

Learn Access Control Concepts in a Game

Patrickson Weanquoi¹, Jinghua Zhang¹, Xiaohong Yuan², Jinsheng Xu², Elva J. Jones¹

¹Department of Computer Science
Winston-Salem State University
Winston-Salem, NC, USA
{zhangji, jones}@wssu.edu

²Department of Computer Science
North Carolina A&T State University
Greensboro, NC, USA
{xhyuan, jxu}@ncat.edu

Abstract— This Innovative Practice Full Paper presents a new way to teach Access Control concepts. Access Control is a key component in computer security, and it is critical for students to have basic understanding of access control techniques. We have developed a 2D educational game, titled "*Temple of Treasures*," that aims to help students learn the basic concepts of Discretionary Access Control and Mandatory Access Control. The game was developed using the Unity game engine. The game's story is centered around an adventurer in search of gold but end up stuck in a temple and must gain knowledge on targeted concepts to unlock the doors along the escape pathways. Students must complete an in-game assessment with immediate feedback after each of the three levels in this game. Player information and assessment data are saved on the cloud through GameSparks for further analysis. To measure the effectiveness, we developed a pre-survey, post-survey, and focus group protocols. In addition, the UI Accessibility Plugin is used to make the game accessible to visually impaired players. The game has been integrated into several computer science courses including Operating Systems at North Carolina Agricultural and Technical State University, System Administration II and Introduction to Information Security at Winston-Salem State University. The game was deployed to a WebGL format so students can play it online. In this paper, we will present game design, development, and assessment results in detail.

Keywords—Security and privacy, Educational game, Access Control; Discretionary Access Control, Mandatory Access Control

I. INTRODUCTION

Access control is a protection mechanism that is used to mitigate malicious access to sensitive information in computer systems. There are four types of access control models: Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control, and Rule-Based Access Control. With DAC, the owner has complete control of the file/directory's security level. MAC is an access control method where the system uses security labels to restrict subjects' access to objects. In this paper, we focus on DAC and MAC in the *Temple of Treasures* game.

Games have been successfully used in many areas of education to engage students in learning [3, 11]. Research shows multiple benefits of cyber security games [10, 13]. Games can provide educational and immersive experiences, which will inspire students to explore more in the security field and help students test their knowledge in authentic settings.

Many games have been used to teach cyber security concepts [1-2, 5-8, 12, 14-15]. Zhang et al. [15] developed a web-based interactive visualization tool to help students gain a deeper understanding of buffer overflow concepts using the Unity game engine. Students will play space shooter game between learning components of the visualization tool. The *Temple of Treasures* game presented in this paper integrates learning of DAC and MAC into a game story of searching for treasures. The CyberCIEGE video game [7] provides several scenarios in which players play the role of a decision maker for some enterprise and make trade off while trying to maintain a balance between budget, productivity, and security. CyberCIEGE includes the concept of access control mechanisms. The *Temple of Treasure game* focuses on DAC and MAC, and uses a typical entertaining game environment (treasure hunt) to make the learning experience fun and engaging.

The *Temple of Treasure* game has four learning objectives:

- 1) Be able to explain read/write/execute permissions of files.
- 2) Be able to use Linux commands to change file permissions.
- 3) Be able to explain/modify the access control list of a file
- 4) Be able to explain the basic concepts of MAC.

Research shows that in-game assessments can increase the students' engagement level [9]. Therefore, the game also includes built-in assessment components. To evaluate the impact of this game on students' learning, we developed in-game assessments, a pre-survey, a post-survey and focus group protocols. Students will complete an in-game assessment after each of the three levels for immediate assessment and learning feedback. This online game has been integrated into several classes at North Carolina Agricultural and Technical State University (NC A&T) and Winston-Salem State University (WSSU) since spring 2020. The classroom experience reports and focus group discussions show that this game improved students' understanding of access control concepts.

This paper is organized as follows: Section II provides game design and development in detail, Section III presents the detailed assessment results, and Section IV describes the conclusion and future work.

