Journal of Education and Learning (EduLearn)
Vol.12, No.1, February 2018, pp. 150~158
ISSN: 2089-9823, DOI: 10.11591/edulearn.v12i1.7736

Evaluation of Game-Based Learning in Cybersecurity Education for High School Students

Ge Jin*, Manghui Tu, Tae-Hoon Kim, Justin Heffron, Jonathan White
Department of Computer Information Technology and Graphics, Purdue University Northwest

Article Info

Article history:

Received Nov 17, 2017
Revised Jan 2, 2018
Accepted Jan 24, 2018

Keywords:

Cybersecurity
Cybersecurity education
Game-based learning
Gamification

ABSTRACT

Game based learning is a new game play mechanism that the players explore various aspects of game play in a learning context designed by the instructor or the game designer. Nevertheless, general acceptance of game based learning as a new learning paradigm was deferred by a lack of well-controlled, large sample efficacy studies. To address the increasing need of cybersecurity workforce, this paper introduces a game based learning method for high school cybersecurity education. Purdue University Northwest launched GenCyber high school summer camps to about 200 high school students in Chicago metropolitan area. The survey conducted after the summer camp indicated that the game based learning for cybersecurity education was very effective in cybersecurity awareness training. Further analysis of survey data revealed that there is a gender difference in raising students' interests in cybersecurity and computer science education using game based learning method.

Corresponding Author:

Ge Jin,
Department of Computer Information Technology and Graphics,
Purdue University Northwest,
2200 169th Street, Hammond, IN, 46321, USA.
Email: ge.jin@pnw.edu

1. INTRODUCTION

National infrastructure, corporations, and agencies have fallen victims to cyber-attacks, and millions of sensitive data records have been compromised, especially in financial and healthcare sectors [1], [2]. Such security breaches not only result in substantial financial losses, but also greatly hurt the confidence of customers, business partners and stakeholders [3]. To protect against the cyber threats, a significant demand for skilled cybersecurity workforce is predicted in government and industrial sectors. Cybersecurity is a shared mission between government and industry, because a large portion of the national cybersecurity infrastructure is in the private sectors. Cybersecurity workforce development is the key to assuring that a nation has adequate security measures to protect and defend information and information systems. However, a global shortage of "1.8 million cybersecurity professionals by the year 2022" has been estimated [4]. According to the U.S. Bureau of Labor Statistics, the growth rate of jobs in information security is projected to be 37% from 2012–2022, and at the same time more than 209,000 cybersecurity jobs in the U.S. are unfilled every year. The increasing demand for cybersecurity professionals from both government and private sectors makes it a critical mission for higher education institutions to attract and train next generation of cybersecurity workforce and citizenry who are capable of advancing national economic prosperity and security.

Research indicates that students receiving computer education in high school are 8 times more likely to major in a computer degree. Nevertheless, the introductory secondary school computer science courses have decreased in number by 17 percent from 2005 and the number of Advanced Placement (AP) Computer Science Courses has similarly decreased by 33 percent [5]. A consensus report from The National Academies

of Sciences, Engineering and Medicine suggested that "to prepare students for expanding role of computing in academia, and industry, government agencies and states should support local, state and national programs for computing education for the purpose of increasing exposure to computing, computational principles, information security and data analytics thoughout the K-12 pipeline" [6]. These statistics and reports indicate that the key to produce more graduates in the cybersecurity field is establishing a meaningful pathway earlier in the educational process. A primary challenge to achieving this goal is the lack of age-appropriate cybersecurity curricula implemented with pedagogical methods that are most conducive to learning at the high school level [5]. The continued increase in undergraduate and graduate enrollment in computing programs is consistent with the interests of governments in nurturing Science, Technology, Engineering and Mathematics (STEM) disciplines. Nevertheless, the increased enrollment of international students has contributed most in computing related graduate programs. It will be helpful to increase the interest of domestic (US) students in pursing graduate degrees in computing programs. [7]

