Comparing Serious Games for Cyber Security Education

Winston Hill, Mesafint Fanuel, Xiaohong Yuan
North Carolina A&T State University

Abstract

Serious games have been used to increase student engagement in cybersecurity education. The design and content of serious games affect learners' potential to form knowledge, skills and habitual patterns. In this paper, we compare twenty serious games for teaching cyber security at different levels from the following two aspects: (1) the cybersecurity topics covered by the games; (2) the effectiveness of the games in terms of their organization design, instructional design and delivery, and game based learning. We use the cyber security knowledge unit (KUs) defined by NIETP (National IA Education & Training Programs) for CAE/CDE (Center of Academic Excellence in Cyber Defense Education) designated academic institutions to categorize the cyber security topics covered by the games. We evaluated the user interface quality of the games in terms of visuals, animation, and audio; the problem characteristics embedded in the games; and the ease of controls. A rubric is used to compare the games. This study could inform instructors in selecting serious games to teach cyber security effectively.

Keywords

Serious Games, K-12, CAE/CDE, Cybersecurity, Knowledge Units, Rubric

Introduction

Originally defined by Clark Abt in 1970 [1] and then redefined by Mike Zyda in 2005 [2], a serious game is "a mental contest, played with a computer in accordance to specific rules that uses entertainment to further government or corporate training, education, health, public policy, and strategic communication objectives." [2]Such games typically provide an immersive in-game environment to play out subject related scenarios such as phishing attacks, basic networking, etc. Applying domain knowledge to complex situations arising in the in-game-world allows users to internalize subject matter[3].

The concept of serious games for cybersecurity awareness initially was one part of a broader awareness campaign led by governments, corporations, cyber education organizations to teach basic information assurance concepts such as: confidentiality, authentication, integrity, and availability to informal learners (people with no prior knowledge or limited knowledge). When it comes to formal learners or Computer Science students in a higher education setting, the use of games as a supplemental educational material has been investigated and utilized [4]. Nevertheless, the mass adoption of serious games to teach cyber security in general, has not yet materialized.

Studies have shown that today's schools face major problems when it comes to holding student motivation, engagement and focus for an extended period of time[5]. Because learners of this generation are "digital natives", it has also been argued that using games is more in tune with their general habits[6]. In comparison to traditional teaching methods, game-based learning allows students to make mistakes and learn from them in a risk-free environment [7],[8]. Students are free to re-enact a precise set of circumstances multiple times. Thus, they can explore the consequences of different in-game actions which are not repeatable in most school settings. For example, students could initiate a DDOS attack on a game's DNS server to understand how it affects websites. This would not be a viable nor desirable option during hands-on training. Students are also free to explore the immersive in-game world at their leisure, promoting self-directed learning.

In this paper, the cyber security topics of twenty serious games are identified using the knowledge unit (KUs) defined by NIETP (National IA Education & Training Programs) for CAE/CDE (Center of Academic Excellence in Cyber Defense Education) designated academic institutions. Furthermore, a rubric was used to measure the effectiveness of the games in terms of their organizational design, instructional design and delivery, and game based learning.

NIETP Knowledge Unit

Using a well-known cybersecurity framework for categorizing the serious games could show the educational potential of the games. Defining the content area covered by a game informs decision makers in placing the game appropriately within a cyber-security curriculum. We choose the Knowledge Units(KU's) defined by NIETP for CAE-CDEs, a framework created by the National Security Agency (NSA) and the Department of Homeland Security (DHS) [9]. Knowledge units (KU's) are defined as "mandatory topics and associated objectives that must be included in an institution's degree or certificate program" [10]. In CAE-CDE framework, each of the KU's are validated by top subject matter experts in the field of cybersecurity. Therefore, an institution seeking the CAE-CDE designation must have a cybersecurity curriculum closely aligned to this framework, covering all the KUs.

NIETP KU's mapped to another robust framework, the NICE 2.0 Framework [11]. NICE, an acronym for the National Initiative for Cybersecurity Education, is a framework prepared by the National Institute of Standards and Technology (NIST) of the U.S Department of Commerce. Primarily focused on job duties in the cyber workforce, NICE provides a superset of cybersecurity Knowledge, Skills, and Abilities (KSAs) and Tasks for each work role, category, and specialty area[11].Therefore, using the NIETP KU's provides a stronger platform for categorizing game content.

