Toward Guidelines for Designing Cybersecurity Serious Games

Miriam Gáliková
Masaryk University
Czech Republic
galikova@ics.muni.cz

Valdemar Švábenský
Masaryk University
Czech Republic
svabensky@ics.muni.cz

Jan Vykopal
Masaryk University
Czech Republic
vykopal@ics.muni.cz

ABSTRACT

Cybersecurity serious games provide hands-on training of cybersecurity skills and enhance security awareness. Besides the learning content, they use gamification elements to engage and motivate the players. We propose guidelines for creating technical cybersecurity games in a higher education context, based on a literature review and experience of cybersecurity instructors. We also introduce topics for further research in this area.

CCS CONCEPTS

• **Social and professional topics → Computing education**.

KEYWORDS

cybersecurity education, hands-on training, game design

1 INTRODUCTION

The shortage of cybersecurity professionals has become a significant global problem [3]. To address it, effective training approaches need to be developed. Cybersecurity serious games are one such approach since they combine proven teaching methods and creative means of cybersecurity education [1, 2]. They aim to effectively reproduce real-world security situations that require strategic and adversarial thinking [5]. While playing the game, players can acquire knowledge from various areas, such as penetration testing, network forensics, or secure coding. Besides enhancing technical skills, educational games can support soft skills, such as teamwork, leadership, crisis management, or multi-institutional cooperation.

Currently, there is no standardized methodology for creating cybersecurity serious games. However, multiple research papers, government recommendations, and industry best practices focus on educational games and practical training in the cybersecurity field. Based on the literature review and lessons learned from cybersecurity instructors, we are creating practice-oriented game design methods suitable for security courses and hands-on learning activities at universities. These methods can be interesting for cybersecurity instructors and education researchers.

2 GAME DESIGN GUIDELINES OVERVIEW

Our methods focus on technical games that train students' offensive or defensive security skills in an interactive learning environment. The methods aim at beginner game designers. They introduce essential game design concepts, which altogether create comprehensive guidelines on how to create a cybersecurity game. They cover multiple aspects of game design, including:

- Learning objectives
- Design of challenges/tasks and their solutions
- Rules and anti-cheating policies
- Hints and suitable scaffolding
- Gamification elements, such as narrative, players' game identity, injects, and special rewards
- Technical environment, testing and troubleshooting
- Data gathering, privacy, and ethical considerations
- Evaluation, final documentation and game licenses

The game design methods are centered around learning objectives, which are categorized using the ACM/IEEE Cybersecurity Curricular Guidelines [4]. Specifically, the games can train players in data, software, component, connection, and system security knowledge areas. Our methods recommend practical examples for each area to help game designers create challenge content.

3 CONTRIBUTIONS AND FUTURE WORK

The poster will introduce our work in progress: practice-oriented methods for creating serious cybersecurity games. We will present a handout and flowchart-like diagram explaining the recommended order and structure of the game design steps. So far, we performed a comprehensive literature review of more than 70 sources. Currently, we are complementing the methods with the guidance of expert cybersecurity instructors from our university. They found the preliminary results useful and applicable in teaching practice.

We tested our preliminary results by implementing a new game based on the guidelines. They have also been applied in courses at two universities, in which the students create cybersecurity games. Subsequently, other students will play these games and evaluate them in a post-game survey. We will also collect qualitative feedback from the game designers via questionnaires and interviews. These data will be used to research whether our guidelines proved useful during the process of game design and how the guidelines could be improved.

REFERENCES

[1] V. Aleven, E. Myers, M. Easterday, and A. Ogan. 2010. Toward a Framework for the Analysis and Design of Educational Games. In *2010 Third IEEE International Conference on Digital Game and Intelligent Toy Enhanced Learning*. 69–76.

[2] L. A. Annetta. 2010. The "I's" Have It: A Framework for Serious Educational Game Design. *Review of General Psychology* 14, 2 (2010), 105–113. https://doi.org/10.1037/a0018985

[3] (ISC)^2. 2019. *Cybersecurity Workforce Study*. Retrieved December 07, 2020 from https://www.isc2.org/Research/2019-Cybersecurity-Workforce-Study

[4] Joint Task Force on Cybersecurity Education. 2017. *Cybersecurity Curricular Guideline*. Retrieved December 07, 2020 from http://cybered.acm.org

[5] N. M. Katsantonis, I. Kotini, P. Fouliras, and I. Mavridis. 2019. Conceptual Framework for Developing Cyber Security Serious Games. In *2019 IEEE Global Engineering Education Conference (EDUCON)*. 872–881.

SIGCSE '21, March 13–20, 2021, Virtual Event, USA
The definitive Version of Record was published in *Proceedings of the 52nd ACM Technical Symposium on Computer Science Education (SIGCSE '21), March 13–20, 2021, Virtual Event, USA*, https://doi.org/10.1145/3408877.3439568.