Studies have shown that students learn only 20% of what they hear and read, but can learn 90% of what they have practiced [8]. A study conducted by the Kansas State University showed that adults learn best when they are active partners in the learning process. The author of the study urged educators not to lecture adult learners but rather involve learners in discussions, problem solving, and hands-on activities [9]. As Anzalone, Poudel, and Vincent also indicated, “Hands-on activities and challenge tests enhanced students’ interest, motivation, and ability to think critically about contemporary environmental issues in the region” [10]. Learners at the high school level experience greater cognition if they are given opportunities to actively engage in classroom activities that support the development of critical thinking and problem solving skills. Therefore, there is a critical need for an innovative curriculum and pedagogical methods in the area of cybersecurity education. One of the most emergent and rapidly growing filed in computer-based education is "game based learning.” Game based learning include virtual reality games, web-based games, multi-user virtual environments, massively multiplayer online games, and simulations [11]. In game based learning, players can explore relevant aspect of games in a learning context designed by the instructor. In an effective game-based learning environment, a student can choose actions and experience the consequences of those actions along with the game play. Learners can make mistakes in a risk-free setting, and through experimentation, they actively learn and practice the right way to do things. However, till date, applying game based learning instructional method to cybersecurity education is limited [12].

U.S. Congress passed major legislative proposals to enhance U.S. cybersecurity and combat cyber threats. The U.S. Congress has urged that it is critical to develop high-quality educators to expand cyber education at early age [13]. To increase K-12 students' interest and and raise their awareness in cybersecurity, the National Security Agency (NSA) and the National Science Foundation (NSF) have jointly funded more than 300 summer camps to K–12 students and teachers across the nation for the past 3 years [14]. Purdue University Northwest (PNW), a NSA/DHS designated National Center of Academic Excellence in Cyber Defense Education, has successfully launched four GenCyber summer camps for 181 high school students with 51.3% of underrepresented minority (Africa Americans and Hispanics) ratio. PNW GenCyber camp developed an innovative game based cybersecurity education modules to provide high school students with hands-on activities in an immersive learning environment. PNW summer camp activities were delivered in the format of game based learning and hands-on labs. Four cybersecurity education games were developed to teach social engineering, cyber-attack and defense methods, secure online behavior, and cybersecurity principles. The game based cybersecurity education is extremely beneficial to the future cybersecurity workforce by exposing more high school students to the cybersecurity education pathway at a time when they are making decisions regarding higher education. Survey result of 154 camp participants indicated that the cybersecurity education games were very effective in cybersecurity awareness training. The innovative pedagogical methods and age appropriate game based learning curriculum, has made cybersecurity concepts more accessible to students of varying ability levels.

2. RESEARCH METHOD

The primary goals of PNW GenCyber high school summer camp are: 1) increase interest in cybersecurity, 2) raise general awareness of cybersecurity and help all students understand appropriate and safe online behavior, and 3) increase diversity in the US cybersecurity workforce. To achieve aforementioned Gencyber goals, we developed four cyber security education games for high shool students. The rationale of game topics selection will be described in the following sections. Futhermore, to evaluate the effectiveness of the developed cybersecurity education games, post-camp survey was conducted after the completion of summer camp activities. The survey questions and study protocol were carefully reviewed by the Purdue Internal Research Board to protect minor high school students.

The game topics were selected based on the following reasons:

a. Game topics were selected based on the priority and importance announced by NSA GenCyber program. The request for proposal (RFP) from NSA GenCyber clearly indicated that appropriate and safe online behavior and 10 cybersecurity first principles are the top priority of GenCyber program. Threfore, we developed 3D secure online behavior game, and 2D GenCyber first principle card game.
b. One game topic was selected based on the insight and experience of principle investigators. Quite a lot of cyber attacks start from social engineering. Social engineering is a way to manipulate and deceive people to acquire confidential information for further cyber attacks. Threfore, we developed a 3D social engineering game to prepare high school students to overcome social engineering scams.
c. Another game topic was selected based on the game player's interest. Tower defense game is a sub-genre of Realtime Strategy (RTS) game, which is one of the most played game genre for high school kids. We developed cyber security tower defense game to allow the high school students learn basic cyber security knowledge by playing realtime cybersecurity tower defense game.

In the following section, we will describe each cybersecurity game in detail:

1. Social engineering game: Social engineering is the art of manipulating people so they give up confidential information, and social engineering scams such as phishing email have been extremely effective in security attacks. PNW GenCyber camp implemented a 3D VR game to simulate Piggybacking, Tailgating, and Mantrap in a security enhanced office environment to raise general awareness of social engineering scams.