NIETP identifies three foundational knowledge units: Cybersecurity foundations(CSF), cybersecurity principles(CSP) and IT System Components(ISC). Under each foundational KU's, a further five technical core KU and five Non-technical core KUs are stated. Dozens of optional KU's are also defined. Each KU contains several topics and subtopics that need to be covered in order for a student to be a master of that specific unit. Refer to Table 1[9].

Table 1. The Knowledge Units and Topics

(KU) Knowledge Units	**Topics**
Foundational KU's	Cybersecurity Foundations, Cybersecurity Principles, IT Systems Components

Technical Core KU’s	Basic Cryptography, Basic Networking, Basic Scripting and Programming, Network Defense, Operating Systems Concepts
Non-Technical Core KU’s	Cyber Threats, Cybersecurity Planning and Management, Policy, Legal, Ethics, and Compliance, Security Program Management, Security Risk Analysis
Optional KU’s	Advanced Algorithms, Advanced Cryptography, Advanced Network Technology and Protocols, Algorithms, Analog Telecommunications etc.

Categorizing The Cybersecurity Topics Covered by Serious Games

To search for serious games on cybersecurity, we used the search terms “cybersecurity games”, “firewall games”, “network security games”, “SQL injection games”, and “cross site scripting games”. This search yielded a bulk of games to evaluate. We looked into specific cyber security attacks to craft a better search because of the lack of access to many of the games found. We chose to analyze the games that are accessible online. The serious games that were found came from different sectors including military, academia and private companies. These cyber security games cover many different topics including Cross Site Scripting, Network Simulation, SQL Injection, Cyber Awareness, etc.

To find the cybersecurity topics covered by the games, and the KU’s the games map to, we looked at the learning objectives, the descriptions, the audience of the game, and how to access the game. We also played the games paying attention to the sounds, scenarios, point system and duration of the games. After playing each game a few times and gathering details about the game, we moved on to mapping the topics they cover to the KUs. Table 2 shows the list of the games we analyzed along with the topics they covered, and the Knowledge Units associated with the games.

Table 2. The Games with the Knowledge Units

Games	**Topic**	**(KU) Knowledge Units**
Cyber Awareness[12]	Sensitive Information-PII(Personal Identifiable Information),PHI (Personal Health Information), Malicious Code -Phishing, Compressed URLs, Spear Phishing , Leaked Information	Foundational - Cybersecurity Foundations (CSF) (Common Attacks) Non-Technical Core - Cyber Threats (CTH) (Types of Attacks) Non-Technical Core - Security Program Management (SPM)(Security Training Awareness and Education)

Cyber Challenge [13]	Firewall - where they should be placed on the network, Binary Number Operation, User's Intent - adversity thinking	Technical Core - Basic Networking (BNW) (Network Protocol Introduction)
Growing an Online Reputation[14]	Social Ethics - being able to conduct one's behavior on the internet, Cyber Bullying- to point out abusing terminology against peers on the internet.	Cybersecurity Ethics (CSE) (Ethics and Cyberspace)
Proofpoint Security - Security Awareness Trial[15]	Email Security, Phishing Attack, Spear Phishing Attack	Foundational - Cybersecurity Foundations (CSF) (common attacks)
Aggie life[16]	Cybersecurity Awareness(Credit Card usage and Online Purchase)	Cyber Crime (CCR) (Fraud and Financial)
Keep Tradition Secure[17]	Cybersecurity Awareness(Credit Card usage and Online Purchase), Phishing	Foundational - Cybersecurity Foundations (CSF) (Common Attacks) Cyber Crime (CCR)(Fraud and Financial)
Football Fever[18]	Cybersecurity Awareness(Credit Card usage and Online Purchase), Phishing	Foundational - Cybersecurity Foundations (CSF) (Common Attacks)
Fight Back[19]	Cybersecurity Awareness(Credit Card usage and Online Purchase), Phishing , User's Intent	Foundational - Cybersecurity Foundations (CSF) (Common Attacks)
Cyber Security Lab[20]	Programming(Coding Challenge), Social Engineering , Password Cracking	Non-Technical Core - Cyber Threats (CTH) (Social Engineering, Password Cracking) Technical Core - Basic Scripting and Programming (BSP) (Basic Programming Constructs and Concepts)
Google Interland[21]	Anti-Bullying , Internet Safety, Phishing, Information Protection, Cybersecurity Awareness	Foundational - Cybersecurity Foundations (CSF) (Common Attacks) Non-Technical Core - Cyber Threats (CTH) (Web App Attacks) Cyber Crime (CCR)(Cyber Bullying)
Targeted Attack the Game[22]	Decision Making, Taking care of Business and Security Cost, Adversity Thinking	Foundational - Cybersecurity Foundations (CSF)(Risk Assessment)

