Development and Evaluation of Cybersecurity Education Games for High School Students

Ge Jin, Purdue University Northwest; Manghui Tu, Purdue University Northwest; Tae-Hoon Kim, Purdue University Northwest; Justin Heffron, Purdue University Northwest; Jonathan White, Purdue University Northwest, Anastasia Trekles, Purdue University Northwest

Abstract

Cybersecurity workforce development is the key to protect information and information systems, and yet, more than 30% of companies are short of security expertise. To address this need, the authors have developed four cybersecurity education games to teach social engineering, secure online behavior, cyber defense methods, and cybersecurity first principles. These games are intended to recruit the next generation cybersecurity workforce by developing an innovative cybersecurity curriculum and pedagogical methods which provide high school students with hands-on activities in a game-based learning environment. Purdue University Northwest (PNW) offered high school summer camps for 181 high school students in June 2016 and June 2017. Out of 181 high school participants, 107 participants were underrepresented minority students, including African Americans, Hispanics, Asians and Native Americans. To evaluate the effectiveness of developed cybersecurity education games, post-camp surveys were conducted with 154 camp participants. The survey results indicated that the developed cybersecurity education games were very effective in cybersecurity awareness training. Furthermore, the cybersecurity education games were more effective for male students than female students in raising students' interests in computer science and cybersecurity.

Introduction

With the recent high profile cybersecurity incidents targeting Sony Pictures, Target, and Anthem, and the massive Office of Personnel Management (OPM) government data breach that followed, cybersecurity has become a top priority for the U.S. government. Cybersecurity is a shared mission between government and industry, because a large portion of the national cybersecurity infrastructure is in the private sectors. Over the past few years, millions of gigabytes of sensitive data have been compromised, and a large number of fraud incidents have been committed, especially in the 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]. Cybersecurity workforce development is the key to ensuring that a nation has adequate security measures to protect and defend its 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% between 2012–2022, and thus far, more than 209,000 cybersecurity jobs in the U.S. have gone unfilled every year. The increasing demand for cybersecurity professionals requires collaborative efforts from government, industry, and K-12 and higher education institutions to attract, prepare, and train future cybersecurity professionals.

Cybersecurity has become a top priority for the U.S. government. The U.S. government and major legislative proposals have been passed to enhance U.S. cybersecurity and new government agencies have been proposed to 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 [5]. Expanding cybersecurity education to high schools is sorely needed, as "the key to training more cybersecurity experts… is exposing students to STEM education… as well as adding some cybersecurity training in high school" [6]. National Security Agency (NSA) and 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 [7].

Research indicates that students receiving computer education in high school are eight times more likely to major in a computer degree, yet in the last 20 years, enrollment in computer education courses has seen a dramatic decrease at the high school level [8]. In addition, student participation does not align with overall national demographics. These statistics indicate that the key to developing more graduates in the cybersecurity field is establishing a meaningful pathway earlier in the educational process and making it accessible to all students. 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].

Studies have shown that students tend to retain only 20% of what they hear and read, but can retain 90% of what they have practiced [9]. Traditional teaching uses lectures as the major vehicle to deliver scientific knowledge and technology to learners, which has proven to fall short for learners. Learners at the high school level experience greater learning gains 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 curriculum that uses innovative pedagogical methods in the area of cybersecurity education.

Computer-assisted instruction (CAI) comes in many forms, and one of the most popular emergent methods is commonly referred to as "game-based learning." As its name suggests, this method uses computer games to immerse learners in an artificial or simulated game environment while experiencing it as real. Game based learning includes virtual reality games, web-based games, multi-user virtual environments (MUVEs), massively multiplayer online games (MMOs), and simulations [10]. To date, however, applying game based learning instructional methods to cybersecurity education has been limited [11].

Starting in 2016, Purdue University Northwest successfully launched four GenCyber summer camps for 181 high school students, with 107 participants from underrepresented minorities (e.g., African American, Hispanics, Asians, and Native Americans). The PNW GenCyber camp developed innovative game-based cybersecurity education modules to provide high school students with hands-on activities in an immersive learning environment. Included with this were virtual reality (VR) 3D games, robotic programming games, and practical ethical hacking and cyber forensics labs based on simulated cases for cybersecurity training for high school students. Such game-based cybersecurity education is extremely beneficial to the future cybersecurity workforce, as it exposes more high school students to the cybersecurity career pathway at a time when they are making decisions regarding higher education. The innovative pedagogical methods and age-appropriate game-based learning curriculum has made cybersecurity concepts more accessible to students of varying ability levels. This was supported by the post-camp survey answered by 154 participants (return rate of 85%).

