Design and Evaluation of Mixed Reality Programs for Cybersecurity Education

Yan-Ming Chiou, Chien-Chung Shen
Department of Computer and Information Sciences
University of Delaware
Newark, Delaware
steveice,cshen@udel.edu

Chrystalla Mouza, Teomara Rutherford
School of Education
University of Delaware
Newark, Delaware
cmouza, teomara@udel.edu

***Abstract*—With the shortage of cybersecurity professionals, there is a critical need to train more young-generation cybersecurity professionals to fill the gap. In this work, we designed interactive activities that make abstract cybersecurity concepts more tangible by using exciting new mixed reality (MR) technology to teach cybersecurity skills and raise the potential interest in cybersecurity careers for middle school students. We plan to analyze the immersive experience, situational interest, and workload after the experiment to study the participants' learning performance and user experience.**

Keywords—Mixed Reality, Cybersecurity Education, STEM

I. INTRODUCTION

On a daily basis, individuals around the world are turning to information and communication technology (ICT) to help manage all aspects of life–social, education, business, entertainment, etc. With that, sensitive data is frequently stored on devices making them targets of cybercrimes. ICT companies are continuously developing new approaches to advance online safety, security, and privacy, yet there is a tremendous need for more cybersecurity professionals to develop a robust workforce that could build secure networks and systems [1]. The shortage of cybersecurity professionals creates risks for both national and homeland security [2]. These risks are exacerbated by the lack of diversity among cybersecurity professionals, as fewer than 20% are women or members of underrepresented groups [4]. Exposing students to cybersecurity education at an early age could not only help raise awareness and knowledge of cybersecurity, but could also lead to a potential future interest in cybersecurity careers, thus creating a pipeline for a robust and diverse cybersecurity workforce.

The need for content to teach about and stimulate interest in cybersecurity has been a driver in the creation of programs, such as cybersecurity competitions. However, these programs are likely to have high barriers to entry; women, and students from underserved communities may be discouraged by the structure of the competitions or may not have access to these programs [3,5]. Cybersecurity programs that meet the needs of a more diverse group of students are desperately needed. Such programs should encourage growth of fundamental skills and knowledge around cybersecurity and should be engaging to students who lack background in cybersecurity or strong coding skills to avoid discouraging novices from further involvement [3]. Furthermore, these programs need to be accessible and easily implemented by educators without highly-specialized cybersecurity knowledge.

Importantly, creating cybersecurity content to educate and engage children before high school is critical for future engagement with the field. In this work, we focus on the critical middle school years (Grades 6-8), as these are years when students often begin to solidify their academic and other identities and can envision possible future selves, including in their careers [6]. By enhancing skills and positive motivation for Computer Science (CS) in general and cybersecurity in particular, we lay a foundation for student selection into more advanced CS in high school and college, a necessary prerequisite for student selection of cybersecurity careers.

More specifically, we focus on prototyping interactive activities that can make abstract concepts (e.g., steganography, phishing, firewalls) more tangible for novices by using the exciting new technology of MR to teach cybersecurity skills, capture situational interest, and develop student self-efficacy and value for cybersecurity and CS broadly. MR encompasses a range of experiences that include Augmented Reality (AR) and Augmented Virtuality (AV) within an Extended Reality framework [7]. The use of MR provides major educational benefits by integrating physical with virtual interaction typically afforded by AR applications [8]. Prior studies have reported positive impacts of AR games on motivation, long-term memory retention, and content understanding [9]; however, the focus has been on overlaying information on top of real-world objects and less on how students interact with these systems and importantly, with each other [10,11]. Further exploration is needed to examine ways of designing MR games that improve students' motivation, learning, and collaboration by blending physical and virtual interactions [12]. The ideas explored in the paper are even more timely and urgent during pandemic. Towards this end, MR can facilitate remote collaborative learning through a shared virtual space where participants join a shared MR session via smartphones or tablets to interact and collaborate without being physically close to one another. Therefore, students can become collaborative partners and co-creators of their learning [13]. More work is needed, however, to facilitate design choices that take advantage of MR systems to support student interactive and collaborative learning experiences.

The focus of this work will be the iterative design of concrete and interactive activities covering key cybersecurity concepts addressed in the Computer Science Teacher Association standards (Networks & the Internet with a specific focus on safety, privacy, and security). The outcomes of this paper will be (1) a set of MR cybersecurity activities with the potential to engage and motivate middle school students, (2) a set of design principles that guide future development of concrete and interactive content to advance cybersecurity education and interest towards cybersecurity careers among students.

