DOI: https://doi.org/10.56198/ZH3JOJ4XF

Work-in-Progress-Participatory Design of an Augmented Reality Firewall Game

Syed Ali Asif[1], Raymond Patt[1], Teomara Rutherford[1], Chrystalla Mouza[2], and Chien-Chung Shen[1]

[1] University of Delaware, Newark, Delaware, United States
{asifrabi, raypatt, teomara, cshen}@udel.edu
[2] University of Illinois Urbana-Champaign, Urbana and Champaign, Illinois, United States
cmouza@illinois.edu

Abstract. To ensure children's online safety in response to cyber threats, such as hacking, phishing, and misinformation, children must learn about cybersecurity. Through an iterative design process in collaboration with middle school teachers, we developed an Augmented Reality (AR) firewall game for middle school students (aged 10-14 years) to familiarize them with cybersecurity fundamentals. The iterative design process consisted of a series of design sprints in which the teachers detailed how they teach cybersecurity in the classroom and discussed the design choices of a firewall game. Through this process, we developed an AR game to teach about firewalls that teachers feel is suitable for classroom use and capable of making cybersecurity education concrete and interactive. This work-in-progress paper presents the AR firewall game's iterative design and initial prototype. Future work will explore the cybersecurity knowledge students develop from using this gamified platform and potential games of other cybersecurity concepts.

Keywords: Augmented Reality, Cybersecurity Education, Firewall, Interactive Learning.

1 Introduction

With advancements in technology, blending real-world environments and computer-generated material is made possible through Augmented Reality (AR). AR applications have become more accessible to the general public and are used by practitioners like teachers [4]. In the education sector, AR applications are making a positive mark [4]. Through AR technology, course content becomes more dynamic and lively, allowing for interactive classroom learning. In particular, research has demonstrated that AR technology can make learning more expressive, efficient, and effective for students [4]. Additionally, research has shown that classroom learning with the aid of AR technology can be more interactive [12]. Beyond this, research has found that AR is associated with increased content understanding, long-term memory retention, improved collaboration, and increased student motivation [5]. Yip et al., for instance, found that AR video integration in the classroom resulted in higher learning efficiency, which enabled students to gain a better conceptual understanding of complex issues, such as 3D processes and spatial learning in the process of knitting needles [7]. AR may also have negative impacts; Radu et al. demonstrated that poor application design and ineffective classroom integration can limit learning [5]. Thus, while AR may be fruitful, it should be thoughtfully designed and integrated; the authors in [1], suggest this can be done by incorporating teachers' beliefs. In this work-in-progress paper, we've incorporated teachers in the design and implementation of AR games to glean the benefits of AR.

Interconnected computer systems, like the Internet, are constantly under the threat of malicious actors that desire the hardware, software, and data these networks harbor. Cybersecurity seeks to inhibit these actors by preventing information from being passed to them. As the Internet has become integral to our daily lives, cybersecurity education becomes fundamental. Early education is especially important, as some adults are less cognitively able to adapt to the paradigms needed for cybersecurity [13]. Further, young children are just as susceptible to the risks posed by malicious actors as adults. Importantly, this early exposure may be fruitful in the

©2023 Immersive Learning Research Network

nurturing of future cybersecurity professionals, which national security experts have called a need for [21]. Our primary focus in this paper is on Firewalls, which is a key topic in Cybersecurity. Firewalls are security systems designed to prevent unauthorized access to or from a private network while allowing authorized communication.

We have designed and developed a concrete, interactive AR-based firewall game in collaboration with middle school teachers. In this game, students learn the concepts underlying firewalls, which the Computer Science Teacher Association (CSTA) has identified as fundamental for students' effective use of digital technologies [8]. Additionally, we are using cybersecurity standards from cyber.org to assess the game's effectiveness. This collaboration consisted of a series of design sprints and prototype-testing meetings with the teachers to assess the gameplay. Given the success of this model, future work will follow this method in the development of other cybersecurity-focused AR games.