Figure 1. 3D Social engineering game

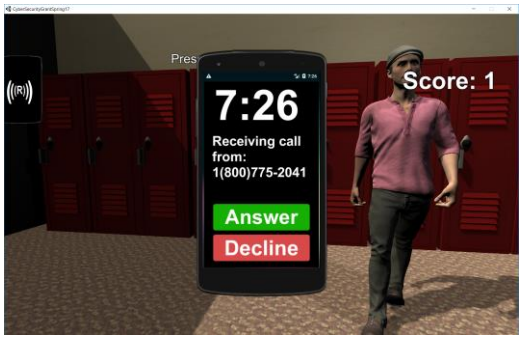

Figure 2. 3D Secure online behavior game

2. Secure online behavior game: Secure online behaviors include: identifying phishing emails and appropriately handling them, distinguish between trustworthy web links and insecure links, handling phony phone calls, and protecting personal information. A 3D VR secure online behavior game was developed to simulated high school computer lab and student's bedroom environment. The secure online behavior game allows students to appropriately handle email messages, text messages, web links and phone calls, using various computing devices such as school computers, mobile phones, laptop computer, and networked game console.
3. Cyber Defense Tower Game: Tower defense game is a subgenre of strategy game to defend a player's territories or possessions by placing defensive structures on or along their path of attack [15]. A Cyber Defense Tower Game was created to allow students to protect their virtual computer server from the different cyber-attacks by applying GenCyber first principles and cybersecurity knowledge. Students need to select the correct types of defense tower to stop each wave of cyber-attacks. As the game progresses, the combinations of the different cyber-attacks would come faster and will make it more difficult for students to defend their servers.
4. 2D GenCyber Card Game: The Gencyber card game is a computerized version of physical GenCyber card game. Physical GenCyber card game requires two players to play the game in face-to-face mode. The computer based GenCyber card game is a single-player version of the GenCyber card game, which allows the student to play the card game by themselves at any convenient time.

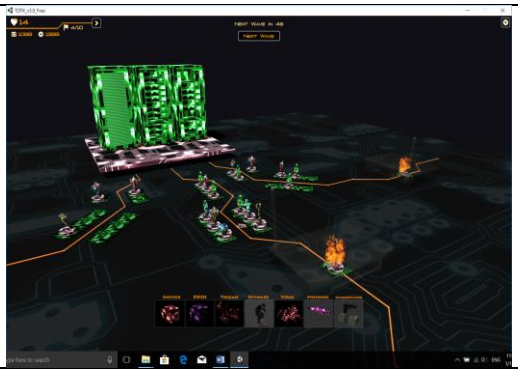

Figure 3. Competition level in cyber tower defense game

Figure 4. Single-player genCyber card game

2.1. 3D Virtual Reality Game Development in Unity3D

Social engineering and secure online behavior game were developed in Unity3D game engine. Both games can be classified as 3D Role-Playing-Game (RPG) genre. The development of 3D RPG cyber security game consists of three major technical components: (1) 3D character and game environment modeling, (2) animation of the 3D game characters, and (3) scripting/programming of the interaction between game characters and dynamic behaviors.

The 3D characters of the game were created from Adobe Fuse software. Instead of modeling a 3D character from scratch, Adobe Fuse allows a user to assemble a 3D character from more than 20 base characters and further customize it into a unique character with different weight, height, skin tones, and texture.

