PNW GenCyber Summer Camp: Game based Cybersecurity Education for High School Students

Dr. Ge Jin, Purdue University Northwest

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.

Michael Tu, Purdue University Northwest

Michael Tu, Ph.D. in Computer Science, 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 is a Certified Ethical Hacker (CEH), Certified Pen Tester (CPT), Certified Hacking and Forensics Investigator (CHFI), & AccessData Computer Examiner (ACE).

Prof. Tae-Hoon Kim, Purdue University Northwest
Mr. Justin David Heffron, Purdue University Northwest
Mr. Jonathan Kakahiaka White

PNW GenCyber Summer Camp: Game based Cybersecurity Education for High School Students

Ge Jin[1], Manghui Tu[2], Tae-Hoon Kim[3], Justin Heffron[4], and Jonathan White[5]

1-5 Department of Computer Information Technology and Graphics, Purdue University Northwest

Abstract

Cybersecurity is critical to the national infrastructure, government, military and industry. To defend the U.S. against the cyber threats, a significant demand for skilled cybersecurity workforce is predicted in government and industrial sectors. To address this issue, Purdue University Northwest has successfully launched four GenCyber summer camps for 181 high school students in Chicago metropolitan area to stimulate the high school students' interest in the cybersecurity field and raise their awareness of cybersecurity and safe online behavior. PNW GenCyber summer camp activities were delivered in the format of game based learning and hands-on labs. The use of game-based learning in the camp was an excellent platform to teach concepts of cyber security principles. Game based learning provided an immersive, learner-centered experience to high school students, which has been proven to be very effective on cybersecurity awareness training and practical skill acquisition for learners from diverse backgrounds.

Keywords

Game based learning, Cybersecurity.

Introduction

With the recent high profile cybersecurity incidents, 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 sector. Over the past few years, millions of sensitive data records have been compromised and a large number of frauds have been committed, 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].

Cybersecurity workforce development is the key to assuring that the 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]. 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. The U.S. Congress has urged that it is critical to develop high-quality educators to expand cyber education at early age [5]. To increase K-12 students' interest in cybersecurity and the diversity of cybersecurity workforce, 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[6].

PNW GenCyber camp developed an innovative game based cybersecurity education modules to provide hands-on learning activities for the high school students. We developed virtual reality (VR) 3D games, robotic programming games, and practical ethical hacking and cyber forensics labs for high school cybersecurity summer camps. 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. The innovative pedagogical methods and age appropriate game based learning curriculum, have made cybersecurity concepts more accessible to students of varying ability levels. This was supported by the post camp survey conducted for 154 participants.

Related works

Research indicates that students receiving computer education in high school are 8 times more likely to major in a computer degree, while in the last 20 years, enrollment in computer education courses has seen a dramatic decrease at the high school level[7]. In addition, student participation is unrepresentative of 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. 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 learn only 20% of what they hear and read, but can learn 90% of what they have practiced[8]. The advance of technologies, high-speed connections, and the pervasiveness of mobile devices, have enabled various computer based pedagogical methods. One of the most emergent and rapidly mutating forms of computer-based learning is "game based learning.” As its name suggests, computer game allows learners to be immersed in an artificial or simulated game environment while experiencing it as real. Game based learning include virtual reality games, web-based games, multi-user virtual environments (MUVEs), massively multiplayer online games, and simulations[9]. Till date, applying game based learning instructional method to cybersecurity education is limited[10].

Methodology

The primary goals of NSA/NSF GenCyber program 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. As described in the introduction section, PNW GenCyber camp recruited 51.3% of underrepresented minority high school students, and met the goal of increasing diversity of summer camp participants.

To raise general awareness of cybersecurity and safe online behavior of high school students and increase their interest in cyber security, we developed game based cyber security learning modules to meet the GenCyber program goals.

The topics of cybersecurity education games were selected in the following areas:

- Social engineering and information security: 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.

- 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.

- 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[11]. 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.

- 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.

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.

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.

