on the network. After the completion of a round, another attempt of exercise is recorded. This is usually done with two screens in user friendly interface and gameplay. Giannakas et. al [12] also developed a mobile game based application called CyberAware for K-6 Aged children on Cybersecurity Education and Awareness. The one player game has a conceptual framework that uses the ARCS (Attention, Relevance, Confidence and Satisfaction) Motivational Model as the Instruction Design Model. The CyberAware application involved games structured based on different fields in cybersecurity, progressing in the application by unlocking different fields in cybersecurity known as security shields thereby transitioning through the paths gradually and in a bid also learning the rudiments in cybersecurity. Different topics on security or privacy were listed on the application associated with a series of mini-games. The virtual "security shield" associated with each mini-game is unlocked upon completion. A CyberAware Certificate is awarded to the learner upon the accomplishment of all the hurdles in the game. The application was designed with scalability which increased the level of difficulty of a mini-game after the other. It was tested on 43 elementary students aged between 9 to 11 years. Before taking the test, the students had to attend a security learning course in accordance to their curriculum. Then, a preliminary evaluation was carried out through the use of pre and post

questionnaires in which the results showed a significant improvement in the learning outcome of each student.

Kumaraguru et. al [13] developed an online game called "Anti-Phishing Phil" with a major aim of educating and training users on how to defend against phishing attacks. It enables the learner to be able to differentiate the fraudulent links from the legitimate ones after consistent practice. It is an extension of the PhishGuru software earlier developed. The game is divided into four rounds, before the commencement of the game a short tutorial was provided on anti-phishing tips. For each of the rounds, Phil encounters eight worms with an embedded URL displayed when Phil gets closer to it. Phil is awarded 100 points if he is able to eat the good worms and reject the bad worms. At the end of the study the game was identified as a useful tool for knowledge acquisition and retention.

CyberCIEGE, a security awareness tool developed by the Naval Post Graduate School in 2005 employs the concept of information assurance for education and training. It has major components which includes the unique simulation engine, domain specific scenario definition language, scenario development tool and a video enhanced encyclopedia [14]. A virtual environment is birthed from the use of the scenario definition language. CyberCIEGE was used as a training and awareness tool in the US Navy. To fulfil the Navy requirements, Cone et. al [15] designed two scenarios with the first scenario alerting the player of the fundamental problems and principles and the other scenario targeted at advanced users of computer assets with a major focus of the users on the basics of computer security. Raman et. al [16] also used CyberCIEGE to investigate the grasp and application of cyber security concepts amongst graduate students. 20 scenarios were used in this research with each of them describing the concept of network security. The purpose of the study is to examine the effectiveness of this approach in learning cyber security concepts by putting game based scenarios into action. For this analysis, a study was conducted on 20 engineering graduate students offering a formal cyber security curriculum divided into 2 control groups. The first control group which contained 10 graduate students were tested without playing the game and the other control group which also comprises of 10 graduate students were tested after playing the game. The results displayed a better learning outcome for the group that played the game before the taking the test.

2.3. Category 3: Multi Player Game

This category involves more than one player where the individuals were tested based on the understanding of cybersecurity concepts introduced in the application. It involves competition between different individuals or teams with reward based outcomes.

Nagaran et. al [17] conducted a research on exploring Game Design for Cybersecurity Training and developed a gaming application called CyberNEXS which was designed to train users on the following fields in Cybersecurity; password usage and management, protection from malware and spam including the use of anti-virus and anti-malware tools with updated definitions and training on scanning, patch management, social engineering phishing techniques. The purpose of the application is to teach cyber defense and penetration testing skills to participants. It involved two teams; the blue team and the red team. CyberNEXS-CND (Computer Network Defense Centralized) is an exercise developed for defending a network under attack by the red team. There is also an administrator tagged the white team which served as a medium to communicate findings of the attack from the red team to the blue team. CyberNEXS-CND Lite was also a feature of the application developed for the availability of critical

services and secure hosts. CyberNEXS-Forensics was developed to discover evidence of intrusions and malware attacks, examining payloads, logs and trace attacks. CyberNEXS-CNA was developed to scan a system and exploit the vulnerabilities so as take control of the system. CyberNEXS-CTF (Capture the Flag) involves the two mode of operations with the first part of scanning a network and exploiting for full access control and the other part for defending the hosts from incoming attacks. There is an increasing use of the gaming application in health, education, management and other sectors. The genre of games used includes; Action Games, Role playing games, Adventure Games, Strategy Games, Sport Games, Fighting Games and Sandbox Games.