II. GAME DESIGN AND DEVELOPMENT

The game titled *Temple of Treasures* was developed using the Unity game engine and can be deployed to multiple platforms. It has three levels, and the game's story is centered around a group of adventurers in search of gold but end up stuck in a temple and must gain knowledge on targeted concepts to unlock the doors along the escape pathways. Currently, this game was built to the WebGL format and is also accessible to visually impaired players shown in Fig.1. Students can play it online at <https://gamelab.wssu.edu/modules.htm>. To collect and analyze the player data, we used GameSparks [4] to record player profile/data on the cloud, set up analytics dashboard, manage player registration and validation as shown in Fig.1, and create the leaderboards. In addition, we implemented the level control that allows the player to restart the level instead of restarting the game when necessary.

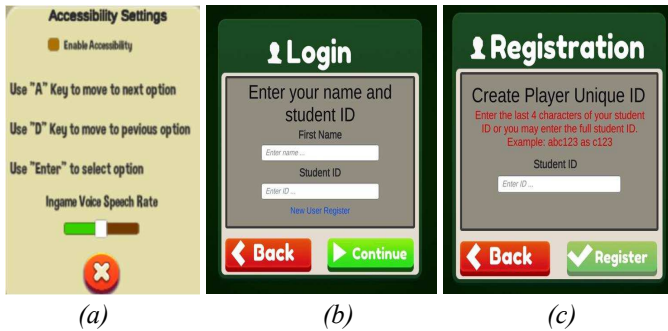


Fig. 1 (a) Accessibility Settings (b) Login (c) Registration

A. Level One - Linux File Mode

The level one aims to help students understand Linux File Mode. The player will learn how to use the `chmod` command to change file permissions in the Linux environment. Fig. 2 shows the environment of this level that has two gates. To pass this level, the player must open the Northgate. The Westgate prevents the player from accessing the treasure chest which contains the required script for unlocking the Northgate.

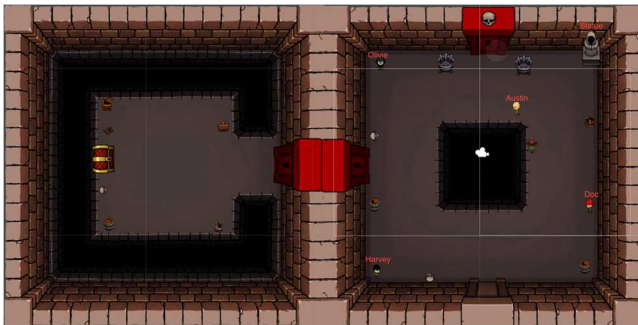


Fig. 2 Level One Environment

This level has a learning section and a challenge section. The concepts to be learned are structured as tasks shown in Fig.3. Each task is activated by a selective Non-Playing Character (NPC). For instance, the Read task is taught by Austin while the Write task is taught by Harvey. The terminal on the right of the panel is used to practice/run Linux

commands. The ultimate reward for manipulating a script is to open a gate; therefore, it requires having possession of a script to control the corresponding gate. Furthermore, each gate's script is discretionarily granted by the owner of the script, thereby establishing the concept of DAC. The commands taught within the Learning Section include `ls`, `cat`, `chmod` and `echo`. The player is provided with a step-by-step explanation of the command being taught. Each time the player learns a particular command, the player is forced to practice that command as shown in Fig. 3.

The next tab within the statue is the challenges section. The challenges section panel is designed to assess the player's understanding of the information learned from the learning section and holds two scripts, `westgate.sh` and `northgate.sh`, which are essential to opening the gates. Each gate can be locked/unlocked by modifying its corresponding script. Fig. 4 shows the Northgate and Westgate scripts on the left and the terminal on the right. To unlock a gate, the player needs to add permissions to the corresponding script so they can read the content of the script, append/write code to the script, and execute the script to open the gate.