978978-1-7348995-2-8/21/$31.00 ©2021 Immersive Learning Research Network

II. Related Work

A. Cybersecurity Education

Most curricular and learning activities designed to introduce cybersecurity concepts focus on games, including board games that teach high-level security concepts, capture-the-flag that helps practice skills of defending against hackers, and immersive simulated role-playing games [14,15]. For instance, Wen et al., developed What.Hack, an anti-phishing online simulation game that includes a series of puzzles. The game teaches phishing concepts and simulates actual phishing attacks in a role-playing game to encourage players to practice defending themselves. Although these efforts are promising, we seek to leverage new and emerging technologies to create cybersecurity activities that interactively blend the physical and virtual world. In order to prepare teachers and students to address key challenges of our connected world, we need to develop and reinvent teaching tools that make such experiences meaningful and motivating [16].

B. Augmented Reality Education

MR technologies have generated much attention in the development of play and learning experiences for students, making it possible to add new layers of meaning to the physical world [17]. Specifically, the coexistence of both virtual and tangible information allows students to visualize abstract concepts [18]. Kim et al. [19] examined the role of MR for learning programming, which allows students to physically interact with a program, concretizes coding errors, and provides real-time feedback to support student understanding and reduce cognitive load. Similarly, Li et al. [20] reported that children found tangible interaction in an MR mathematics learning game interesting and fun, and benefitted from the embedded feedback. Despite the attention, specific efforts to understand the affordances, potential, and design principles that make MR solutions valuable for teaching and learning are under-developed [17]. In particular, applications co-designed with teachers and students to support utility and value are not readily available in the literature.

III. Research Goals and Proposed Work

The research goals of the work are to design MR-based applications for cybersecurity education and to evaluate their effectiveness of increasing students' interests in pursuing careers in cybersecurity.

Specifically, we plan to develop three MR-based prototypes and refine the design principles that can be applied to design future MR-based curriculum in cybersecurity.

A. Firewall

In cybersecurity, a firewall is a security mechanism that helps protect a network by filtering data traffic and blocking outsiders from gaining unauthorized access to the private data on the computers in the network based on predefined security policies. Typically, a firewall is located on the boundary between the public Internet and a private network (such as a home network or a campus network) to inspect data packets (the units that carry information) that want to enter the network according to the security policies: letting in those that are eligible and trashing those that are not. Security policies are specified in terms of rules on the features and contents of the packets, which are enforced by the software implementing the firewall. By changing the rules, a firewall can be programmed to allow different data packets to enter the network.

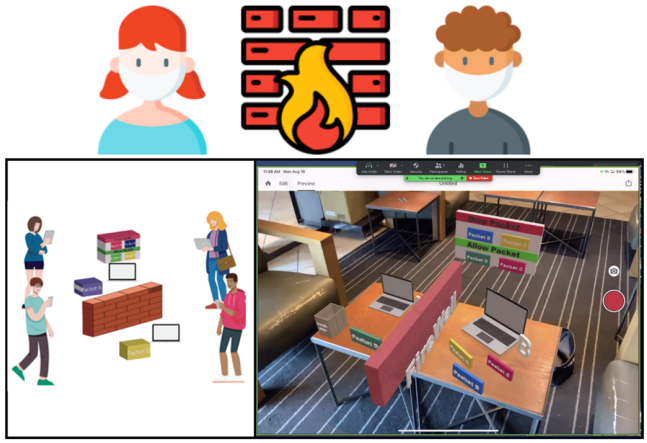

Fig. 1. At Left: Students collaborate on Firewall MR Activity via phones and tablets; At Right: MR View of Firewall Activity within Zoom

We propose a game-based firewall MR activity played between an attacker and a defender, as described in Figure 1, where the defender (Alice) specifies the colors of packets that are allowed to pass through the firewall. Packets of other colors will be dropped into a trash bin. Figure 1 depicts the "overall" MR view of a firewall activity shared within a Zoom session by the teacher, for instance. When the MR firewall game is played by two students, as defender and attacker, respectively, the "panel" above the table will be visible only to the student who plays Alice, the defender, so that she can specify which colors of packets are allowed to pass through the firewall and which colors of packets will be dropped into the trash bin.

B. Steganography

Steganography is an ancient technique for hiding information in plain sight. It is rumored that the ancient Greek would shave the head of a messenger and write a secret message on his bald head. Over time, his hair would grow in and hide the secret message. The messenger would pass through the enemy without anyone being aware that the secret message was right in front of them. The messenger would get his head shaved again when he was ready to deliver the message to the intended recipient. Technically, steganography is the practice of concealing messages or information within other non-secret data such as images or photographs.

Below we present how MR can be used to introduce the concept of steganography. In Figure 2, Alice chooses a picture (e.g., Eddie Peng) (Step 1), and scans the image through a steganography app to hide (encrypt) a secret message inside it (Step 2). Then, Bob tries to guess which photo contains the secret message and uses his steganography apps to scan (decrypt) each photo to find out (Step 3).