Boopathi et. al [18] introduced a gaming approach to InCTF (India Capture The Flag) with an objective to learn cybersecurity at various levels, testing the knowledge of students on the concept of cybersecurity at the various times. Three rounds of learning were introduced in the paper; the learning round which majored on the introduction of the concepts of cybersecurity, jeopardy round which involved testing the knowledge of the participants based on the learning round through a gaming approach which divided the game into various levels and the interactive round which also involves the application of cyber security in the real world scenario through the creation of virtual images. Each team would have an understanding of their vulnerabilities so as to be able to attack other teams and defend their own systems from incoming attacks. A reward system would be implemented and teams which successfully launches an attack to the other team would be awarded points. This was done through the game server. Defense points were also awarded to teams that could successfully defend their system from attacks from other teams displaying results on a scoring board. Salazar et. al [19] conducted a related research on high school students through augmented reality using virtual objects such as wooden shields as an interaction model for students to learn on the concepts of cybersecurity.

Jin et. al [20] introduced a game based learning method on cybersecurity education for high school students. GenCyber High School summer camp was launched by Purdue University Northwest to increase awareness and interest in cybersecurity and to enable high school students understand the required and safe online behavior. The games embedded in the program includes the social engineering game, secure online behavior game, Cyber Defense Tower Game, 2D GenCyber Card Game. The different classes of games were embedded for an adequate understanding of the basic principles of cybersecurity. The game topics were chosen based on the level of importance, game player's interest, insight and experience of the principle investigators. It involved the use of the attacker-defender mechanism, highly interactive and reward based. Survey design was carried at the end of the summer camp to evaluate the effectiveness for possible improvement. SecurityCom, another multiplayer game was also developed for security personnel to validate theories learnt on the concept of cybersecurity . It was tested on the effectiveness of Shared Situational Awareness and against other security games earlier developed (CyberCIEGE, CyberProtect)[21].

3. Discussion

Based on the classifications of the existing games highlighted above, distinct features were drawn out to identify the contributions of the model to the field of cybersecurity. The features below highlight the characteristics of the existing gaming models identified in this research paper.

- **Awareness:** These features entails minimal knowledge from the players on the concept of cybersecurity. It is majorly focused on evaluating the level of vulnerabilities in a system. Sufficient information is provided to the participants to develop the required skill for the game.

- **Defensive Strategy:** In this feature, substantial knowledge is required by the player to be able to efficiently use the tools to defend cyber-attacks in the game.
- **Attacker Strategy:** Here, the learner is adequately trained and equipped with the knowledge of cybersecurity to attack the other players in the game.

Table 1. Features of the Existing Gaming Models

Gaming Models	Awareness	Defensive Strategies	Attacker Strategies
CyberCiege	Yes	Yes	No
CyberProtect	Yes	No	No
CyberNexs	No	Yes	Yes
GenCyber	Yes	Yes	Yes
InCTF	Yes	Yes	Yes
CyberAware	Yes	No	No
SecurityCom	Yes	No	No
PhishGuru	No	Yes	Yes

The following section identifies the advantages and disadvantages of the categories mentioned above from the various models reviewed based on the categories described in the literature review.

3.1. Category 1 (Theoretical Approach)

This section includes Control-Alt-Hack, Stop That Post and Shadow runs with the following advantages and advantages based the practical applications:

3.1.1. Advantages

- Fun and Engaging.
- Increased awareness of risks involved in computer security and career opportunities associated with it.

3.1.2. Disadvantages

- Not enough fun since there is no incorporation of key concepts into game play.
- Longer assimilation time.
- Inadequate pedagogical content.

3.2. Category 2 (One Player Game)

This involves the classification of the following gaming models; CyberProtect, CyberAware, PhishGuru, CyberCIEGE with the following pros and cons based the practical applications:

3.2.1. Advantages

- User friendly interface for interaction with learner.
- Stimulates learners' interest with the pedagogical scenarios.
- It involves active participation of the learner with the constant problem solving method.
- It is scalable and flexible.

- Clear cut objectives for the learner to get familiar with the concept of cybersecurity.
- Guaranteed result of instant feedback for improved learning.

3.2.2. Disadvantages

- Overtime it becomes a monotonous activity as it becomes less challenging to the learner involved.
- Players' decisions are against discrete and algorithmic opponents.