Fig. 3 Learning Section Panel

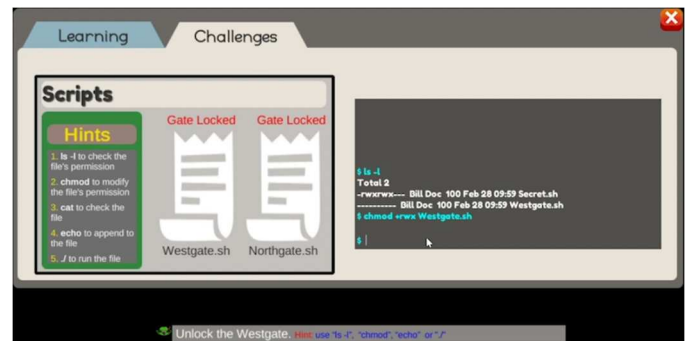


Fig. 4 Challenges Section Panel

Once the Northgate is unlocked, the player will enter a mandatory assessment (Quiz #1) stage. This stage includes an in-game assessment to test the player's knowledge of the targeted concept learned at this level. Fig. 5 shows the sample quiz question and sample feedback which is given immediately after submitting the quiz.

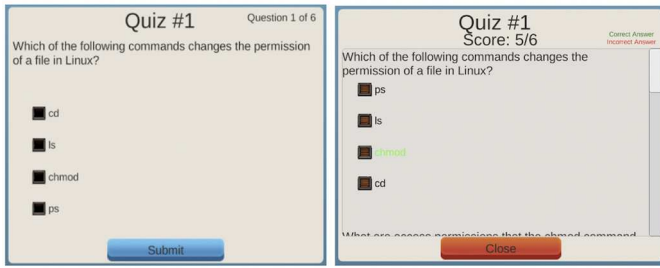


Fig. 5 In-Game Assessment (Quiz #1)

B. Level Two - Access Control List

This level teaches Access Control List (ACL) concepts. Students will learn how to use `setfacl` and `getfacl` commands to read/set ACL of a file.

This level has two rooms, as shown in Fig. 6. In the room on the left, the player is introduced to an antagonist named Jasper, a friend of Bill Doc, who has partially explored the temple and he was able to obtain access to the temple's final exit gate. However, he exited through the red gate without telling Doc and his colleagues how to exit the temple. Doc asked the player to chase after Jasper to retrieve the key. First, the player must obtain access to the red gate. To do so, the player must receive the key in the room on the right and give it to the gatekeeper.

The room on the right is designed to illustrate the concepts of ACL and has two obstacles: levers and an ACL minigame. The player must visit three levers before talking to Sheldon, who has ownership of the file needed by the gatekeeper. Each lever provides some key points of ACL which are essential to win the second obstacle-ACL minigame. After the player talks to Sheldon, the red statue in the corner will appear, where the player can learn more concepts and play the minigame.

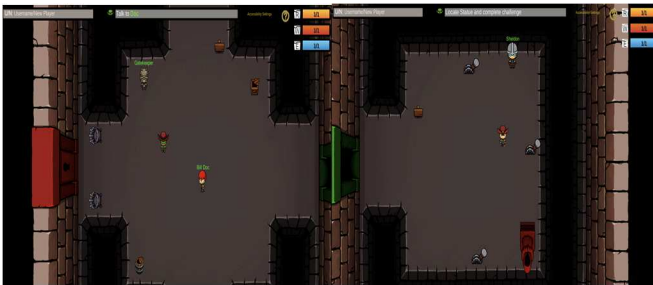


Fig. 6 Level Two Environment

The minigame has two parts: concept learning and practicing through game play. The player learns how to get/set the ACL of a file using the `getfacl` and `setfacl` commands as shown in Fig. 7. The player will practice the ACL commands through the game play shown in Fig. 8 and needs to protect a file within the limited time frame without granting more than three invalid accesses to the requesters. Essentially, for any request (read, write, or execute) to a file, the player can perform three actions: deny, grant, and modify access. The buttons on the left in Fig. 8 show those options. The access grant and deny buttons are below the terminal while the list of requesters requiring access modification are located within the

Modify Access panel. After completing the minigame, the player can add the gatekeeper to the ACL of `key.sh` as shown in Fig. 9. If everything is done correctly, the player completes the level successfully as shown in Fig. 10. The in-game assessment for this level will be presented before the player enters the next level.