2 Related Work

2.1 Augmented Reality in Education

In education, AR may afford educators the ability to teach complex, abstract concepts by making them concrete. Indeed, Shelton et al. have shown that AR's play-and-learn approach makes abstract concepts easier to understand [10]. Educators have used AR to teach a range of topics. For example, intellectual property educators utilized an AR application to aid in trademark registration [2]. Further, engineering and manufacturing educators have used AR to teach motion analysis in assembly tasks in the manufacturing process [3]. AR math games for 7- and 8-year-olds [6] have also been used in the classroom to create a better learning experience for the students. AR games for other subjects exist as well. For instance, AR has been used to teach history to middle school students [14]. Despite AR being implemented often in education, the literature mentioned above lacks AR solutions that incorporate the design considerations of teachers and students. Including this valuable feedback has been proven to augment the incorporation and utilization of AR [1].

2.2 Cybersecurity Education

Most of the approaches to teaching cybersecurity to students rely on various kinds of games, such as role-playing games. Wen at el. [11] developed an anti-phishing game that teaches participants about phishing scams and how to stay safe. Other gamified approaches for cybersecurity education are CyberAware [16]—a mobile game for K-6 children and SherLOCKED [17]—a 2D top-down puzzle adventure game. Gamified approaches have been found to be interesting, motivating, and effective across domains [18].

The immersive and interactive nature of AR could potentially be more useful in teaching cybersecurity concepts to students, as it could integrate both the physical and virtual aspects of the environment [10] providing a comprehensive and immersive learning experience for students. Some studies have already focused on the design and evaluation of AR and other Mixed Reality applications for phishing [9] and other cybersecurity concepts [8]. Consistent with this stream of research, in this work, we iteratively design and develop an AR game to teach the concept of firewalls in the classroom.

3 Research Goals and Proposed Work

Our research aim is to develop an AR game to teach students about the cybersecurity concept of firewalls. Additionally, the plan is to evaluate the effectiveness of the game by conducting cognitive interviews with students and assessing their knowledge using a pre-/post-test approach.

3.1 Firewall

Firewalls protect computer systems. Often, they are software installed on networking devices to filter data traffic and prevent malicious attackers from gaining unauthorized access. Firewalls work as an access point for the data packets from outside public networks to local private networks. Based on the security policy and regulations, the firewall lets certain data packets through to the private network and blocks others.

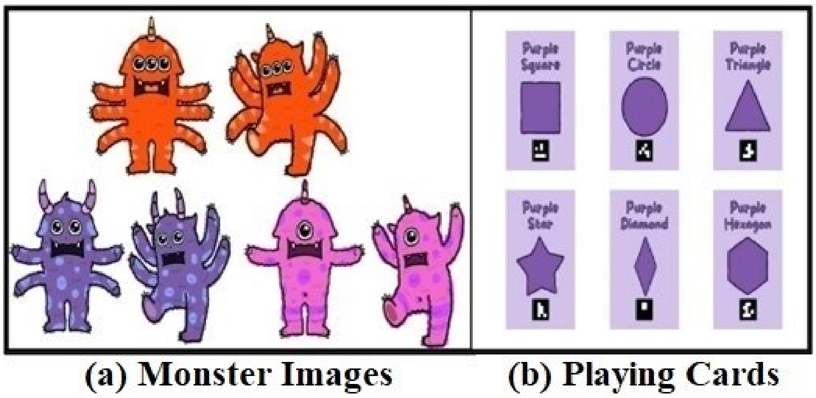
3.2 Iterative Development / Participatory Design

In the development of this work, we followed an iterative development approach [19] inspired by participatory design [20]. In iterative development approaches, designed products are continuously presented, evaluated, and improved upon based on evaluations. In participatory design frameworks, those using the technology are treated as experts in how it works and its features. These experts influence how the product is designed, making it work best for them and their purposes. For this work, teachers are the expert stakeholders. Thus, we met with middle school teachers to discuss how to teach their students about firewalls. Through a series of design sprints, we presented game ideas, discussed classroom implementation feasibly, and incorporated their considerations into our designs. The design sprint meetings were audio recorded to incorporate the feedback we may have yet to notice. Our ideas were presented to the teachers through paper prototypes, storyboards, and implementation guides following Ehn's original protocol [22], in which product variations were presented to stakeholders.