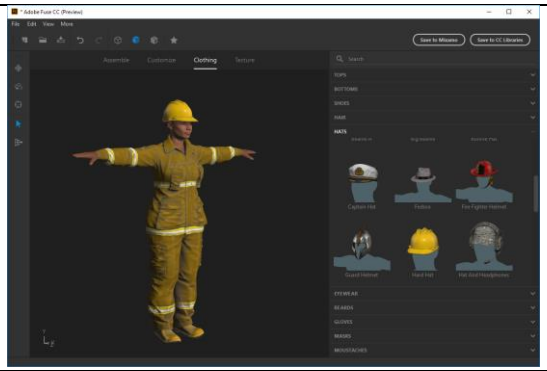

Figure 5. 3D Character modeling and customization in Adobe Fuse

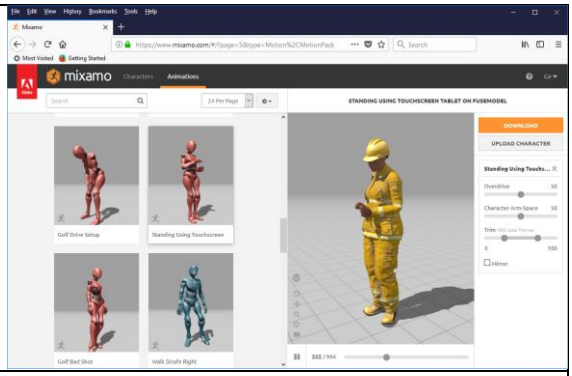

Figure 6. Character animation in Mixamo

The 3D character from Adobe Fuse was transferred seamlessly into Mixamo software. Mixamo will automatically rig the 3D character and provide hundreds of different motion clips that can be used to animate the character. We selected essential motion clips (such as idle, walk, run, talk, sit, and stand) for each character and export the animated 3D character to Unity3D game engine.

The game environment was modeled mostly using the loyalty-free 3D assets from Unity Marketplace. Several 3D assets that related with social engineering and secure online behavior were modeling using Autodesk 3D Max and Maya software. The behaviors of the 3D game characters were implemented by programming Unity C# script for each 3D character and dynamic assets in the game environment.

Figure 7. Programming interactions and dynamic behaviors using Unity C# script

2.2. Development of Cyber Tower Defense Game in Unity3D

The cyber tower defense game was implemented on top of Tower Defense Toolkit (TDTK) developed by Song Tan [16]. TDTK is a C# coding framework for the easy construction of Tower Defense games. TDTK comes with a bundle of scripts that can be adjusted to fit a variety of Tower Defense gameplay scenarios. The toolkit is customizable, and user can integrate their own art assets to make unique Tower Defense game. We have created 7 unique cyber-attacks (Figure. 8) and 6 cyber defense towers (Figure. 9).

Figure 8. Types of cyber-attacks in cyber defense tower game

Figure 9. Types of cyber-defenses in cyber defense tower game

One limitation of TDTK is that there are only two types of attacks: ground, air and three types of defense towers: ground, air and hybrid. It's impossible to use the built-in attacks and defense towers to simulate the cyber-attacks and defenses. We have customized the Tower Defense Toolkit to include 7 additional attack types (Virus, Phishing, Trojan, Spyware, Ransomware, DDoS, and Sniffer), and 6 additional defense towers (Antivirus, Password, System Update, Secure Cyber Behavior, Encryption, and Firewall). Some defense towers will defend single type of attack, while other defense towers can defend multiple attack types. For example, the Antivirus tower will defend against Virus, Trojan and Spyware. In addition, certain type of attack can be defended by multiple defense towers. The Sniffer attack can be defended by Password tower and Encryption tower. Cyber Defense Tower Game contains three difficulty levels: tutorial, intermediate and competition level.

2.3. Single-player GenCyber Card Game

The single player version of GenCyber Card game was developed to enhance the students' understanding of 10 Cyber Security First Principles. The original card game was designed and created by Dr. Vincent Nestler at California State University San Bernardino [17]. The computerized GenCyber card game was created by scanning the cards and uploading the images into Processing programming environment. The

site team observed students playing this game during the down time at camp and some students were even creating "cheat sheets" so they could beat their friends' times.

2.4. Post-camp Survey Design

An anonymous post camp survey on cybersecurity knowledge and career interests has been conducted to evaluate the effectiveness of the summer camp activities. The survey was conducted independent of the camp activities and the participation of the survey is totally voluntarily. The survey questions were designed to collect the following data: 1. Demographic data of the participants, activity participation rate, lab/game results; 2. Students' assessment of self-efficacy related to cybersecurity knowledge and the GenCyber camp experiences; 3. Consent form signed by the participants or guardians, and assent form from the Minor students.

Table 1. shows the survey questions on demographic information, and Table 2. Shows survey questions evaluating self-efficacy in cybersecurity knowledge and GenCyber camp experiences.