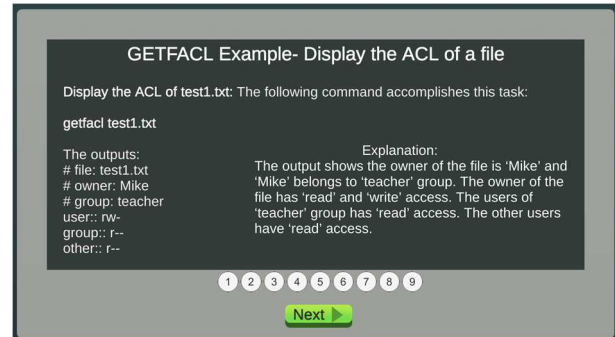


Fig. 7 Concept Learning Part

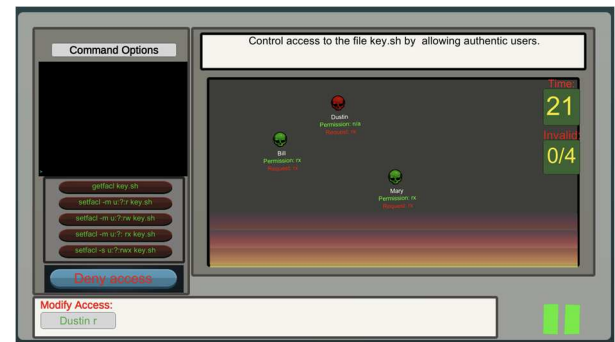


Fig. 8 Minigame window

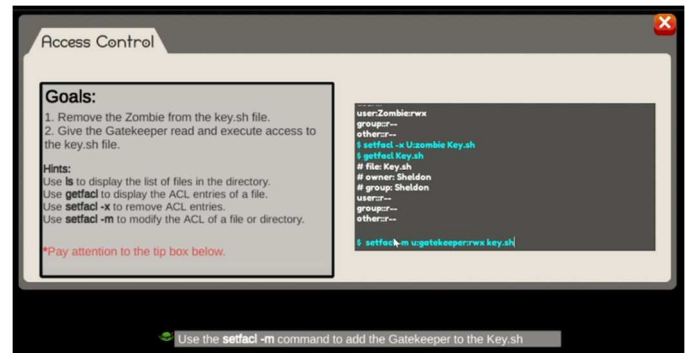


Fig. 9 Adding the Gatekeeper to the ACL of `key.sh`



Fig. 10 Level Two-Congratulations Page

C. Level Three - Mandatory Access Control

This level is where Jasper resides. It only has one room shown in Fig. 11. Jasper informed the player that he must understand some SELinux commands such as `getenforce`, `setenforce`, `sestatus`, `chcon`, `semanage` and `restorecon` to exit the temple. The player will learn the basic MAC concepts through collecting the hints and examples in the learning station as shown in Fig. 10. This level has a minigame as well. Given a real-world scenario, the player must make the right decision for each task within the time limit and arrows on-hand. If the player fails, they must complete a secondary task in the terminal to reset the game. Upon successfully completing the minigame, the player will be able to escape the temple with his friends. When the game ends, the player can check the leader board to see the scores and names of the top ten players as shown in Fig. 14.