Research Method

The primary goals of the GenCyber high school summer camp were to: "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" [12]. To raise general awareness of cybersecurity and safe online behavior of high school students, PNW developed cybersecurity education games to meet the GenCyber program goals, which included the following:

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 emails have been extremely effective in security attacks. The PNW GenCyber camp implemented a 3D VR game to simulate piggybacking, tailgating, and mantraps in a security-enhanced office environment to raise general awareness of social engineering scams.

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 fraudulent phone calls, and protecting personal information. A 3D VR secure online behavior game was developed to simulate a high school computer lab and a typical student's bedroom environment. The secure online behavior game allows students to explore how 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" [13]. 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. During play, students need to select the correct type of defense towers to stop each wave of cyber-attacks. As the game progresses, the combinations of different cyber-attacks come faster and become more complex, making 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 [14]. The physical GenCyber card game requires two players to play the game, while the computer-based GenCyber card game is a single-player adaptation, allowing the student to use the game for self-study at any time.

Through their research, the authors of this paper also created a number of case studies based on the following digital simulation and modeling tools in both the mechanical and electrical engineering technology fields.

Development of Social Engineering Game and Secure Online Behavior Game in Unity3D

Social engineering and secure online behavior games were developed in the Unity3D game engine. Both games can be classified as 3D Role-Playing-Games (RPG). The development of the 3D RPG cyber security game consisted 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 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 with different weight, height, skin tones, and texture (Figure. 1).

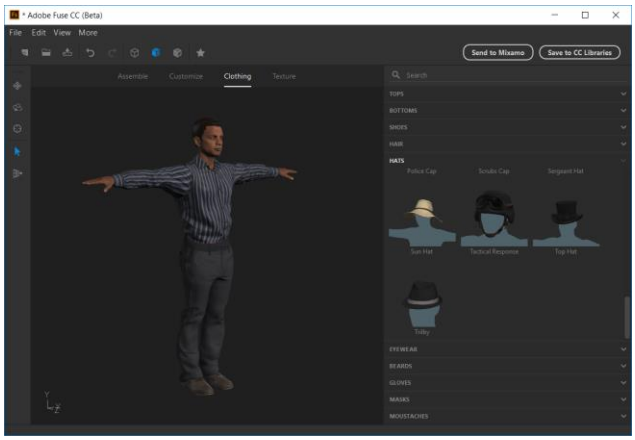

Figure 1. 3D Character Modeling and Customization in Adobe Fuse

The 3D character created in Adobe Fuse was transferred seamlessly into the Mixamo software (Figure. 2). Mixamo offers hundreds of different motion clips that can be used in animation, so essential motion clips (such as idle, walk, run, talk, sit, and stand) were chosen for each character and exported to the Unity3D game engine.

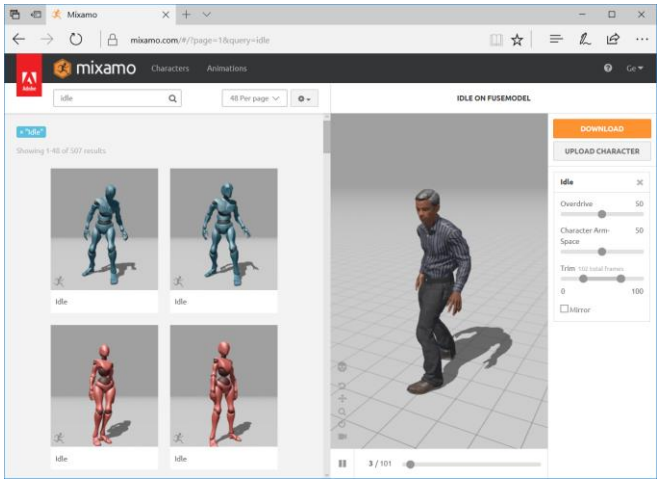

Figure 2. Character Animation in Mixamo

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

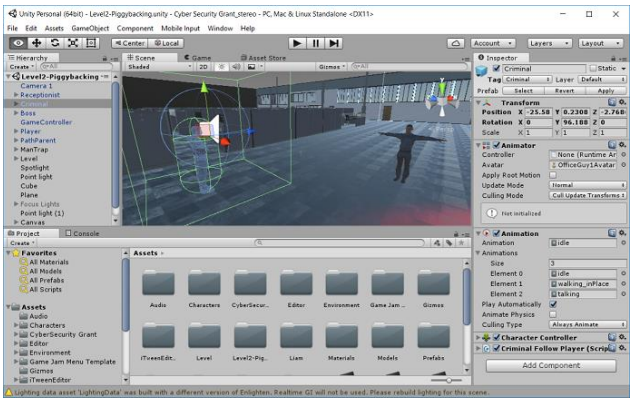

Figure 3. Programming Interactions and Dynamic Behaviors Using Unity C# Script

The social engineering game and secure online behavior game required 3D characters to walk, talk, and make unique gestures. To animate a game character in RPG style games, an animation component was added to the imported 3D character asset, providing these essential movements to the character so that a game player can control and animate the 3D virtual character in different situations (Figure. 4).