Table 1. Demographics information in post-camp survey

Gender:	____Male ____Female
Ethnic Category:	_____American Indian _____African American ___Asian _____ Hispanic _____ Pacific Islander ___ White

Table 2. Post-camp survey questions

Question Number	Post-Camp Survey Questions
Q1.	I enjoyed learning about computer science
Q2.	I would like to learn more about computer science
Q3.	I enjoyed learning about cybersecurity
Q4.	I would like to learn more about cybersecurity
Q5.	The teachers/faculty in this program made me more interested in cybersecurity
Q6.	I know what cybersecurity means
Q7.	I know more about cybersecurity than I did before this camp
Q8.	I know more about computer science than I did before this camp
Q9.	I am more comfortable learning cybersecurity concepts now
Q10.	I know more about information security than I did before this camp
Q11.	I can explain why cybersecurity is important
Q12.	Overall this camp was a good experience
Q13.	I am glad I attended this camp
Q14.	I would like to attend more camps like this
Q15.	My opinions and ideas were respected in this camp
Q16.	I found the camp activities interesting
Q17.	I liked interacting with the teachers at this camp

3. RESULTS AND ANALYSIS

Purdue University Northwest has successfully launched two 1-week summer camps in June 2016, and another two 1-week summer camps in June 2017. A total of 181 high school students attended the with 93 students (51.3%) were underrepresented African American and Hispanic students. During the 1-week summer camp, each student participated in activities mentored by a team of PNW faculty members and student assistants. The students were exposed to cybersecurity first principles and cybersecurity awareness by playing various cyber security computer games during the first two days. About 25 students in one classroom have competed for 3D Secure Online Behavior game, Cyber Defense Tower game and Single-player Gencyber Card game. We picked one winner from each competition and awarded the winner with a small gift on the last day of the summer camp.

Table 3. Demographic information of PNW GenCyber post-camp survey participants

Year	Gender	Numer of participants	Race	Numer of participants
2016	Male	50	Caucasian	30
	Female	22	Non-Caucasian	42
2017	Male	45	Caucasian	34
	Female	25	Non-Caucasian	48
Total		154		154

The post-camp survey was conducted at the last day of the summer camp. A 5-point Likert scale was used to measure the student's satisfactory rate of camp activities and experiences ranging from 5 (strongly agree) to 1 (strongly disagree). The post-camp survey of 154 camp participants (Table. 3) indicated that game based learning for cybersecurity enhanced student's knowledge in cybersecurity, and understanding of the cybersecurity first principles, and educated a digital citizenry with security awareness, and motivated them to pursue higher education and careers in the field of cybersecurity.

Table 4. Post-camp survey results

Question Number	Average Rating	Question Number	Average Rating	Question Number	Average Rating
Q1.	4.36	Q7.	4.36	Q13.	4.46
Q2.	4.22	Q8.	4.26	Q14.	4.17
Q3.	4.27	Q9.	4.08	Q15.	4.32
Q4.	4.05	Q10.	4.29	Q16.	4.22
Q5.	4.20	Q11.	4.18	Q17.	4.28
Q6.	4.27	Q12.	4.46		

The authors further analyzed the survey data to investigate the gender and racial difference of participants' experience in game-based learning. Hypothesis testing for two population means with unequal variance (T-Test) was used to test gender and racial difference for each survey question. For each survey question, we performed both two-tail and one-tail hypothesis test. For example, the hypothesis for "Qi. I enjoyed learning about computer science" was:

1. Two-tail hypothesis test
   H_0: There is no difference in mean survey rating of Qi between female and male students ($\mu1 = \mu2$).
   H_A: There is difference in mean survey rating of Qi between female and male students ($\mu1 \neq \mu2$).
   Significance level (α)= 0.05
2. One-tail hypothesis test
   H_0: The mean survey rating of female students is higher than or equal to the male students ($\mu1 \geq \mu2$).
   H_A: The mean survey rating of female students is lower than the male students ($\mu1 < \mu2$).
   Significance level (α)= 0.05

Table 5. Evaluation of the gender difference in game-based learning for cyberseucrity education

Question Number	Average Female Rating (sample size = 47)	Average Male Rating (sample size = 107)	p-value (two-tail test)	p-value (one-tail test)
Q1.	4.09	4.48	0.01	0.00
Q3.	4.06	4.36	0.09	0.05
Q5.	3.98	4.30	0.06	0.03
Q11.	3.96	4.28	0.07	0.04
Q16.	3.91	4.36	0.01	0.01

The result of hypothesis testing shows that: there are significant differences between male and female students' impression about the camp activities in survey question 1 and survey question 16. The one-tail hypothesis test indicates that: the male students rated the survey question 3,5,11, higher than female students. These results can be interpreted as: the male students thought the game based learning camp activities were more enjoyable and interesting than female students.