Antiphishing Phil[23]	Phishing Attack	Foundational - Cybersecurity Foundations (CSF) (Common Attack)
Netsim[24]	Network Security, Network Attacks	Foundational - Cybersecurity Foundations (CSF) Technical Core- Basic Networking (BNW), (Network Protocols Introduction) Technical Core - Network Defense (NDF) (Network Attacks)
Data Center Attack[25]	Decision Making, Taking care of Business cost and Security cost, Adversity Thinking, Management	Foundational - Cybersecurity Foundations (CSF) (Basic Risk Assessment)
Permission Impossible[26]	Firewall Concepts	Technical Core - Basic Networking (BNW)(Network Protocols Introduction)
Blue Team[27]	Firewall Concepts	Foundational - Cybersecurity Foundations (CSF) (Common Attacks) Technical Core - Basic Networking (BNW)(Network Protocols Introduction)
Google's XSS-Game[28]	XSS Cross Site Scripting	Foundational - Cybersecurity Foundations (CSF) (Common Attack) Non-Technical Core - Cyber Threats (CTH)(Web App Attacks)
The Weakest link, A User Security Game [29]	Cybersecurity Awareness(cyber security terms), Phishing	Foundational - Cybersecurity Foundations (CSF) (Common Attacks)
Injection Game[30]	SQL Injection, XSS Cross Site Scripting	Foundational - Cybersecurity Foundations (CSF) (Common Attacks) Non-Technical Core - Cyber Threats (CTH)(Web App Attacks)
Tomorrow's Internet[31]	Cybersecurity Awareness(Cyber Security Terms)	Foundational - Cybersecurity Foundations (CSF)(Common Attacks)

Evaluating the Games Using the Rubric

To evaluate the games, we adopted the educational electronic games rubric, which was developed at California State University of Sacramento in 2004 and revisited in 2007 [32]. The rubric was developed to help evaluate an electronic game in an educational setting. The rubric was chosen because it was accessible and functional to our research. It is split into three components: Organization and Design, Instructional Design and Delivery, Game Based Learning. It defines three levels of effectiveness from lowest to highest: Baseline, Effective and Exemplary. To get a baseline score the game must make 30 points or below, for an Effective score the game must score between 30-39 points and to score an Exemplary score the game must have between 40-50 points. The different components of the rubric are describing as below.

Organization and Design

- Layout and Design. The points (0, 3, or 5) are assigned according to the number of graphic elements, variation in layout and whether the design elements assist students in understanding concepts and ideas.
- Navigation. The points (0, 3, or 5) are assigned according to the game's organization, ease of navigation, and whether the students can clearly understand where they are and where to go next.

Instructional Design and Delivery

- Objectives. The points (0, 3, or 5) are assigned according to the learning objectives are clearly identified.
- Different Learning Styles. The points (0, 3, or 5) are assigned according whether the game multiple auditory, kinesthetic, textual and/or visual activities with intent to enhance student learning.
- Higher Level Learning Skills. The points (0, 3, or 5) are assigned according to whether the game provides multiple activities to help students increase their cognitive skills, such as analysis, synthesis and evaluation.

Game Based Learning

- Rules. The points (0, 3, or 5) are assigned according to whether every rule is clearly stated.
- Goals. The points (0, 3, or 5) are assigned according to whether the goals are clearly stated and measure what students must know and be able to do to accomplish the game.
- Feedback. The points (0, 3, or 5) are assigned to the game according to whether there are frequent opportunities for students to receive timely feedback on their performance.
- Interaction. The points (0, 3, or 5) are assigned according to whether Student-to-computer and student-to-student interactions can be clearly identified. Whether there is a definitive increase in social interaction.
- Subject. The points (0, 3, or 5) are assigned according to whether the subject or topic of the game is clearly stated.

Evaluation of the Games

Table 3 is the evaluation of the games using the rubric. The highest each game can receive is 50 points. The most points that a game can gain from the Organization and Design section is 10, from the Instructional Design and Delivery section the most points that a game can receive is 15 and from the Game Based Learning section the most points a game can receive is 25 points. Table 4. shows the audience level of the games reviewed in the research. The audience level was determined by the source of the game, the game play, terminology, and difficulty of play. This table will help educators to find the games that would most impact their course.