We consulted with five middle school teachers who taught computer science and STEM subjects to develop the AR game. Collaborating with these teachers gave us a unique edge concerning the design and development of our game. The perspectives and classroom experiences of the teachers afforded us new points of view. Two examples of these key findings are given below:

- Reducing text prompts: Teachers provided insight that students would not want to read texts while playing games, thus visual content is used.
- Changing gameplay: We originally conceptualized this game to be competitive, but the teachers suggested this game be cooperative to align with their schools' vision on collaboration and teamwork to avoid classroom disorder**.**

We are developing an AR game that teaches the concepts underlying firewalls while maintaining students' motivation and engagement. The game is developed with the help of design sprints, multiple focus group meetings, and prototype demonstrations. The incorporation of teacher feedback facilitates technology-classroom integration.



(a) Monster Images (b) Playing Cards

Fig. 1. (a) Monsters used in the game; (b) playing cards with shapes and colors.

3.3 Augmented Reality-Based Firewall Game

In the AR firewall game, there are three categories of players with respect to the firewall: (1) users of connected computer systems, (2) defenders who determine the rules of firewalls, and (3) attackers who also try to learn the rules of firewalls but for malicious purposes. Players use physical playing cards (Figure 1) to represent data packets in the game, which are then scanned and turned into virtual objects in AR. The game can be played as a single team or between two teams, depending on the technological capacity of the classroom. User players act as a team of ethical hackers and learn what features of shapes, monsters, or files are blocked by the firewall and what objects are considered malicious. By playing the game, user players can understand how firewalls work and what ethical hacking entails and practice their analogical reasoning skills [23], which teachers expressed would be helpful as they taught cybersecurity skills. After consulting with the teachers, we identified four main ideas to convey through the game: (1) firewalls block things from entering the computer, (2) firewalls do not block everything, (3) firewalls block good and bad things based on characteristics, and (4) AR should be used to convey the idea better and facilitate interest.

3.4 Overview of the Game

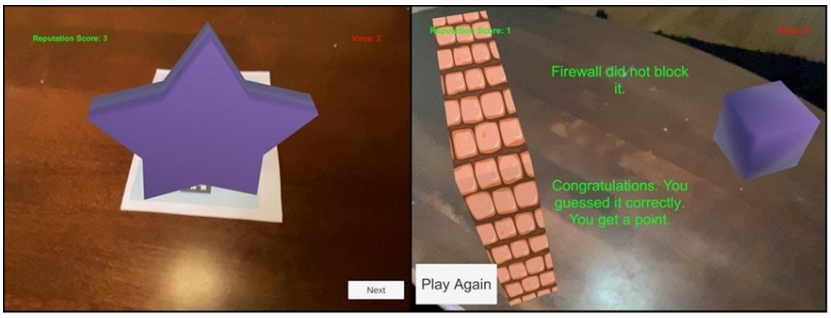
The game has multiple levels suggested by the teacher collaborators that increase in difficulty and relevance to cybersecurity, with the first level using shapes and the third level using monsters with varying features. Students use corresponding cards scanned and placed in an AR world to determine whether the firewall blocks them. AR animations illustrate the results. If students guess correctly, their protection score increases, and if they let a virus pass through, their virus score increases. Upon reaching a predefined protection score maximum, students receive an AR reward object, such as an animated AR lion or fish, but if they reach a predefined maximum of viruses, the game ends with no reward. Based on the teachers' suggestions, showing an animated AR reward object in the physical world can pique the student's interest and make the learning experience more engaging.