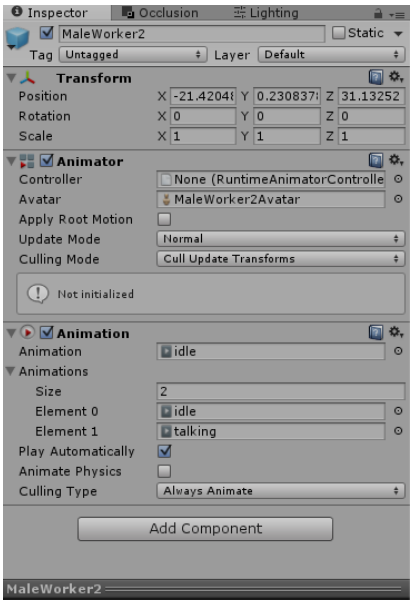

Figure 4. Adding Animation Component to a 3D Character in Unity Game Engine

To make the virtual game character perform different actions based on the input event, a “Box Collider” from Unity Inspector control panel was added to the character to trigger different animations when another character entered the “Box Collider” area (Figure. 5).

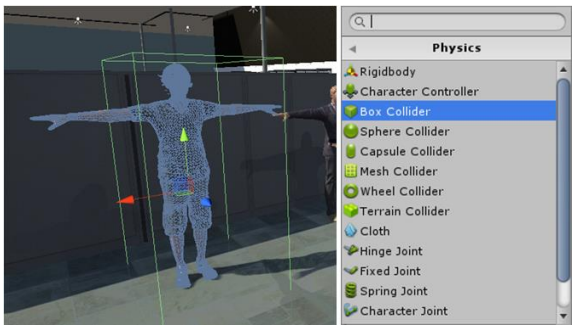

Figure 5. Adding a "Box Collider" to a 3D Character

A character control C# script was also programmed to allow a 3D character behave differently based on the input event used. Figure 6 shows a simple dialogue script that has been applied to a game character. The character will repeat "idle" motion until a game player approaches a non-player character. If a game player entered the "Box Collider" region, the character will start to talk with the game player by triggering a "talking" animation clip.

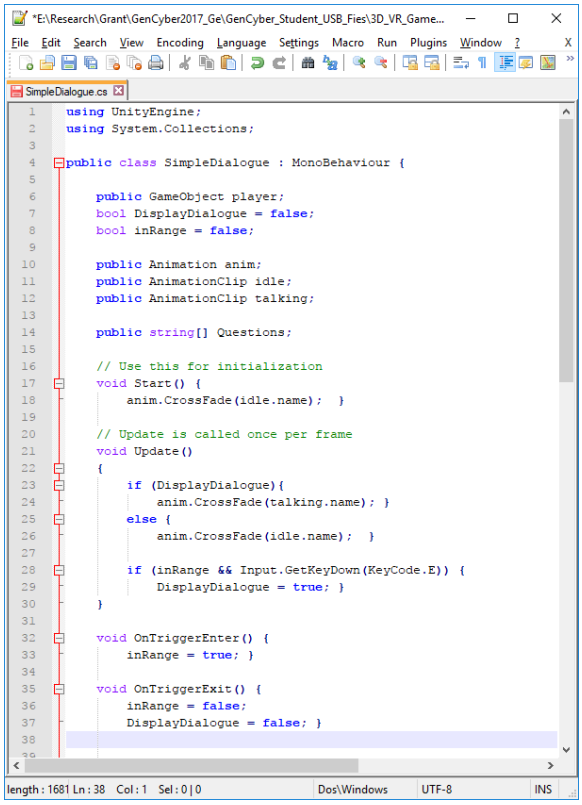

Figure 6. Unity C# Script to Trigger "Talking" Animation

The simple dialogue script was added to the 3D game character through the Unity Inspector control panel. Figure 7 shows examples of public variables that can be assigned or modified in various situations. The "Player" variable controls the game player that can be interacted with the 3D character, and the "Question" variable provides the content of a dialogue between the game player and a non-player character.

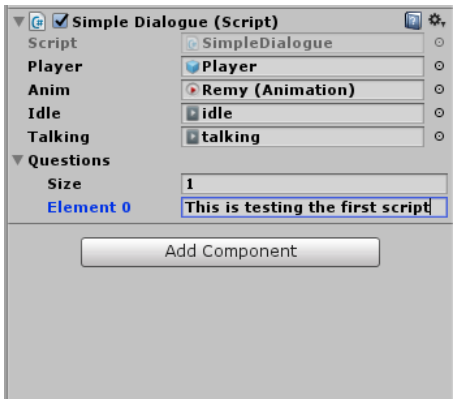

Figure 7. "Simple Dialogue" Script Interface to Set a Number of Public Variables

Figures 8 and 9 were captured from the social engineering and secure online behavior games respectively.