3.3. Category 3 (Multi Player Game)

This includes CyberNEXS, InCTF, GenCyber and SecurityCom with the below advantages and disadvantages:

3.3.1. Advantages

- It allows for increased situational awareness.
- Improved level of engagement among participants.
- Increase in social connections through team competitions.
- Increased level of enthusiasm especially in a reward based outcome.
- There is a direct engagement in the real or virtual cybersecurity challenges.
- The players learn how to harden systems and how to think like attackers and defenders which can be applicable in the real world.
- It is flexible, scalable and highly interactive.

3.3.2. Disadvantages

- It can be time consuming as it involves input from different individuals or teams.
- The knowledge acquired might be used for nefarious purposes.
- It can result to heavy consumption of bandwidth and space.

The various categories have adequately explained the different game based learning systems in existence till date highlighting the advantages and disadvantages of each of the classes. The gaming application that stood out amongst all that was reviewed are the InCTF and GenCyber application. These applications are self-explanatory as they involved walkthroughs which made it easier for the learner to grasp the basics of cybersecurity before proceeding to carry out the assessment test. Also, the assessment test was very interactive with of the involvement of the attacker and defender. This interactive medium of learning enables the learner(s) to adequately understand what is required in the world of cybersecurity with the test carried out in a virtual and physical environment.

4. Conclusion

Cybersecurity plays a prominent role in the society today. Incorporating games into learning has proven to improve the learning outcome overtime. The major objective of this paper is to review the existing Game Based Learning (GBL) in cybersecurity, categorizing the studies into themes and identifying the various approaches, shortcomings were also highlighted. Valid tools have been developed to consolidate and enhance learning. The multiplayer game approach can be identified as one of the best interactive

mediums for GBL with more advantages and less disadvantages. However, a collaboration of the above mentioned systems with better improvement on the scalability, flexibility and increased use of themes can better equip and prepare students on cybersecurity education. Also, an improvement on the existing game based learning system is recommended to include the added features on awareness, defensive and attacker strategies. For future research, we would recommend an introduction of naturality to further improve on the existing features on the Multiplayer Game category for maximum effectiveness .

5. Acknowledgement

This research is made possible by the National Science Foundation under grant 1723650. The authors are grateful to the support of Department of Technology Systems in the College of Engineering and Technology at East Carolina University.

6. Biblography

[1] UBC (n.d.) Game Based Learning: An Emerging Market Analysis. Retrieved from: https://blogs.ubc.ca/gamebasedlearning/history/
[2] Eames, J. (2014). What Game-Based Learning Can Do for Student Achievement. EdSurge. Retrieved from: https://www.edsurge.com/news/2014-05-28-what-game-based-learning-can-do-for-student-achievement
[3] Paloalto (n.d.) What is Cybersecurity? A Definition of Cybersecurity. Paloalto Networks. Retrieved from: https://www.paloaltonetworks.com/cyberpedia/what-is-cyber-security
[4] CISCO. (2014). Annual Security Report. [PDF Document] Retrieved from: http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.
[5] Johnson, T.J. (2016). The Cybersecurity Skills Gap – And How to Fill it. Nemertes. Retrieved from: https://nemertes.com/cybersecurity-skills-gap-fill/
[6] Center for Strategic and International Studies. (2013).The Economic Impact of Cybercrime and Cyber Espionage. Retrieved from: http://csis.org/files/publication/60396rpt_cybercrimecost_0713_ph4_0.pdf
[7] Control-Alt-Hack (n.d.) White Hacking For Fun and Profit. Retrieved from: http://www.controlalthack.com/index.php
[8] 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. Computer Science & Engineering. University of Washington. ACM Publication. Retrieved from: http://dx.doi.org/10.1145/2508859.2516753
[9] Gestwicki, P., & Stumbaugh, K. (2015). Observations and Opportunities in Cybersecurity Education Game Design. *IEEE Conference on Computer Games: AI, Animation, Mobile, Multimedia, Educational and Serious Games (CGAME) Louisville*. DOI:10.1109/CGames.2015.7272970
[10] Miller, M. (2013). The Archetypes of Shadowrun Returns. Game Informer. Retrieved from: http://www.gameinformer.com/b/features/archive/2013/01/02/shadowrun-returns-online-feature.aspx
[11] Trevor, T. (2013) Shadowrun Returns. The Straits Times. Retrieved from: http://search.proquest.com.jproxy.lib.ecu.edu/docview/1428300519?accountid=10639
[12] Giannakas, F., Kambourakis, G. & Gritzalis, S. (2015). CyberAware: A Mobile Game-Based App for Cybersecurity Education and Awareness. *International Conference on Interactive Mobile Communication Technologies and Learning (IMCL) Greece*.
[13] Kumaraguru, P., Sheng, S., Acquisiti A., Cranor, L.F. & Hong, J. (2010). Teaching Johnny Not to Fall. Carnegie Mellon University. ACM Transactions on Internet Technology, Vol. 10, No. 2, Article 7. Retrieved from: http://doi.acm.org/10.1145/1754393.1754396.
[14] Irvine, C.E, Thompson, M.F. & Allen, K. (2005). CyberCIEGE: An Extensible Tool for Information Assurance Education. Naval Postgraduate School, Monterey, CA. Retrieved from: http://cisr.nps.edu/cyberciege/downloads/CISSE_CyberCIEGE_NPS_050305.pdf
[15] Cone, B.D., Irvine, C.E., Thompson, M.F. & Nguyen, T.D. (2006). A Video Game for Cyber Security Training and Awareness. Department of Computer Science. Naval Postgraduate School, Monterey, CA.