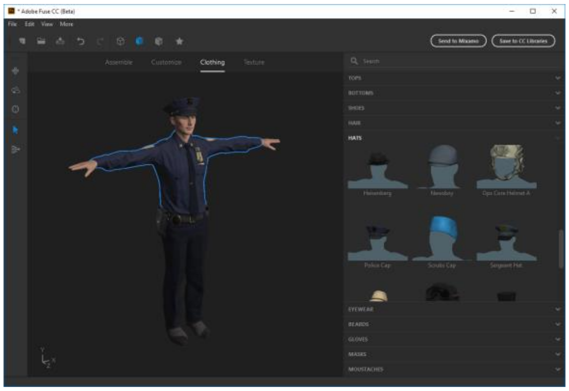


Figure 1 Left: Character Modeling in Adobe Fuse

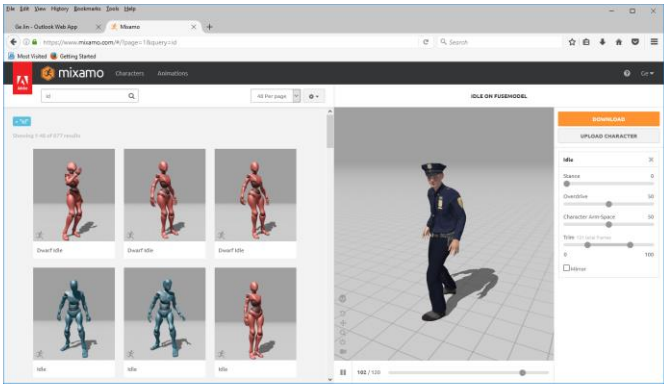
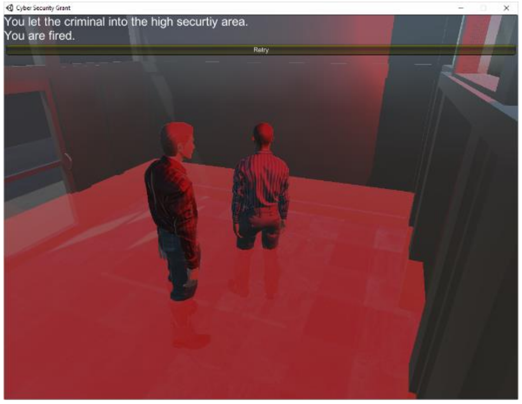


Figure 1 Right: Character Animation in Mixamo

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. The flowing figures were captured from social engineering game and secure online behavior game.



You let the criminal into the high securtiy area.
You are fired.

Figure 3 Left: 3D Social Engineering Game

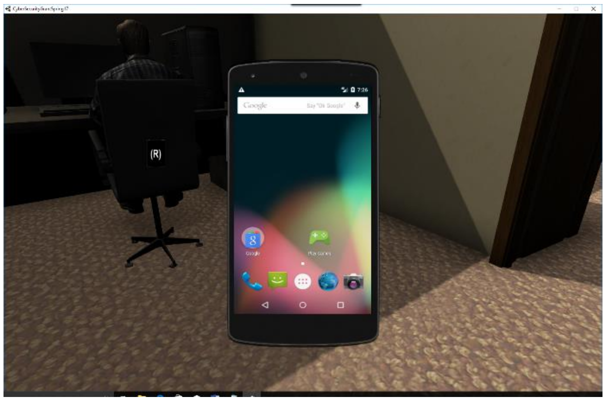


Figure 3 Right: 3D Secure Online Behavior Game

Development of Cyber Defense Tower Game in Unity3D

The cyber defense tower game was implemented on top of Tower Defense Toolkit (TDTK) developed by Song Tan[12]. 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 designed custom models and art assets, and user can integrate their own art assets to make unique Tower Defense game. We have created 7 unique cyber-attacks (Figure 4) and 6 cyber defense towers (Figure 5).

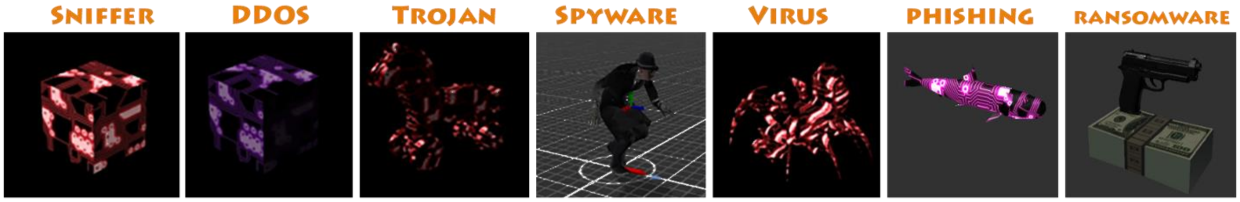


Figure 4: Seven Cyber-Attacks in Cyber Defense Tower Game

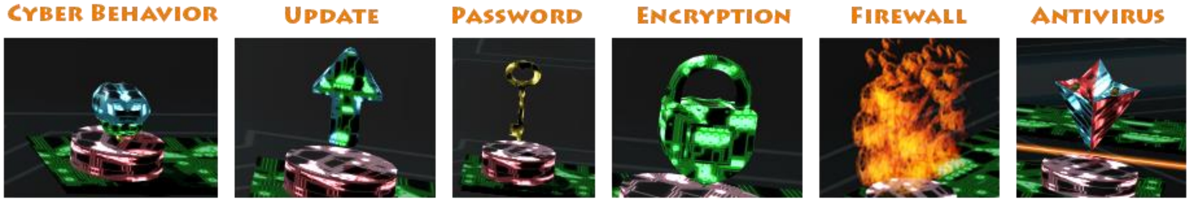


Figure 5: Six Defense Towers in Cyber Defense Tower Game

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. Figure 7 left is the tutorial level and right is the competition level.

