Teaching Security and Privacy Through Game-Based Learning: A Literature Review/Systemization of Knowledge

Abdul Kanu
University of Utah, Salt Lake City
Advisor: Dr. Sameer Patil

Abstract

This report presents the results of a summer research project conducted under the supervision of Dr. Sameer Patil at the University of Utah. The project aimed to review existing literature on video games designed to teach security and privacy concepts to non-technical professionals. The project involved creating a literature matrix to systematically organize findings from 100 papers. Based on this matrix, an outline for the Systemization of Knowledge (SoK) was created to complement a broader research effort within Dr. Patil's lab, contributing to the growing field of game-based learning for security and privacy education. This paper provides a scholarly review of the prior work, including the methodologies, key findings, and contributions of various systems, alongside a technical description of the project's progress.

1. Introduction

Security and privacy are critical concerns in today's digital landscape. However, many non-technical users lack the knowledge necessary to safeguard their personal information online. Game-based learning offers a promising approach to teaching these concepts by engaging users through interactive and immersive experiences. This research project focuses on reviewing and categorizing games designed to educate non-technical users about security and privacy.

The main goal of this study was to identify patterns and gaps in the existing literature to inform the development of more effective educational games. Working with a Ph.D. student from the prost (Dr. Sameer Patil's lab), I was able to compile a comprehensive literature matrix and began drafting an outline for a Systemization of Knowledge (SoK) to further the work of Dr. Patil's lab.

2. Methodology

2.1 Literature Matrix Creation

The primary task of this research was to create a literature matrix from 100 selected scholarly papers on game-based learning in security and privacy. To compile this matrix, I conducted comprehensive searches across multiple academic databases, including the **IEEE Xplore**, **ACM Digital Library**, and **Google Scholar**. I was also given the freedom to create my own inclusion and exclusion criteria for selecting papers. These criteria ensured the relevance of the chosen studies to the project's objectives, focusing on games designed to teach security and privacy concepts, with an emphasis on non-technical audiences.

After careful consideration, I developed research questions that would guide the literature review, which were later reviewed and approved by Dr. Patil. The research questions focused on understanding the methodologies used in the design and evaluation of security and privacy games, the effectiveness of these games, and the key security topics they addressed.

For each paper selected, I extracted the following information:

- **Author(s) and Year**
- **Objective**
- **Methodology**
- **Key Findings**
- **Relevance**
- **Security and Privacy Topics**
- **Game Genre and Platforms**

The literature matrix served as a tool for systematically analyzing the contributions of each paper and identifying common themes, methodologies, and gaps in the literature. This matrix became the foundation for developing a Systemization of Knowledge (SoK) outline, which aims to categorize the existing knowledge in this domain and provide insights for future game-based learning systems.

2.2 Systemization of Knowledge (SoK)

After completing the literature matrix, we initiated the process of developing a Systemization of Knowledge (SoK) paper. The SoK aimed to organize and categorize knowledge from the reviewed literature, identifying best practices in game design for security and privacy education. The outline we developed is intended to complement another paper being prepared by Dr. Patil's lab.

3. Scholarly Review of Related Work

This section provides an overview of key findings from the literature matrix, organized by methodology, security/privacy topics, and game design approaches.

3.1 Methodologies

The papers reviewed in the literature matrix employed various methodologies to evaluate the effectiveness of security and privacy games, including:

- **Questionnaires and Surveys**: Many studies, such as those by Vibha Singh et al. (2023) and Michael Christensen et al. (2023), used surveys to assess players' knowledge and engagement after participating in game-based learning experiences. These studies demonstrated that interactive games significantly improved players' understanding of key concepts such as malware and phishing.
- **Action Research**: In studies like Iolanda Bernardino et al. (2021), action research was used to iteratively test game prototypes with target audiences. This method allowed researchers to refine the games based on real-time feedback, leading to better outcomes for teaching cybersecurity awareness.
- **Experimental Evaluations**: Papers like Stephen Hart et al. (2020) used controlled experiments to measure the impact of serious games on cybersecurity awareness. Players were guided through scenarios and asked to complete tasks designed to reinforce learning outcomes.

3.2 Key Findings

Several key findings emerged from the literature:

- **Effectiveness of Immersive Environments**: Vibha Singh et al. (2023) found that immersive technologies, such as virtual reality (VR), enhanced players' retention of security concepts by creating engaging, realistic scenarios.
- **Generative AI in Game Design**: The study by Suthada Muengsan et al. (2023) highlighted the use of generative AI to create adaptive learning experiences in cybersecurity games. AI-driven content dynamically adjusts to the player's performance, providing tailored challenges and feedback.
- **The Role of Narrative and Gamification**: Several papers emphasized the importance of incorporating narrative elements and gamification techniques to increase player engagement. These features make abstract security concepts more relatable, particularly for non-technical audiences.

3.3 Security and Privacy Topics

The reviewed literature covered a wide range of security and privacy topics, including:

- **Phishing and Malware Awareness**: Many games, such as "Riskio" by Stephen Hart et al. (2020), focused on teaching players how to recognize phishing attempts and malware. These games used realistic scenarios to simulate cyberattacks, helping users develop strategies for avoiding threats.
- **Privacy and Data Protection**: Michael Christensen et al. (2023) developed a game that engaged players in understanding data protection principles. The game allowed users to make decisions about data sharing, highlighting the trade-offs between privacy and convenience.
- **Ethics in Cybersecurity**: Several papers, such as those by Suthada Muengsan et al. (2023), addressed ethical considerations in security practices, including the moral implications of hacking and data breaches. These topics are critical in raising awareness about responsible digital behavior.

---

4. Systemization of Knowledge Outline

The SoK outline that was drafted based on the literature matrix includes the following sections:

- **Introduction**: Overview of game-based learning in the context of security and privacy.
- **Methodology**: Description of how games are evaluated, including the common use of questionnaires, surveys, and experimental methods.
- **Game Design Principles**: Categorization of design principles for creating effective security/privacy games, such as narrative integration and adaptive learning.
- **Security/Privacy Topics**: Summary of the key security and privacy concepts addressed by these games.
- **Best Practices and Gaps**: Identification of best practices in game design, as well as gaps in the literature where further research is needed.

This outline is intended to complement ongoing research within Dr. Patil's lab, particularly a paper being prepared for submission to conferences.

---

5. Conclusion

This report highlights the progress made during my summer research project at the University of Utah. By creating a comprehensive literature matrix and outlining a Systemization of Knowledge paper, I contributed to the broader understanding of how game-based learning can be used to teach security and privacy concepts to non-technical professionals. Future work will focus on refining the SoK paper and exploring new game design approaches that leverage technologies such as generative AI to enhance player engagement and learning outcomes.