ASEE 2022 ANNUAL CONFERENCE
Excellence Through Diversity
MINNEAPOLIS, MINNESOTA, JUNE 26TH-29TH, 2022 ASEE
Paper ID #38282

Developing and Assessing Educational Games to Enhance Cyber Security Learning in Computer Science

Jinghua Zhang

Dr. Jinghua Zhang is a Professor of Computer Science. She received her doctoral degree in Computer Science and Engineering from Michigan State University in 2005. Her research interests are in the areas of computer graphics, computer science education, and game-based learning. Dr. Zhang has seventeen years of experience in teaching and advising both undergraduate and graduate students. She has received funding awards with a total amount of $900,000 and her research activities have resulted in many peer-reviewed publications.

Developing and Assessing Educational Games to Enhance Cyber Security Learning in Computer Science

Abstract

Cyber security education is critical to preparing Computer Science students for the increasing security challenges they will face in the future. Games have been successfully used in many areas of education, including Computer Science, to engage students in learning. Although some games are available to increase cyber security awareness among high school students, it is hard to find serious games that focus on advanced security topics for college students. The cyber security educational community needs this type of tool to keep students motivated and engaged in learning difficult security concepts. Furthermore, many of the creators of the educational games have not put sufficient emphasis on the evaluation and assessment of the games. We developed three educational games to teach cybersecurity concepts including Buffer Overflow, Access Control, LAN and ARP Spoofing. The games were developed using the Unity game engine and deployed to the WebGL format so students can play them online. None of these games require prior experience in gaming. To measure the effectiveness, we developed pre-survey, post-survey, and focus group protocols. Additionally, each game module has in-game assessments which require students to complete after each level of the game. Player information and assessment data are saved on the cloud through GameSparks for further analysis. These games have been utilized many times in the classroom with positive student feedback and promising evaluation results. In this poster, we will present game design, development, and assessment results.

Project Implementation

The goal of our project is to develop and assess three educational games that aim to help students master important abstract concepts in cyber security in a fun and competitive environment. The major project activities are shown in Figure 1. Three games have been developed to teach cybersecurity concepts including Buffer Overflow, Access Control, LAN and ARP Spoofing. Each game development followed a similar implementation process. The project team produced a detailed storyboard for the targeted security topic, and then developed prototypes, which were reviewed, assessed, and refined. The following sections will briefly present each game.

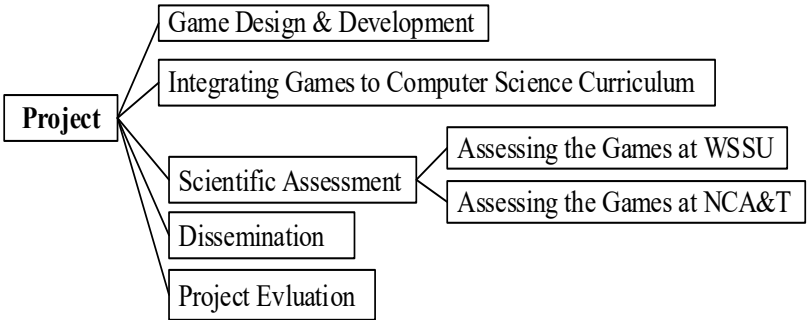

Figure 1. Project Activities

Buffer Overflow Game Module

We developed a web-based interactive visualization tool that aims to help students understand buffer overflow concepts. It has six levels that build upon one another as well as an assessment after each level for immediate learning feedback. There is a mini-game between each level that uses similar concepts learned in the previous level. To evaluate the impact of this online visualization tool on students' learning, we developed in-game assessments, a pre-test, a post-test, and a survey. This tool has been used many times in the Network Security class at North Carolina A&T State University (NC A&T) and the Organization of Programming Languages class at Winston-Salem State University (WSSU) since Fall 2019. The classroom experience report and focus group discussion show that this tool helped students improve their understanding of buffer overflow concepts. The detailed information about the game development and assessment results can be found in [1].

Access Control Game Module

The "Temple of Treasures" game is designed to help students learn basic concepts of Discretionary Access Control and Mandatory Access Control in a fun environment. It has three learning objectives: After playing the game, students should be able to 1) explain read/write/execute permissions of files and change file permissions; 2) explain/modify the access control list of a file; 3) explain the basic concepts of MAC. The game's story is centered around an adventurer in search of gold but ends 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. This game has been used multiple times in the Operating Systems class at NC A&T and Introduction to Information Security class at WSSU. The first level of the game was also used in the System Administration II class at WSSU. According to the survey, 75% of the students agreed that the learning objectives of the game were met. The detailed information about the game development and assessment results can be found in [2].

LAN and ARP Spoofing Game Module

We created a game to teach Local Area Network (LAN) and Address Resolution Protocol (ARP) spoofing concepts. The game has several levels of difficulty that guide learning from the basics of LAN to the countermeasures. It has three learning objectives: 1) Learn how switches and hubs work, and how ARP protocol works; 2) Learn how ARP spoofing works; 3) Learn the countermeasures against LAN attacks. It is presented in the form of a three-level building. Each level has multiple rooms where each room holds the content to learn on a different concept. The player must go through each concept and answer the quiz questions before moving to the next room. At the end of each level, the player will get additional challenges to complete to move to the next level. This game has been used in the COMP420 Network Security class at NC A&T in Fall 2021. We plan to use it this semester at both universities and present our findings during the poster session.

Summary

These games have been made available online (https://gamelab.wssu.edu/modules.htm) for educators and students at other universities. If adopted, these will help instructors engage their students in the process of learning about cyber security, improving the quality of education in this important field. The project team will host a faculty workshop in summer 2022 to share these games. We will demo these games during the poster session at the conference.

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] J. Zhang, X. Yuan, J. Johnson, J. Xu, M. Vanamala (2020), “Developing and Assessing a Web-Based Interactive Visualization Tool to Teach Buffer Overflow Concepts”, Proceedings of IEEE Frontier in Education Conference (FIE'20), Virtual Event, Uppsala, Sweden, October 21-24, 2020.

[2] P. Weanquoi, J. Zhang, X. Yuan, J. Xu, and E. J. Jones (2021), “Learn Access Control Concepts in a Game”, Proceedings of IEEE Frontier in Education Conference (FIE'21), Lincoln, NE, October 13-16, 2021.