Figure 8. 3D Social Engineering Game Example Screen

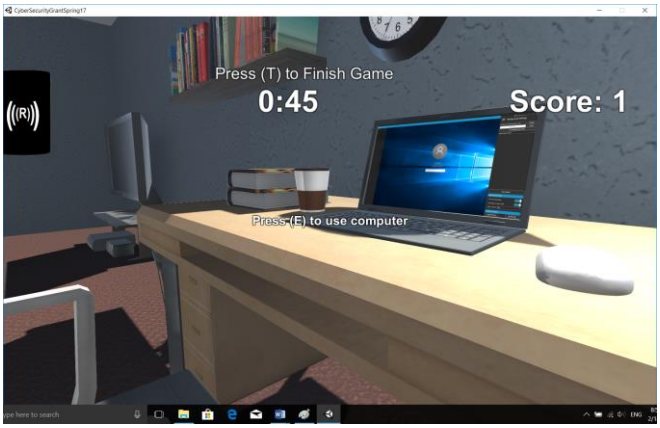

Figure 9. 3D Secure Online Behavior Game Example Screen

Development of Cyber Defense Tower Game in Unity3D

The Tower Defense Toolkit (TDTK) developed by Song Tan is a Unity C# script library to assist game developers quickly create Tower Defense prototype games [15]. The Cyber Defense Tower game was implemented on top of this TDTK framework, and includes designed custom models and art assets. The user can also integrate their own art assets to make their own unique Tower Defense game. Seven unique cyber-attacks (Figure. 10) and six cyber defense towers (Figure. 11) are included.

Figure 10. Types of Cyber-Attacks in Cyber Defense Tower Game

Figure 11. Types of Cyber-Defenses in Cyber Defense Tower Game

One limitation of TDTK is that there are only two types of attacks – ground and air (Figure. 12) – and three types of defense towers, ground, air and hybrid (Figure. 13). It is impossible to use the built-in attacks and defense towers to simulate the cyber-attacks and defenses.

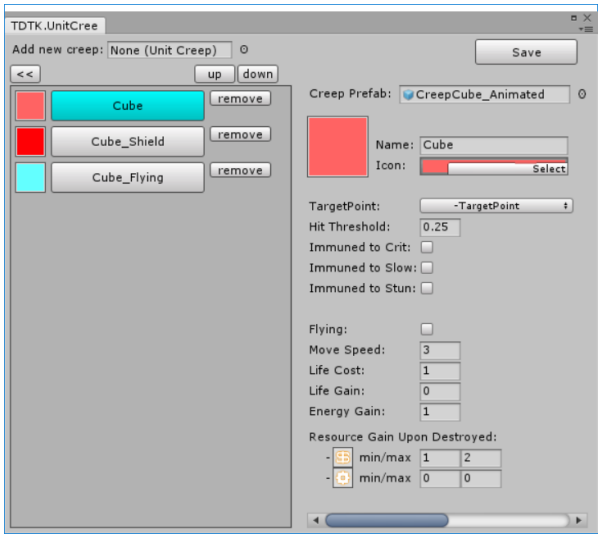

Figure 12. Two Types of Attacks in Original Tower Defense Toolkit

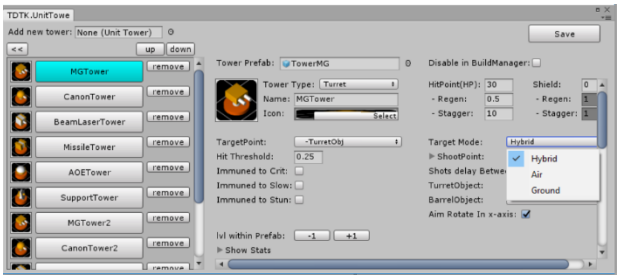

Figure 13. Three Types of Defense Towers in Original Tower Defense Toolkit

In order to solve this issue, the Tower Defense Toolkit was customized to include seven additional attack types, including Virus, Phishing, Trojan, Spyware, Ransomware, DDoS, and Sniffer (Figure. 14), and six additional defense towers, including Antivirus, Password, System Update, Secure Cyber Behavior, Encryption, and Firewall (Figure. 15).