Table 3. Evaluation of the game using Rubric

Games	**Organization and Design**	**Instructional Design and Delivery**	**Game Based Learning**	**Total**	**Effectiveness**
Cyber Awareness[12]	10	13	25	48	Exemplary
Cyber Challenge [13]	10	13	25	48	Exemplary
Growing an Online Reputation[14]	6	9	15	30	Baseline
Proofpoint Security - Security Awareness Trial[15]	10	11	23	44	Exemplary
Aggie life[16]	6	9	15	30	Baseline
Keep Tradition Secure[17]	6	9	23	38	Effective
Football Fever[18]	6	9	23	38	Effective
Fight Back[19]	6	9	23	38	Effective
Cyber Security Lab[20]	10	11	25	46	Exemplary
Google Interland[21]	10	13	25	48	Exemplary
Targeted Attack the Game[22]	6	11	23	40	Exemplary
Antiphishing Phil[23]	10	11	19	40	Exemplary
Netsim[24]	10	11	25	46	Exemplary
Data Center Attack[25]	6	11	23	40	Exemplary
Permission Impossible[26]	10	13	25	48	Exemplary
Blue Team[27]	10	11	25	46	Exemplary

Google’s XSS-Game[28]	10	13	25	48	Exemplary
The Weakest link, A User Security Game [29]	10	11	23	44	Exemplary
Injection Game[30]	10	11	25	46	Exemplary
Tomorrow's Internet[31]	10	11	19	40	Exemplary

Table 4. Audience Level of the Games

Audience Level	**Games**
K-12	Growing an Online Reputation[14],Cyber Security Lab[20],Google Interland [21],Antiphishing Phil[23],Tomorrow's Internet[31].
College and up	Injection Game [30],The Weakest link, A User Security Game[29],NetSim[24],Permission Impossible[26],Google’s XSS-Game[28],Blue Team[27] ,Data Center Attack [25],Targeted Attack the Game[22],Fight Back [19],Football Fever [18],Cyber Challenge [13],Cyber Awareness[12],Proofpoint Security - Security Awareness Trial[15]. Aggie life[16] ,Keep Tradition Secure[17].

Conclusion

Through this research we found more serious games that dealt with cybersecurity awareness than technical topics like SQL injection or network security. Seven out of the twenty serious games examined have the topic of cybersecurity awareness. Another finding was that private companies had more interactive and overall visually better games. For example, Google’s Interland[21] was very interactive and has very clean graphics versus other games like Aggie life[16]. Furthermore, though some games are oriented to K-12, most are not at the level suitable for K-8.

Despite the merits of serious games for higher education, most were originally designed with the intentions of providing guidance to a target audience of informal learners and are not aligned to an advanced learners’ needs. Thus, most of the open source serious games explored are not advanced enough to include in a cybersecurity curriculum. The few that are advanced turn out to be: less immersive, less visually engaging, and more simple and narrowly focused. This of course defeats the engagement value of game-based learning. We believe that serious games for cyber security awareness should be implemented gradually with complex concepts, starting with the most basic aspects of cyber security. Our research identifies concepts covered by some of the existing, publicly available serious games. This will uncover the cybersecurity knowledge areas that have not yet been gamified. It will also inform instructors in selecting serious games in order to teach cyber security effectively.

