Using Gamification to Teach Security Analysis in Higher Education

Clara Ayora[1], Jose Luis de la Vara[1]
[1]Universidad de Castilla-La Mancha
Avda. España s/n, 02071 – Albacete – Spain
{clara.ayora, joseluis.delavara}@uclm.es

Abstract. *Teaching security analysis at university allows future professionals to acquire with the necessary skills to protect and maintain the integrity of digital infrastructures. This work presents a board game and its practical use for teaching security analysis in 1st-year bachelor students. The game has been employed in the past four years and our perception of use is positive. Being a game with a simple and most-likely known mechanics, it could be adapted and used by other educators to teach software engineering topics.*

1. Introduction

Security analysis is an integral aspect of requirements engineering to ensure systems are robust and resilient against potential threats [McGraw 2004]. As future professionals, university computer science students will design and maintain essential systems, e.g., e-banking. Understanding security analysis is vital to protect data, ensure privacy, and safeguard against cyber threats [Stallings 2015]. Early learning enables students to identify vulnerabilities, implement security measures, and respond to incidents.

Simultaneously, gamification has gained attention in higher education [Chung 2019, Schreuders 2016]. Defined as applying game-design elements in non-game contexts [Chung 2019], gamification enhances student engagement, motivation, and learning outcomes. By leveraging motivational factors like rewards and progress tracking, gamification creates a dynamic and interactive educational experience.

Following [Schreuders 2016], we present a game for teaching security analysis in higher education. It is called '*Cyberpatrol*' and is a board game with a mechanics like the '*game of the goose*'. Upon landing on the squares, players must answer whether a statement about security analysis is true or false. The statements are about *Security Fundamental Concepts*, *Encryption Types*, *Protection Measures,* and *Security History*.

2. Game description and discussion

The board of the game can be found in [Ayora 2025]. The mechanics is as follows: **1.** Students are grouped in teams of four students each. **2.** Teams start with 0 points. **3.** A playing order is established for the teams. **4.** Using turns, each team rolls a die to determine how many squares they move on the board. **5.** Depending on the type of square a team lands on (Figure 1), they must answer a question about *security concepts* (square with a light bulb), *encryption* (padlock), *protection* (shield), or *history* (clock and scroll), *suffer an attack* (hacker), *challenge another team* (swords), or *roll the die again* (pipe). **6.** Teams will earn 3 points if they answer correctly or lose 1 point if they answer incorrectly. **7.** When suffering an attack, a team will lose 5 points. **8.** When landing on a challenge square, the corresponding team can challenge another by selecting two questions that both teams need to answer. If one team wins (i.e., one team

has more correct answers than the other), it will earn 5 points, and the losing team will lose 3 points. In case of a tie, the team that issued the challenge will lose 1 point and the challenged team will gain 1 point. **9.** During the game, why a statement is true or false is explained if needed. **10.** A game ends when a team reaches the final square or when the teaching session finishes **11.** The team with the highest number points is the winner.

Figure 1. Types of squares

The game has been used the past four years in a 1st-year course on "*Information Systems*" of a Bilingual (in Spanish and English) Bachelor's Degree in Computer Science and Engineering at the *University of Castilla-La Mancha* in *Albacete, Spain*. This course introduces what information systems are, their role, and how they are managed and used (including security aspects). Around 50 students, including exchange ones, attend the course each year. Being a 1st-year course, students have no (or very little) knowledge about security analysis. To encourage students' participation, winning students are rewarded with 0.25 additional points to their grade for the exam on security analysis. Security analysis is the last unit of the course. The board game is currently implemented in Excel. We have used it as part of a content review session.

During these four years, our perception and experience using the game has been positive and we plan to continue using it. First, the game has remained unchanged since its initial use, beyond adding questions, showing a suitable design for teaching security analysis. Second, students appear to enjoy playing, especially the challenges, showing interest in security analysis and eagerness to win the game. Third, we consider that the game contributes to students' learning on security analysis. These perceptions could be further analyzed via empirical studies, e.g., surveys and experiments.

Given its simple mechanics and design, the game can be easily adapted to other topics, e.g., by defining different question categories and symbols. Educators could use the game to teach (or reinforce) software engineering topics such as software modelling or processes. As potential improvements, multiple-choice questions could be used instead of true/false ones. This would increase the game difficulty. Besides, the board game could be implemented in a mobile app so that students can play (alone or in groups) even after the teaching session. This could help students with the course exam.

Acknowledgement. This work has received funding from the REBECCA project (HORIZON-KDT 101097224; MCIN/AEI PCI2022-135043-2; NextGen.EU/PRTR).

References

Ayora, C., et al. (2025). Cyberpatrol-game board. *CIbSE 2025*. Zenodo. https://doi.org/10.5281/zenodo.15088573

McGraw, G. (2004). Software security. *IEEE Security & Privacy*, *2*(2), 80-83.

Stallings, W., et al (2015). *Computer security: principles and practice*. Pearson.

Chung, C. et al. (2019). Students' acceptance of gamification in higher education. *(IJGBL)*, *9*(2), 1-19.

Schreuders, Z. C. et al. (2016). Gamification for teaching and learning computer security in higher education. In ASE 16.