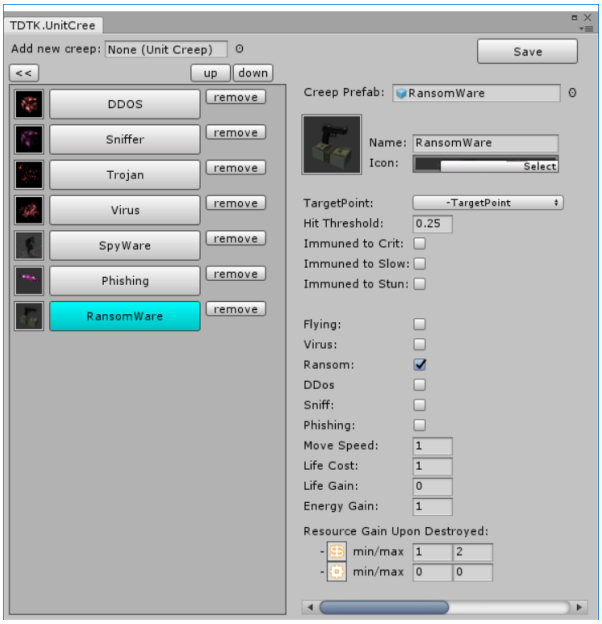

Figure 14. Additional Seven Cyber Attacks in Cyber Tower Defense Game

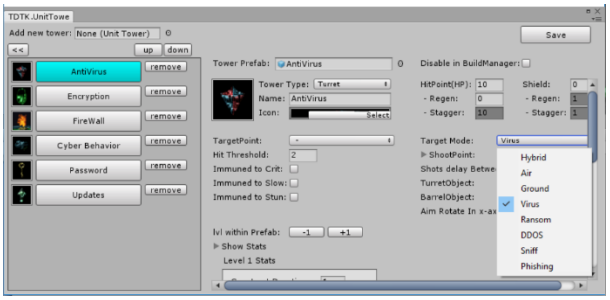

Figure 15. Six New Cyber Defense Towers in Cyber Tower Defense Game

Some defense towers will defend a 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 attacks. In addition, multiple defense towers can be used together, such as implementing the Password and Encryption towers against a Sniffer attack. The Cyber Defense Tower Game contains three difficulty levels: tutorial, intermediate, and competition. Figure 16 shows the tutorial level and Figure 17 shows the competition level to demonstrate the different levels of complexity.

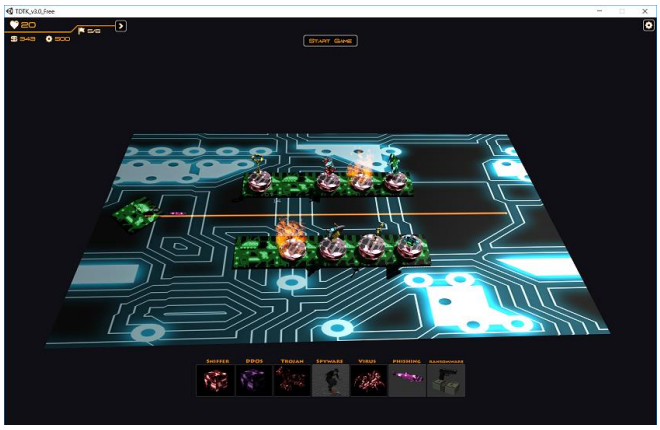

Figure 16. Tutorial Level in Cyber Tower Defense Game

Figure 17. Competition Level in Cyber Tower Defense Game

Single-player GenCyber Card Game

The original GenCyber card game was designed and created by Dr. Vincent Nestler at California State University at San Bernardino [14]. The single-player adaptation of the GenCyber Card game was developed in the Processing programming environment to enhance the students' understanding of ten cybersecurity First Principles (Figure. 18). The site team observed GenCyber camp participants playing the game during their down time, and some students were even creating "cheat sheets" so they could beat their friends' times.

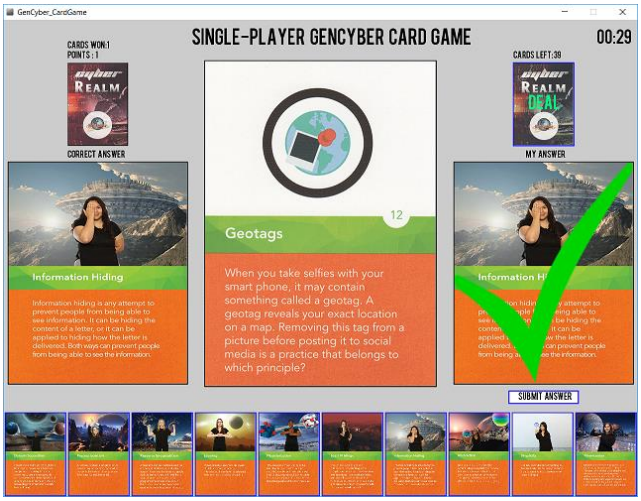

Figure 18. Single-player GenCyber Card Game

Comparison of Four Cybersecurity Games

Table 1 compares the four cybersecurity education games developed in this paper. The technical features of each game were compared based on game genres, dimension of game world, game development engine, 3D character modeling, 3D character animation, and game scripting.