[16] Raman, R., Lal, A. & Achuthan, K. (2014). Serious Games Based Approach to Cyber Security Concept Learning: Indian Context. Semantic Scholar.
[17] Nagarajan, A., Allbeck, J.M., Sood, A., & Janssen, T.L. (2012). Exploring Game Design for Cybersecurity Training. *IEEE International Conference on Cyber Technology in Automation, Control and Intelligent Systems, Thailand.*
[18] Boopathi, K., Sreejith, S. & Bithin, A. (2015). Learning Cyber Security Through Gamification. *Indian Journal of Science and Technology,* Vol. 8(7), 642-649.
[19] Salazar, M., Gaviria, J., Laorden, C. & Bringas, P. G. (2013). Enhancing Cybersecurity Learning Through an Augmented Reality-Based Serious Game) 2013 IEEE Global Engineering Education Conference (EDUCON), Berlin, 2013, pp. 602-607. doi: 10.1109/EduCon.2013.6530167
[20] Jin, G., Tu, M., Kim, T.H., Heffron, J. & White, J. (2018). Evaluation of Game-Based Learning in Cybersecurity Education for High School Students. *Journal of Education and Learning (EduLearn).* Vol. 12, No. 1.
[21] Twitchell, D. P. (2007). SecurityCom: A multi-player game for researching and teaching information security teams. *The Journal of Digital Forensics, Security and Law : JDFSL,* 2(4), 9-18.
[22] Adams, M., & Makramalla, M. (2015). Cybersecurity Skills Training: An Attacker-Centric Gamified Approach. Technology Innovation Management Review, 5(1): 5–14. Retrieved from: http://timreview.ca/article/861.
[23] Rahim, N.H.A., Hamid, S.M.K., Laiha, M. Shamshirband, S. & Furnell, S. (2012). A Systematic Review of Approaches to Assessing Cybersecurity Awareness. *IEEE Security & Privacy Vol. 10 Issue:4*. DOI: 10.1109/MSP.2012.112.
[24] NSTEENS (n.d.) Stop That Post. National Center For Missing & Exploited Children. Retrieved from: http://www.nsteens.org/games/stopthatpost
[25] Fandom (n.d.) Shadowrun Returns. Shadowrun Wiki. Retrieved from: http://shadowrun.wikia.com/wiki/Shadowrun_Returns

Biography

TOLULOPE AWOJANA is a graduate student of Network Technology in East Carolina University where she also currently works with the Department of Technology Systems as an Information Security Research Assistant. Prior to now, she was worked as a Technical Support Engineer with leading multinationals in the world of Information Technology. She has also collaborated with other professors in the institution to publish other articles on cybersecurity and internet of things (IoT).

TE-SHUN CHOU is an Associate Professor in the Department of Technology Systems at East Carolina University. He received his Bachelor degree in Electronics Engineering at Feng Chia University and both Master's degree and Doctoral degree in Electrical Engineering at Florida International University. He serves as the program coordinator of the Master program in Network Technology for the Department of Technology Systems and the lead faculty of Digital Communication Systems concentration for the Consortium Universities of the Ph.D. in Technology Management. He is also the point of contact of ECU National Centers of Academic Excellence in Cyber Defense Education (CAE-CDE). Dr. Chou teaches IT related courses, which include network security, network intrusion detection and prevention, wireless communications, and network management. His research interests include machine learning, wireless communications, technology education, and information security, especially in the field of intrusion detection and incident response.