Fig. 11 Level Three Environment

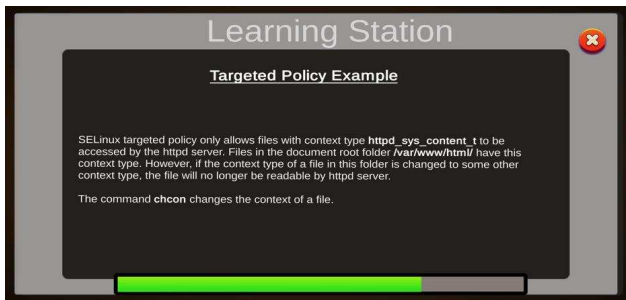


Fig. 12 Level Three-Learning Station

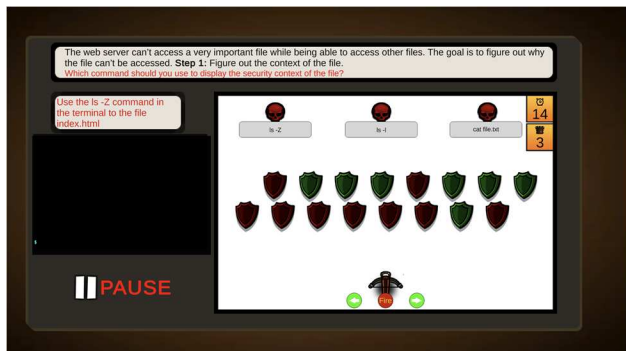
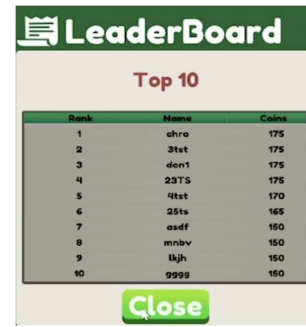


Fig. 13 MAC-Minigame



Rank	Name	Coins
1	shiro	175
2	31st	175
3	don1	175
4	23TS	175
5	41st	170
6	25ts	165
7	asdf	150
8	mnbv	150
9	lkjh	150
10	9999	150

Fig. 14 Game Leader Board

III. CLASSROOM EXPERIENCE REPORT

Since spring 2020, this online game has been used in several classes. The full game has been used in the Operating Systems class at NC A&T and the Introduction to Information Security class at WSSU. The first level of the game was used in System Administration II at WSSU.

The pre-survey and post-survey were conducted to learn about students' experience on cybersecurity before and after the access control game. Fifty-three students participated in the pre-survey while forty-one students filled out the post-survey after the completion of the game. The same set of questions is utilized for the pre-test and post-test. The pre-test and post-test are included in the pre-survey and post-survey respectively. In the pre-survey, 65% out of fifty-three students were male and 35% were female. 82% of students are self-identified as Black or African American. All the students were either a junior or senior.

In the Operating Systems class at NC A&T, students did all activities as homework assignments. Students were given three weeks to complete the assignment. They were asked to first complete a pre-survey, watch the game demo, then play the game, and fill out a post survey after the game. In previous semesters before the *Temple of Treasures* game was introduced to the Operating Systems class, the topic of access control was taught through lectures and reading. At WSSU, students completed the pre-survey, game, and post-survey in one sitting as an in-class activity. The game developers were able to help students through Zoom during the class session. It took students about an hour to complete all activities. The survey data from both the operating systems class and the Introduction to Information Security class were merged together for analysis.

A. Survey Analysis

Fifty-three students took the pre-survey. According to the pre-survey, 12% of students have taken cybersecurity courses or formal training. Some of the courses taken are Network Security, Operating Systems and Fundamental of Cyber Security. 4% of students read cybersecurity-related newsletters or articles very frequently.

Forty-one students filled out the post-survey after the completion of the game. The students were asked to rank their agreements on a list of statements on a 5-point Likert scale

(where 5 means strongly agree, and 1 means strongly disagree) on their motivation and experience in learning with the access control game. The detailed results are presented in Table 1.