References

[1] Abt, C. C. (1970). Serious Games. Viking Press.
[2] Zyda, M. (2005). From Visual Simulation to Virtual Reality to Games. Computer, 38(9), 25-32
[3] Swanwick, , C. C. (2016, January 24). SERIOUS GAMES MAKE STEM FUN. Retrieved October 14, 2019, from https://www.seenmagazine.us/Articles/Article-Detail/articleid/5380/serious-games-make-stem-fun.
[4]J. Tioh, M. Mina and D. W. Jacobson, "Cyber security training a survey of serious games in cyber security," 2017 IEEE Frontiers in Education Conference (FIE), Indianapolis, IN, 2017, pp. 1-5.doi:10.1109/FIE.2017.8190712 URL:http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8190712&isnumber=8190427
[5] Papastergiou, M. (2009). Digital game-based learning in high school computer science education: Impact on educational effectiveness and student motivation. Computers & education, 52(1), 1-12.
[6] Wyld, D. C. (2009). Developing the "gamer disposition": The key to training and learning with the digital native generation may be "serious games".... seriously. Competition Forum, 7(2), 354-360. Retrieved from http://ncat.idm.oclc.org/login?url=https://search.proquest.com/docview/214848059?accountid=12711
[7] Baycrest Centre for Geriatric Care. (2018, June 11). Making mistakes while studying actually helps you learn better: When learning something new, there are instances where trial and error helps rather than hinders, according to recent findings by Baycrest researchers. ScienceDaily. Retrieved November 12, 2019 from www.sciencedaily.com/releases/2018/06/180611133437.htm
[8] Selen Turkay, Daniel Hoffman, Charles K. Kinzer, Pantiphar Chantes & Christopher Vicari (2014) Toward Understanding the Potential of Games for Learning: Learning Theory, Game Design Characteristics, and Situating Video Games in Classrooms, Computers in the Schools, 31:1-2, 2-22, DOI: 10.1080/07380569.2014.890879
[9] National Centers of Academic Excellence in Cyber Defense (CAE-CD) Designation Program Guidance on the Internet at https://www.iad.gov/NIETP/documents/Requirements/CAE_Program_Guidance.pdf, accessed: July 17, 2019
[10] Drake, R. (2018, March 6). Updates to the Cyber Defense Knowledge Unit Mapping Guide. Retrieved from https://www.nist.gov/news-events/news/2018/03/updates-cyber-defense-knowledge-unit-mapping-guide.
[11] National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework Guidance on the Internet at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf, accessed: July 17, 2019
[12] Cyber Awareness. (2019). Retrieved 20 September 2019, from https://dl.dod.cyber.mil/wp-content/uploads/trn/online/cyber-awareness-challenge/launchPage.htm
[13] Defense, D. (2019). Cybersecurity Challenge. Retrieved 14 September 2019, from https://www.cybermission.tech/#!/game/strike/1/intro
[14] Online Reputation - The Carnegie Cyber Academy - An Online Safety site and Games for Kids. (2019). Retrieved 12 September 2019, from http://www.carnegiecyberacademy.com/funStuff/onlineReputation/onlineRep.html
[15] Try Our Security Awareness Training | Proofpoint. (2019). Retrieved 15 October 2019, from https://www.proofpoint.com/us/resources/try-security-awareness-training
[16] Aggie LIFE. (2019). Retrieved 13 September 2019, from https://it.tamu.edu/aggielife/
[17] Keep Tradition Secure. (2019). Retrieved 7 October 2019, from https://keeptraditionsecure.tamu.edu/
[18] Football Fever 2016: Secure Your Season. (2019). Retrieved 13 September 2019, from https://footballfever.tamu.edu/
[19] Fight Back (2019). Fight Back | FightBack.tamu.edu. Retrieved 12 October 2019, from https://fightback.tamu.edu/
[20] Cybersecurity | NOVA Labs | PBS. (2019). Retrieved 5 October 2019, from https://www.pbs.org/wgbh/nova/labs/lab/cyber/
[21] Interland. (2019). Retrieved 12 September 2019, from https://beinternetawesome.withgoogle.com/en_us/interland
[22] Targeted Attack: The Game – Defend your data. Choose wisely. Succeed or fail. (2019). Retrieved 8 September 2019, from http://targetedattacks.trendmicro.com/
[23] Antiphishing Phil. (2019). Retrieved 12 November 2019, from https://www.ucl.ac.uk/cert/antiphishing/
[24] ”Netsim” CS4G Network Simulator. (2019). Retrieved 8 October 2019, from https://netsim.erinn.io/
[25] “Data Center Attack”Trend Micro The Game. (2019). Retrieved 13 October 2019, from http://datacenterattacks.trendmicro.com/
[26] ”Permission Impossible” Unity WebGL Player | SecondGameDraft. (n.d.). Retrieved from https://groups.inf.ed.ac.uk/tulips/projects/1617/PermissionImpossible/

[27] ”Blue Team” Unity WebGL Player | NetworkUI. (n.d.). Retrieved from https://groups.inf.ed.ac.uk/tulips/projects/1617/CharlesFirewallGameWebsite/Website/v0.7/index.html
[28] ”Google’s XSS-Game” (n.d.). Retrieved from https://xss-game.appspot.com/
[29] The Weakest Link: A User Security Game. (n.d.). Retrieved October 12, 2019, from https://www.isdecisions.com/user-security-awareness-game/.
[30] Cyber Security Game: Play injection attack game, SQL, XSS, injection web vulnerabilities. (n.d.). Retrieved from https://injection.pythonanywhere.com/
[31] Tomorrow's Internet. (n.d.). Retrieved from https://www.cdse.edu/multimedia/games/TomorrowsInternet/story_html5.html
[32] California State University, Sacramento. (2007). Educational Electronic Games Rubric. Retrieved from https://www.csus.edu/indiv/k/kaym/rubric/edgamesrubric.html
bPJ76BZhjQYQ