Additionally, the rules and policies associated with the shapes, colors, and monsters are recalculated randomly before the next iteration. After teaming with teachers, we used their insights and findings to design a game with two playing modes: one team and two teams. These modes are flexible and do not affect the game's implementation. Instead, they are defined based on how teachers and students want to integrate the game into the classroom. For example, some teachers may need more resources for every student to use their own tablet in the one-team mode. Thus, two teams can be used to increase the number of students per tablet.

When playing as one team, the student or team of students act as ethical hackers by trying to break the system and guess which card would pass through the firewall, increasing the protection score with correct guesses. The goal is to reach the maximum protection score before the virus score maximizes to receive an AR reward object. In the two-team format of the game, students form an attacker team and a defender team. The attacker team's goal is to infiltrate the system by making objects of the cards pass through the firewall while the defender team guesses if the cards will be blocked or not. Correct guesses increase the protection score, and incorrect ones increase the virus score. The game ends when either the virus score reaches the maximum point, and the attacker team wins, or the protection score reaches the maximum, and the defender team wins and receives an AR reward. Both approaches expose students to the rules and policies of the firewall and encourage them to think like cybersecurity professionals, which may encourage them to pursue a career in cybersecurity in the future.

4 Conclusions

We described the development of an AR-based firewall game in collaboration with middle school teachers, aiming to raise students' awareness of cybersecurity and unlock their potential to become cybersecurity professionals. The success of the classroom integration and student learning outcomes will be assessed through observation and knowledge assessments before and after the intervention, with controls for logical reasoning measured by Raven's assessment [15]. The pre-/post-tests will be generated from the skills that cybersecurity professionals deem are necessary to understand firewalls and will be generated from the cybersecurity standards from cyber.org. These tests will be piloted with students through cognitive interviews to ensure they understand the material assessed. After successful implementation, the collaborative procedures used in developing the game will be outlined for other researchers and teachers. These procedures will be used for future successful developments of cybersecurity games and games of other domains for middle school students.



Firewall did not block it.

Congratulations. You guessed it correctly. You get a point.

(a) AR Object (b) AR Animation

Fig. 2. (a) A corresponding AR Object placement on top of the playing card; (b) A snapshot of the AR animation played in the game.

Acknowledgments

Funded by the National Science Foundation (Grant # 2048874). Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the NSF.