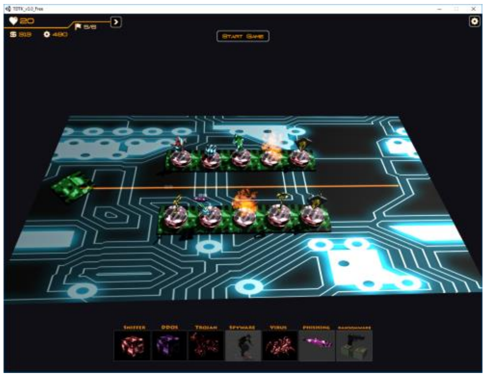


Figure 7 Left: Tutorial Level in Tower Defense Game

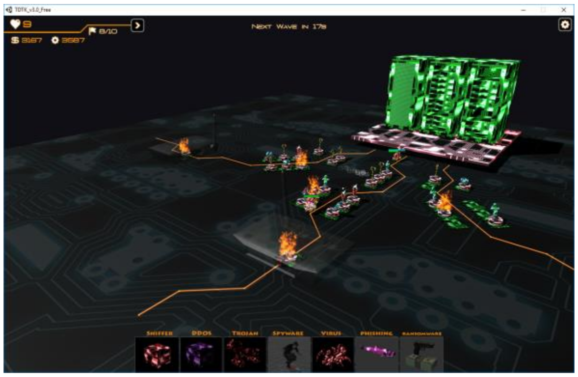


Figure 7 Right: Competition Level in Tower Defense Game

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[13]. 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.

Results

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 summer camps with 93 students (51.3%) were underrepresented minority students. During the summer camp, the students were exposed to cybersecurity first principles and cybersecurity awareness by playing various cyber security computer games during the first two days. Each class has about 25 students and they 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. The post-camp survey of camp participants 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. One challenge that we encountered during the Unity3D game programming lesson is teaching the concept of object oriented paradigm and event driven programming. To maintain the student's interest, instructors provided partial C# script file and students were asked to fill in the variables and complete one or two event function following sample script code.

Table 1: Post-Camp Survey Questions and Results

Survey Questions	Score (1 to 5)
1. I enjoyed learning about computer science	4.36
2. I would like to learn more about computer science	4.22
3. I enjoyed learning about cybersecurity	4.27
4. I would like to learn more about cybersecurity	4.05
5. The teachers/faculty in this program made me more interested in cybersecurity	4.20
6. I know what cybersecurity means	4.27
7. I know more about cybersecurity than I did before this camp	4.36
8. I know more about computer science than I did before this camp	4.26
9. I am more comfortable learning cybersecurity concepts now	4.08
10. I know more about information security than I did before this camp	4.29
11. I can explain why cybersecurity is important	4.18
12. Overall this camp was a good experience	4.46
13. I am glad I attended this camp	4.46
14. I would like to attend more camps like this	4.17
15. My opinions and ideas were respected in this camp	4.32
16. I found the camp activities interesting	4.22
17. I liked interacting with the teachers at this camp	4.28

Conclusions

In this paper, we introduced an innovative game based learning method for cybersecurity education. Four computer games were developed to educate social engineering and information security concept, secure online behaviors and cybersecurity first principles. The use of game-based learning in the PNW GenCyber camp was an excellent platform to teach concepts of cybersecurity principles and secure online behaviors. 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.

References

1 Eric Johnson and Nicholas Willey. Usability failures and healthcare data hemorrhages. IEEE Security and Privacy. Issue March/April 2011, pp. 18-25.

2 Manghui Tu and Kimberly 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, Issue 1. 2015. Pp. 27-44.

3 Lawrence Trautman. Cyberseurity: what about US policy? 2015. [online] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2548561.

4 A Frost & Sullivan Executive Briefing. Global Information Security Workforce Study. 2017. [online] https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf.

5 Jan Cuny and Jim Hamos. NICE cybersecurity in K-12 formal education. 2011 [online] http://csrc.nist.gov/nice/Sept2011-workshop/presentations/Thursday/Thurs_Cuny_NICE_K-12_092211.pdf

6 Tina Ladabouche and Steve LaFountain. GenCyber: Inspiring the Next Generation of Cyber Stars. IEEE Security & Privacy. Volume: 14, Issue: 5, 2016. pp. 84-86.

7 Stuart Zweben. Computing Degree and Enrollment Trends, from the 2012-2013 CRA Taulbee Survey. 2013. [online] http://www.cra.org/.

8 Michael Findley. 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. 2011.

9 Abhishek Kumar, Subham Gupta, Animesh Rai, and Sapna Sinha. Social networking sites and their security issues. International Journal of Scientific and Research Publications, 2013. Vol. 3, No. 4. pp. 1-5.

10 Stephen Tang and Martin 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, UK. 2010.

11 Damon Reece. Best Tower Defense Games of All Time. 2015. [online] http://gameranx.com/features/id/13529/article/best-tower-defense-games/.

12 Song Tan. Tower Defense ToolKit (TDTK). 2016. [online] https://www.songgamedev.com/tdtk.

13 Vincent Nestler. Cyber Realm. 2016. [online] http://gencybercards.com/.

Ge Jin

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.

Manghui Tu

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.

Tae-Hoon Kim

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.

Justin Heffron

Mr. 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.

Jonathan White

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