Table 1. Comparison of Four Cybersecurity Games

	Social Engineering	**Secure Online Behavior**	**Cyber Defense Tower**	**GenCyber Card Game**
Game Genre	Role-Playing	Role-Playing	Tower-Defense	Card-Game
Game Dimension	3D	3D	3D	2D
Game Engine	Unity3D	Unity3D	Unity3D	Processing
Character Modeling	Required	Required	Not required	Not required
Character Animation	Required	Required	Not required	Not required
Game Scripting	C# script	C# script	C# script	Processing

Results and Discussions

Purdue University Northwest successfully launched two one-week summer camps in June 2016, and two additional one-week camps in June 2017. A total of 181 high school students attended the PNW GenCyber summer camps, with

107 of these from underrepresented minority populations as identified by the NSF report on "Women, Minorities, and Persons with Disabilities in Science and Engineering: 2017" [16] (Table 2).

Table 2. Demographic Information of PNW GenCyber Camp Participants

Year	Gender	Numer of participants	Race	Numer of participants
2016	Male	60	Caucasian	34
	Female	26	Non-Caucasian	52
2017	Male	63	Caucasian	40
	Female	32	Non-Caucasian	55
Total		181		181

During the one-week summer camp, each student participated in activities mentored by a team of PNW faculty members and student assistants. At the opening ceremony of the summer camp, the VR social engineering game was presented in the CAVE virtual environment. After the opening ceremony, each camp participant played this 3D social engineering game at his/her own pace to learn the concept of social engineering and get familiar with 3D game control. Once the students got used to the game controls and were exposed to the other games, they competed against one another for prizes and to promote a sense of fun and excitement in the classroom. After competing in groups of twenty-five students in each of the games – 3D Secure Online Behavior, Cyber Defense Tower, and Single-player GenCyber Card Games – one winner was picked from each competition and was awarded with a small gift on the last day of the summer camp.

The post-camp survey was conducted at the last day of the summer camp. A 5-point Likert scale was used to measure the students' satisfaction with camp activities and experiences ranging from 5 (strongly agree) to 1 (strongly disagree). The post-camp survey had 154 respondents (Table 3).

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	57	Caucasian	34
	Female	25	Non-Caucasian	48
Total		154		154

Survey participants indicated that game-based learning for cybersecurity enhanced knowledge in cybersecurity, understanding of the cybersecurity first principles, and general security awareness (Table 4). The activities and games also motivated students to pursue higher education and careers in the field of cybersecurity.

Table 4. Post-Camp Survey Questions and Results

Question	Post-Camp Survey Questions	Rating
Q1.	I enjoyed learning about computer science	4.36
Q2.	I would like to learn more about computer science	4.22
Q3.	I enjoyed learning about cybersecurity	4.27
Q4.	I would like to learn more about cybersecurity	4.05
Q5.	The teachers/faculty in this program made me more interested in cybersecurity	4.20
Q6.	I know what cybersecurity means	4.27
Q7.	I know more about cybersecurity than I did before this camp	4.36
Q8.	I know more about computer science than I did before this camp	4.26
Q9.	I am more comfortable learning cybersecurity concepts now	4.08
Q10.	I know more about information security than I did before this camp	4.29
Q11.	I can explain why cybersecurity is important	4.18
Q12.	Overall this camp was a good experience	4.46
Q13.	I am glad I attended this camp	4.46
Q14.	I would like to attend more camps like this	4.17
Q15.	My opinions and ideas were respected in this camp	4.32
Q16.	I found the camp activities interesting	4.22
Q17.	I liked interacting with the teachers at this camp	4.28

The mean scores of male and female students, as well as the difference in rating scores between various ethnic groups, indicated that there could be gender and racial difference in participants' evaluation of the game-based cybersecurity education method. 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, both a two-tail and one-tail hypothesis test were performed. For example, the hypothesis for "Q1. I enjoyed learning about computer science" was:

1. Two-tail hypothesis test

H0: There is no difference in mean survey rating of Q1 between female and male students ($\mu 1 = \mu 2$).

HA: There is difference in mean survey rating of Q1 between female and male students ($\mu 1 \neq \mu 2$).

Significance level (α)= 0.05

2. One-tail hypothesis test

H0: The mean survey rating of female students is higher than or equal to the male students ($\mu 1 \geq \mu 2$).

HA: The mean survey rating of female students is lower than the male students ($\mu 1 < \mu 2$).