To test the racial difference, we performed both two-tail and one-tail hypothesis test for Caucasian and non-Caucasian participants. The hypothesis for "Qi. I enjoyed learning about computer science" was:

1. Two-tail hypothesis test
   H_0: There is no difference in mean survey rating of Qi between Caucasian and non-Caucasian students ($\mu1=\mu2$).
   H_A: There is difference in mean survey rating of Qi between Caucasian and non-Caucasian students ($\mu1\neq\mu2$).
   Significance level (α)=0.05
2. One-tail hypothesis test
   H_0: The mean survey rating of non-Caucasian students is higher than or equal to the Caucasian students ($\mu1\geq\mu2$).

H_A: The mean survey rating of non-Caucasian students is lower than the Caucasian students ($\mu 1 < \mu 2$).
Significance level (α)= 0.05

Table 6. Evaluation of the racial difference in game-based learning for cyberseucrity education

Question Number	Average Caucasian Rating (sample size = 64)	Average Non-Caucasian Rating (sample size = 90)	p-value (two-tail test)	p-value (one-tail test)
Q11.	4.34	4.07	0.07	0.03

The result of hypothesis testing between racial group shows that: there are no significant differences between Caucasian and non-Caucasian students' about the camp activities and experiences. The one-tail hypothesis test indicates that the Caucasian students rated the survey question 11 higher than non-Caucasian students. This result shows that the Caucasian students have higher self-efficacy than non-Caucasian students after the game-based learning camp activities.

4. CONCLUSION

This paper describes evaluation results of game based learning for high school cybersecurity education. Four cybersecurity computer games were developed to educate social engineering, secure online behaviors, and 10 cybersecurity first principles. The use of game based learning in the PNW GenCyber camp was an excellent platform to teach cybersecurity principles and secure online behaviors for high school students. This approach is beneficial to the future cybersecurity workforce by exposing more high school students to the cybersecurity education pathway at a time when they are making decisions regarding higher education. The game based learning method was well received by the students, support staff, instructors, and site visit team. This was also supported by the post camp survey conducted for 154 participants with average rating of 4.26 out of 5. To investigate the gender and racial difference of game-based learning, hypothesis testing for two population means with unequal variance (T-Test) was conducted to test gender and racial difference. The hypothesis testing result indicated that the male students thought the game based learning activities were more enjoyable and interesting than female students, and the Caucasian students showed higher self-efficacy than non-Caucasian students after the game based learning camp activities.

ACKNOWLEDGEMENTS

This research was supported by NSA & NSF grant H98230-17-1-2006.

REFERENCES

[1] E. Johnson and N. Willey, "Usability failures and healthcare data hemorrhages," *IEEE Security and Privacy,* vol 9, pp. 18-25, 2011.
[2] M. Tu and K. Spoa-Harty, "Data loss prevention management and control: inside activity monitoring, identification, and tracking in healthcare enterprise environments," *Journal of Digital Forensics, Security, and Law*. vol. 10, pp. 27-44, 2015.
[3] L. Trautman, "Cyberseurity: what about US policy?," *Journal of Law, Technology and Policy*, vol. 2015, pp. 341, 2015. Available from: https://ssrn.com/abstract=2548561.
[4] A Frost and Sullivan Executive Briefing, *Global Information Security Workforce Study*, 2017. Available from: https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf. [Accessed 27th August 2017].
[5] Microsoft. A National Talent Strategy: Ideas for Securing U.S. Competitiveness and Economic Growth, 2012. Available from: https://news.microsoft.com/download/presskits/citizenship/MSNTS.pdf. [Accessed 12th Jan 2018].
[6] National Academies of Sciences, Engineering, and Medicine. Assessing and Responding to the Growth of Computer Science Undergraduate Enrollments, 2017. The National Academies Press, Washington, DC. http://doi.org/10.17226/24926. Available from: https://www.nap.edu/read/24926/chapter/1. [Accessed 12th Jan 2018].
[7] S. Zweben, "Computing Degree and Enrollment Trends," 2012-2013 CRA Taulbee Survey, 2013. Available from: http://archive2.cra.org/uploads/documents/resources/taulbee/CRA_Taulbee_CS_Degrees_and_Enrollment_2012-13.pdf. [Accessed 26th August 2017].
[8] M. Findley, "The relationship between student learning styles and motivation during educational video game play," *International Journal of Online Pedagogy and Course Design*, vol. 1 (3), pp. 63-73, 2011.
[9] K-State Research and Extension. Instructor guide for the landscaping and horticultural services industry, 2007. Available from: http://www.ksre.ksu.edu/bookstore/pubs/MF2716.pdf. [Accessed 5th December 2017].
[10] C. Anzalone, D. D. Poudel, and L. M. Vincent, "Hands-On Activities and Challenge Tests in Agricultural and Environmental Education," *The Journal of Environmental Education*, vol. 36 (4), pp. 10-22, 2005.