References

1. Tiede, J., Grafe, S., Mangina, E.: Teachers' attitudes and technology acceptance towards AR apps for teaching and learning. In: 2022 8th International Conference of the Immersive Learning Research Network (iLRN). pp. 1–8. IEEE (2022).
2. Bacca-Acosta, J., Lis-Gutierrez, J.P., Avila-Garzon, C., Sandoval-Escobar, M., Cardenas-Criollo, J.: Work-in-progress—a mobile augmented reality application for learning about trademark registration in intellectual property education. In: 2022 8th International Conference of the Immersive Learning Research Network (iLRN). pp. 1–4. IEEE (2022).
3. Angel, N., Orsolits, H., Garcia, J.: Developing an ar based tool for teaching motion analysis on assembly tasks. In: 2022 8th International Conference of the Immersive Learning Research Network (iLRN). pp. 1–7. IEEE (2022).
4. Pathania, M., Mantri, A., Kaur, D.P., Singh, C.P., Sharma, B.: A chronological literature review of different augmented reality approaches in education. Technology, Knowledge and Learning 28(1), 329–346 (2023).
5. Radu, I.: Why should my students use AR? A comparative review of the educational impacts of augmented-reality. In: 2012 IEEE International Symposium on Mixed and Augmented Reality (ISMAR). pp. 313–314. IEEE (2012).
6. Li, J., van der Spek, E., Hu, J., Feijs, L.: Exploring tangible interaction and diegetic feedback in an ar math game for children. In: Proceedings of the 18th ACM International Conference on Interaction Design and Children. pp. 580–585 (2019).
7. Yip, J., Wong, S.H., Yick, K.L., Chan, K., Wong, K.H.: Improving quality of teaching and learning in classes by using augmented reality video. Computers & Education 128, 88–101 (2019).
8. Shen, C.C., Chiou, Y.M., Mouza, C., Rutherford, T.: Work-in-progress-design and evaluation of mixed reality programs for cybersecurity education. In: 2021 7th International Conference of the Immersive Learning Research Network (iLRN). pp. 1–3. IEEE (2021).
9. Chiou, Y.M., Shen, C.C., Mouza, C., Rutherford, T.: Augmented reality-based cybersecurity education on phishing. In: 2021 IEEE International Conference on Artificial Intelligence and Virtual Reality (AIVR). pp. 228–231. IEEE (2021).
10. Shelton, B.E., Hedley, N.R.: Using augmented reality for teaching earth-sun relationships to undergraduate geography students. In: The First IEEE International Workshop Augmented Reality Toolkit,. pp. 8–pp. IEEE (2002).
11. Wen, Z.A., Lin, Z., Chen, R., Andersen, E.: What. hack: engaging anti-phishing training through a role-playing phishing simulation game. In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. pp. 1–12 (2019).
12. Billinghurst, M., Duenser, A.: Augmented reality in the classroom. Computer 45(7), 56–63 (2012).
13. Campbell, S.G., Saner, L.D., Bunting, M.F.: Characterizing cybersecurity jobs: applying the cyber aptitude and talent assessment framework. In: Proceedings of the Symposium and Bootcamp on the Science of Security. pp. 25–27 (2016).
14. Schiavi, B., Gechter, F., Gechter, C., Rizzo, A.: Teach me a story: an augmented reality application for teaching history in middle school. In: 2018 IEEE Conference on Virtual Reality and 3D User Interfaces (VR). pp. 679–680. IEEE (2018).
15. Raven, J.C., Court, J.H.: Raven's progressive matrices and vocabulary scales. Oxford Psychologists Press Oxford (1998).
16. Giannakas, F., Kambourakis, G., Gritzalis, S.: Cyberaware: A mobile game-based app for cybersecurity education and awareness. In: 2015 International conference on interactive mobile communication technologies and learning (IMCL). pp. 54–58. IEEE (2015).
17. Jaffray, A., Finn, C., Nurse, J.R.: Sherlocked: A detective-themed serious game for cyber security education. In: Human Aspects of Information Security and Assurance: 15th IFIP WG 11.12 International Symposium, HAISA 2021, Virtual Event, July 7–9, 2021, Proceedings 15. pp. 35–45. Springer (2021).
18. Sailer, M., Homner, L.: The gamification of learning: A meta-analysis. Educational Psychology Review 32(1), 77–112 (2020).
19. Cobb, P., Jackson, K., Smith, T., Sorum, M., Henrick, E.: Design research with educational systems: Investigating and supporting improvements in the quality of mathematics teaching and learning at scale. Teachers College Record 115(14), 320–349 (2013).
20. Pilemalm, S., Lindell, P.O., Hallberg, N., Eriksson, H.: Integrating the rational unified process and participatory design for development of socio-technical systems: a user participative approach. Design Studies 28(3), 263–288 (2007).
21. Petersen, R., Santos, D., Wetzel, K., Smith, M., Witte, G.: Workforce framework for cybersecurity (nice framework) (2020).
22. Ehn, P., Brattgård, B., Dalholm, E., Davies, R., Hägerfors, A., Mitchell, B., Nilsson, J.: The envisionment workshop-from visions to practice. In: Proceedings of the Participatory Design conference. pp. 141–152. MIT Boston (1996).
23. Vendetti, M.S., Matlen, B.J., Richland, L.E., Bunge, S.A.: Analogical reasoning in the classroom: Insights from cognitive science. Mind, Brain, and Education 9(2), 100–106 (2015).