Significance level (α)= 0.05

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

Table 5. Evaluation of the Gender Difference in Game-Based Learning for Cybersecurity Education

Quest #	Mean Female Rating (n = 47)	Mean Male Rating (n = 107)	p-value (two-tail test)	p-value (one-tail test)
Q1.	4.0851	4.4766	0.0072	0.0036
Q2.	4.0000	4.3178	0.0973	0.0486
Q3.	4.0638	4.3551	0.0903	0.0452
Q4.	3.9362	4.0935	0.4241	0.2121
Q5.	3.9787	4.2991	0.0587	0.0294
Q6.	4.1915	4.3084	0.4596	0.2298
Q7.	4.3191	4.3832	0.7309	0.3654
Q8.	4.1489	4.3084	0.4471	0.2235
Q9.	3.9149	4.1509	0.2053	0.1027
Q10.	4.2128	4.3178	0.5111	0.2556
Q11.	3.9574	4.2804	0.0745	0.0373
Q12.	4.3913	4.4951	0.4637	0.2319
Q13.	4.3043	4.5243	0.1899	0.0950
Q14.	4.0000	4.2524	0.2075	0.1037
Q15.	4.3043	4.3204	0.9125	0.4563
Q16.	3.9130	4.3592	0.0120	0.0060
Q17.	4.1957	4.3107	0.5073	0.2536

To test differences among ethnic groups, both two-tail and one-tail hypothesis tests were performed for Caucasian and non-Caucasian participants. The hypothesis for "Q1. I enjoyed learning about computer science" was:

1. Two-tail hypothesis test

H0: There is no difference in mean survey rating of Q1 between Caucasian and non-Caucasian students ($\mu 1 = \mu 2$).

HA: There is difference in mean survey rating of Q1 between Caucasian and non-Caucasian students ($\mu 1 \neq \mu 2$).

Significance level (α)= 0.05

2. One-tail hypothesis test

H0: The mean survey rating of non-Caucasian students is higher than or equal to the Caucasian students ($\mu 1 \geq \mu 2$).

HA: The mean survey rating of non-Caucasian students is lower than the Caucasian students ($\mu 1 < \mu 2$).

Significance level (α)= 0.05

The result of hypothesis testing between ethnic groups shows that there are no significant differences between Caucasian and non-Caucasian students regarding the camp activities and experiences. However, the one-tail hypothesis test indicates that the Caucasian students rated survey question 11 higher than non-Caucasian students (Table 6). This result shows that the Caucasian students have higher overall self-efficacy than non-Caucasian students do after the game-based learning camp activities.

Table 6. Evaluation of the Racial Difference in Game-Based Learning for Cybersecurity Education

Quest #	Caucasian Rating (n = 64)	Non-Caucasian Rating (n = 90)	p-value (two-tail test)	p-value (one-tail test)
Q1.	4.4063	4.3222	0.5007	0.2503
Q2.	4.2500	4.2000	0.7555	0.3777
Q3.	4.3594	4.2000	0.2573	0.1287
Q4.	4.1406	3.9778	0.3238	0.1619
Q5.	4.2188	4.1889	0.8393	0.4196
Q6.	4.3594	4.2111	0.2897	0.1448
Q7.	4.3594	4.3667	0.9639	0.4820
Q8.	4.1250	4.3556	0.1903	0.0951
Q9.	4.1429	4.0333	0.4924	0.2462
Q10.	4.2969	4.2778	0.9005	0.4502
Q11.	4.3438	4.0667	0.0694	0.0347
Q12.	4.5238	4.4186	0.3855	0.1928
Q13.	4.5397	4.3953	0.2745	0.1372
Q14.	4.2857	4.0930	0.2412	0.1206
Q15.	4.2857	4.3372	0.7344	0.3672
Q16.	4.2857	4.1744	0.4375	0.2187
Q17.	4.3016	4.2558	0.7724	0.3862

Prof. Zheng Yan and Prof. Melissa Dark conducted independent evaluation of GenCyber camp with support from the NSF EAGER grant, "Developing Cybersecurity Judgment Questionnaire for GenCyber Campers." All PNW camp participants were encouraged to participate in the "quiz"-style independent evaluation. However, due to the nature of the anonymous study, authors could not obtain the performance data from the PNW camp. From year 2018, PNW summer

camps will offer a knowledge assessment quiz both before and after the game-based learning sessions to further enhance understanding of student knowledge attainment.

Conclusion

This paper introduced an innovative game-based learning method for cybersecurity education. Four computer games were developed to educate social engineering and information security concepts, secure online behaviors, and cybersecurity first principles. These games provided an excellent platform to assist high school students in learning these important concepts, as well as differentiate between secure and unsecure online behaviors. This approach is beneficial to the future cybersecurity workforce as it exposes more high school students to cybersecurity as a career 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 with 154 participants, with average ratings of 4.26 out of 5 on all Likert-based responses. To investigate the gender and ethnic differences among participants, hypothesis testing for two population means with unequal variance (T-Test) was conducted with the survey data. The hypothesis testing results indicated that male students overall thought the game-based learning activities were more enjoyable and interesting than female students, and that Caucasian students showed slightly higher self-efficacy with cybersecurity concepts than non-Caucasian students after the game-based learning camp activities.

Acknowledgements

This research was supported by NSA/NSF grant H98230-17-1-2006 and NSF grant #1723666.