[11] A. Kumar, S. Gupta, A. Rai, and S. Sinha, "Social networking sites and their security issues," *International Journal of Scientific and Research Publications*, vol. 3 (4), pp. 1-5, 2013.
[12] S. Tang and M. Hanneghan, "A Model-Driven Framework to Support Development of Serious Games for Game based Learning," *The 3rd International Conference on Developments in e-Systems Engineering*. London, pp. 95-100, 2010.
[13] J. Cuny and J. Hamos, NICE cybersecurity in K-12 formal education, 2011. Available from: http://csrc.nist.gov/nice/Sept2011-workshop/presentations/Thursday/Thurs_Cuny_NICE_K-12_092211.pdf. [Accessed 25th August 2017].
[14] T. Ladabouche and S. LaFountain. "GenCyber: Inspiring the Next Generation of Cyber Stars," *IEEE Security & Privacy*, vol 14 (5), pp. 84-86, 2016.
[15] D. Reece. "Best Tower Defense Games of All Time," Gameranx: Top Rated Games, Reviews and News, 2015. Available from: http://gameranx.com/features/id/13529/article/best-tower-defense-games/. [Accessed 6th May 2017].
[16] S. Tan. Tower Defense ToolKit (TDTK), 2016. Available from: https://www.songgamedev.com/tdtk. [Accessed 12th March 2017].
[17] V. Nestler. Cyber Realm, 2016. Available from: http://gencybercards.com/. [Accessed 25th May 2017].

BIOGRAPHIES OF AUTHORS

Dr. Ge Jin is currently an associate professor in the Department of Computer Information Technology and Graphics at the Purdue University Northwest. He holds a B.S. in Computer Science from Peking University, China, and an M.S. in Computer Science from Seoul National University, South Korea. He earned his Doctor of Science degree in Computer Science with a concentration in computer graphics from the George Washington University. His research spans the fields of computer graphics, virtual reality, computer animation, medical visualization, and educational game development.

Dr. Manghui Tu is an associate professor of Computer Information Technology, Director of the Center of Excellence for Cyber Security and Infrastructure Protection, and the Point of Contact of the NSA/DHS Designated National Center of Academic Excellence in Cyber Defense Education at Purdue University Northwest. Dr. Tu's areas of expertise are information assurance, digital forensics, cybersecurity education, and cloud computing. His research has been supported by NSA and NSF and published over 40 peer reviewed papers in prestigious journals and peer reviewed conference proceedings. Dr. Tu has over 11 years of college teaching and research experiences in cybersecurity and digital forensics.

Dr. Tae-Hoon Kim is currently an associate professor in the Department of Computer Information Technology and Graphics at the Purdue University Northwest. He has 6 years of college teaching and research experience in computer networks and network security with 12 plus publications, taught computer networks, network security, network design & administration courses at both undergraduate/graduate levels, mentored over 60 students through funded research projects, GenCyber and K-12 summer camps.

Mr. Heffron is currently a graduate student in the Department of Computer Information Technology and Graphics at the Purdue University Northwest. He received B.S. degree in Computer Graphics Technology from Purdue University Northwest.

Mr. Jonathan White is currently a STEM educator. He received B.S. degree in Computer Graphics Technology from Purdue University Northwest.