Table 1. Motivation/Experience in Learning with the game module

Statement	Strongly Agree/Agree
I am interested in learning about the topic of access control.	65%
The Access Control game engaged me in learning this topic.	83%
I enjoyed the learning experience with the Access Control game.	65%
I think the learning experience with the Access Control game is effective.	85%
I am satisfied with the level of effort the Access Control game requires for learning this topic.	85%
I wish more cyber security topics will be taught using games.	75%

According to the learning objectives analysis, 75% of students strongly agree or agree that the learning objectives of the access control game are met. Before using this game, students were asked to self-rank their knowledge related to the learning objectives of the game. They were asked to self-rank again on the post-survey. Table 2 shows the students' self-ranking of the learning objectives in the pre- and post- survey. Clearly, the game helped students learn access control concepts.

Table 2. Pre- vs. Post- Survey on Student Learning Objectives

Statement	Pre-survey Result	Post-survey Result
Explain read/write/execute permissions of files.	16%	65%
Use 'chmod' command to change file permissions.	8%	68%
Use Linux commands: 'ls', 'cat'	23%	70%
Explain the basic concept of MAC.	4%	43%
Know basic SELinux commands: ls -Z, sestatus, chcon, restorecon, and semanage.	2%	40%
Apply basic SELinux commands to set context type of files or folders	4%	43%
Explain the access control list of a file with getfacl command	2%	60%
Modify the access control list of a file with setfacl command.	4%	53%

The same questions were used in the pre-quiz and post-quiz as shown in Table 3 along with the pre-quiz and post-quiz results. They are included in the pre-survey and post-survey respectively. Students performed significantly better in the post-quiz.

In the System Administration II class, ten students did the pre-survey and played the first level of the game. Seven students completed the post-survey. Only question #5 in Table 3 is related to the first level so it was used in the pre-test and post-test. Only one student answered incorrectly in both quizzes. All students who took the post-survey think that the

learning experience with the game is effective and that the learning objectives of the game are met.

Table 3. Pre-quiz/Post-quiz Questions and Results

Pre-Quiz/Post-Quiz Questions	Pre-Quiz Percentage	Post-Quiz Percentage
1. In which of the access control methods, the access is decided by the owner of the file? a) Mandatory Access Control (MAC) b) Discretionary Access Control (DAC)	81%	76%
2. which of the following commands changes the Access Control List of a file in Linux? a) chcon b) setfacl c) chmod d) sestatus	40%	61%
3. In which of the following access control methods, the access is decided by the system wide rules or policy? a) Mandatory Access Control (MAC) b) Discretionary Access Control (DAC)	79%	81%
4. Which of the following commands is specific to SELinux module? a) chcon b) setfacl c) chmod d) getfacl	28%	59%
5. Which of the following is the best command that make your file readable to all users in Linux? a) chcon b) setfacl c) chmod d) getfacl	34%	66%

B. Focus Group Discussion

Thirty-five students participated in this focused group discussion after using the game at NC A&T. Collectively, they were asked a series of questions regarding the game and their experience playing it. From the focus group discussions, there were some points that emerged, presented here:

- The students had a good experience with the learning game.
- Students found that learning about something is easier when it is in visual format.
- The students liked the game and the concept of using games for learning.
- The game works well easing the player into using these commands and understanding the concepts in depth.
- The game play and the graphical elements used were interesting.
- The game was good in terms of learning Linux commands.
- The game was also entertaining with the storyline and useful information.
- The game taught the concept of software development including the frontend and backend.
- All the Linux commands used in the game seem to be useful.

- Each of the challenges during the gameplay taught different commands.
- Best features of the game: Storyline, Graphical user interface, Game characters and Linux commands.

Improvements suggested by the students include:

- A pre-learning hands-on would be useful prior to the game play to understand the objectives of the game.
- Color coding would be helpful to visualize technical terms like commands, arguments, filenames etc.
- Accessibility settings and the help icon in the game should be clearly visible.

IV. CONCLUSIONS AND FUTURE WORK

The “*Temple of Treasures*” game is designed to help students learn basic concepts of access control in a fun environment. The game is built to the WebGL format and made available online. Additionally, it is accessible to visually impaired players. Through the integration of GameSparks IDE, we can continuously collect and analyze player data to improve user experience and ensure the quality of the game.