References

[1] Johnson, E., & Willey, N. (2011). Usability Failures and Healthcare Data Hemorrhages. *IEEE Security and Privacy*, 9(2), 18-25.

[2] Tu, M., & Spoa-Harty, K. (2015). Data Loss Prevention Management and Control: Inside Activity Monitoring, Identification, and Tracking in Healthcare Enterprise Environments. *Journal of Digital Forensics, Security, and Law*, 10(1), 27-44.

[3] Trautman, L. (2015) Cyberseurity: What about US policy? *Journal of Law, Technology and Policy*, 2015(2), 341-391. Retrieved August 30, 2017, from https://ssrn.com/abstract=2548561.

[4] A Frost and Sullivan Executive Briefing. (2017, June). Global Information Security Workforce Study. Retrieved August 27, 2017 from https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf.

[5] Cuny, J., & Hamos, J. (2011). NICE Cybersecurity in K-12 Formal Education. Retrieved August 25, 2017 from http://csrc.nist.gov/nice/Sept2011-workshop/presentations/Thursday/Thurs_Cuny_NICE_K-12_092211.pdf.

[6] Fitzpatrick, A. (2012, May 29). Cybersecurity experts needed to meet growing demand. *Washington Post*. Retrieved August 26, 2017, from https://www.washingtonpost.com/business/economy/cybersecurity-experts-needed-to-meet-growing-demand/2012/05/29/gJQAtev1yU_story.html?utm_term=.7ecd9d057621.

[7] Ladabouche, T., & LaFountain, S. (2016). GenCyber: Inspiring the Next Generation of Cyber Stars. *IEEE Security & Privacy*, 14(5), 84-86.

[8] Zweben, S. (2013). Computing Degree and Enrollment Trends. *2012-2013 CRA Taulbee Survey*. Retrieved August 26, 2017 from http://archive2.cra.org/uploads/documents/resources/taulbee/CRA_Taulbee_CS_Degrees_and_Enrollment_2012-13.pdf.

[9] Findley, M. (2011). The Relationship between Student Learning Styles and Motivation during Educational Video Game Play. *International Journal of Online Pedagogy and Course Design*, 1(3), 63-73.

[10] Kumar, A., Gupta, S., Rai, A., & Sinha, S. (2013). Social Networking Sites and Their Security Issues. *International Journal of Scientific and Research Publications*, 3(4), 1-5.

[11] Tang, S. & Hanneghan, M. (2010). A Model-Driven Framework to Support Development of Serious Games for Game based Learning. *The 3rd International Conference on Developments in e-Systems Engineering*, (pp. 95-100). London, UK.

[12] National Security Agency. (2017). What is the GenCyber program? Retrieved June 14, 2017. from https://www.gen-cyber.com/faq/.

[13] Reece, D. (2015). Best Tower Defense Games of All Time. *Gameranx: Top Rated Games, Reviews and News*. Retrieved May 6, 2017 from http://gameranx.com/features/id/13529/article/best-tower-defense-games/.

[14] Nestler, V. (2016). Cyber Realm. [Card game]. Retrieved May 25, 2017 from http://gencybercards.com/.

[15] Tan, S. (2016). Tower Defense ToolKit (TDTK). [Software library]. Retrieved May 12, 2017 from: https://www.songgamedev.com/tdtk.

[16] National Science Foundation, National Center for Science and Engineering Statistics. (2017). *Women, Minorities, and Persons with Disabilities in Science and Engineering: 2017*. Special Report NSF 17-310.

Arlington, VA. Retrieved February 11, 2018 from: www.nsf.gov/statistics/wmpd/.

Biographies

GE JIN is 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. Jin may be reached at ge.jin@pnw.edu

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. Tu may be reached at manghui.tu@pnw.edu

TAE-HOON KIM is 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. Dr. Kim may be reached at tae-hoon.kim@pnw.edu

JUSTIN 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. Heffron may be reached at jheffron@pnw.edu

JONATHAN WHITE is currently a STEM educator. He received B.S. degree in Computer Graphics Technology from Purdue University Northwest. Mr. White may be reached at white341@pnw.edu

ANASTASIA TREKLES is a clinical associate professor in the School of Education and Counseling at Purdue University Northwest. Dr. Trekles has an extensive background with educational technology, including design and pedagogical strategies as well as the effective integration of various technologies into teaching. Among other service activities, she has served on the Indiana Connected Educators (ICE) Board of Directors since 2008, and presents regularly at conferences such as the International Society for Technology in Education (ISTE). Her specialty area is instructional design for online learning and technology integration, and in addition to providing professional development and mentorship for other faculty, she has taught a wide array of undergraduate- and graduate-level courses in these areas, both in-classroom and via distance education. Dr. Trekles may be reached at atrekles@pnw.edu