Based on the initial assessments, students enjoyed this type of learning compared to the traditional lectures. According to the survey, 75% of the students agreed that the learning objectives of the access control game were met. We will refine this game based on the feedback from the instructors and students, revise the structure of the minigame in level two to improve the completion rate, and run more extensive testing to ensure the best possible quality is delivered to all players. Additionally, we will conduct comparative assessments by setting up a control group and an experimental group. The control group will be taught using the traditional lecture teaching method and the experimental group will be taught using this game.

ACKNOWLEDGEMENTS

This work is supported by NSF under the grant DUE-1821960 and 1821965. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of NSF.

REFERENCES

- [1] Compte, A. L., Elizondo D., and Watson, T. (2015) "A Renewed Approach to Serious Games for Cyber Security", *Proceedings of the 7th International Conference on Cyber Conflict: Architectures in Cyberspace*: 203-16, 2015.
- [2] Cullinane, I., Huang, C., Sharkey, T. and Moussavi, S. (2015) "Cyber security education through gaming cybersecurity games can be interactive, fun, educational and engaging" *J. Comput. Sci. Coll.* 30, 6. June 2015, pp. 75-81.
- [3] Eagle, M., Barnes, T., "Wu's castle: teaching arrays and loops in a game", *Proceedings of the 13th annual conference on Innovation and technology in computer science education*, June 30-July 02, 2008, Madrid, Spain
- [4] GameSparks, <https://www.gamesparks.com/>.
- [5] Guimaraes, M., Said, H. and Austin, R. "Using Video Games to Teach Security." *Proceedings of the 16th Annual Joint Conference on Innovation and Technology in Computer Science Education - ITiCSE '11*(2011): 346.
- [6] Herr, C. and Dennis, A. (2015) "Video Games as a Training Tool to Prepare the Next Generation of Cyber Warriors", *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research - SIGMIS-CPR '15*, Newport Beach, CA, 2015.
- [7] Irvine, C., Thompson, M. and Allen, K., "CyberCIEGE: Gaming for Information Assurance", *IEEE Security & Privacy*, vol. 3, no. 3, 2005, pp. 61–64
- [8] Jordan, C., Knapp, M., Mitchell, D., Claypool, M. and Fisler, K. "CounterMeasures: A Game for Teaching Computer Security." 2011 10th Annual Workshop on Network and Systems Support for Games.
- [9] Lee, M., Ko, A. and Kwan, I. (2013), "In-game Assessments Increase Novice Programmers' Engagement and Level Completion Speed," In *Proceedings of the Ninth Annual International ACM Conference on International Computing Education Research (ICER '13)*. ACM, New York, NY, USA, 153–160.
- [10] Pusey, P., Tobey, D. and Soule, R., "An Argument for Game Balance Improving Student Engagement by Matching Difficulty Level with Learner Readiness ". In 2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14). USENIX Association, San Diego, CA
- [11] Repenning, A., Ioannidou, A., "Broadening participation through scalable game design ", *ACM SIGCSE Bulletin*, v.40 n.1, March 2008
- [12] Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L.F., Hong, J. and Nunge, E., "Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish, " *Symposium on Usable Privacy and Security (SOUPS)*, 2007.
- [13] Tobey, D. H., Pusey, P. and Burley, D. L., *Engaging Learners in Cybersecurity Careers: Lessons from the Launch of the National Cyber League*. *ACM Inroads* 5, 1 (2014), 53–56.
- [14] Williams, L., Meneely, A. and Shipley, G., "Protection Poker: The New Software Security 'Game', " *IEEE Security & Privacy*, vol. 8, no. 3, 2010, pp. 14–20.
- [15] Zhang, J., Yuan, X., Johnson, J., Xu, J., Vanamala, M., "Developing and Assessing a Web-Based Interactive Visualization Tool to Teach Buffer Overflow Concepts", *FIE 2020*, October 21-24, Uppsala, Sweden.