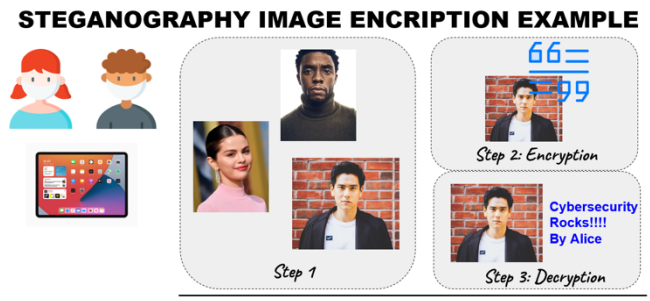

Fig. 2. Steganography with Interactive MR

C. *Phishing*

Phishing is the deceitful attempt to obtain personal information, such as SSN and credit card numbers, by disguising oneself as a well-known or trustworthy authority in the electronic form. Usually, hackers use emails, instant message, text, and social media to trick the users to click or enter a website which looks and feels like the genuine website they intend to browse; once the user clicks, they are asked to enter their personal information.

Below we present how MR can make the concept of Phishing concrete and interactive. In Figure 3, using the MR app, Alice and Bob first pick a social media message from the table.

Then, Alice and Bob discuss the content and figure out whether the selected item is a phishing message and whether to open the associated attachment. If they make the wrong choice, the MR app will play an animation showing, for instance, disappearance of apps on the iPad to demonstrate the damage caused by the phishing attack.

Fig. 3. Draft Phishing MR Activity

IV. Conclusion

In this paper, we proposed three interactive activities that make the abstract cybersecurity concepts of firewall, steganography, and phishing more tangible by using the MR technology to teach cybersecurity knowledge to middle school students. It is anticipated that these MR applications are to raise students' interest in cybersecurity and further pursue CS careers. Our plan is to complete the MR-based applications and evaluate their effectiveness with middle school students.

Acknowledgment

This work is supported by National Science Foundation under grant NSF DRL-2048874.

References

[1] Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National Initiative for Cybersecurity Education (NICE): Cybersecurity Workforce Framework. U.S. Department of Commerce.

[2] Libicki, M.C., Senty, D., & Pollak, J. (2014). H4cker5 wanted: An examination of the cybersecurity labor market. Rand Corporation.

[3] Mirkovic, J., Tabor, A., Woo, S., & Pusey, P. (2015). Engaging novices in cybersecurity competitions: A vision and lessons learned at {ACM} Tapia 2015." 2015 {USENIX} Summit on Gaming, Games, and Gamification in Security Education (3GSE 15).

[4] Morgan, S. (2019). Women represent 20 percent of the global cybersecurity workforce in 2019. Cybercrime Magazine, Mar. 28, 2019.

[5] Pusey, P. Gondree, M., & Peterson, Z. (2017). The outcomes of cybersecurity competitions and implications for underrepresented populations. In IEEE Security & Privacy, vol. 14, no. 6, pp. 90-95, Nov.-Dec. 2016, doi: 10.1109/MSP.2016.119.

[6] Wigfield, A., & Eccles, J. S. (2002). The development of competence beliefs, expectancies for success, and achievement values from childhood through adolescence. In A. Wigfield & J. S. Eccles (Eds.), A Vol. in the educational psychology series. Development of achievement motivation (p. 91–120). Academic Press.

[7] Chen, A., Darst, P. W., & Pangrazi, R. P. (1999). What constitutes situational interest? Validating a construct in physical education. Measurement in Physical Education and Exercise Science, 3(3), 157–180

[8] Radu, I. (2014). Augmented reality in education: A meta-review and cross-media analysis. Personal and Ubiquitous Computing 18, (6), 1533–1543.

[9] Kim, J., Marotta, K., Leo, J. Agarwal, S., Li, S., & Chau, D.H. (2019). Mixed reality for learning programming. Proceedings of ACM IDC conference, June 2019, https://doi.org/10.475/123_4.

[10] Fotaris, P., Pellas, N., Kazanidis, I., & Smith, P. (2017). A systematic review of Augmented Reality game-based applications in primary education. In Proceedings of the 11th European Conference on Games Based Learning (ECGBL17). Graz, Austria (pp. 181-190).

[11] Seo, D.W., & Lee, J.Y. (2013). Direct hand touchable interactions in augmented reality environments for natural and intuitive user experiences. Expert Systems with Applications, 40(9), pp.3784-3793.

[12] Radu, I. (2016). Exploring the usability of augmented reality interaction techniques during children's early elementary-school tears (Doctoral dissertation, Georgia Institute of Technology).

[13] Bovill, C., Cook-Sather, A., & Felten, P. (2011). Students as co-creators of teaching approaches, course design, and curricula: implications for academic developers. International Journal for Academic Development 16,2, 133–145.

[14] Lima, L., Araujo, C., Magalhaes, L.G., & Henriques, P. (2020). Learning resources with augmented reality. First International Computer Programming Education Conference (ICPEC 2020). Editors: Ricardo Queirós, Filipe Portela, Mário Pinto, and Alberto Simões; Article No. 15; pp. 15:1–15:8 Open Access Series in Informatics.

[15] Wen, Z. A., Lin, Z., Chen, R., & Andersen, E. (2019). What.Hack: Engaging anti-phishing training through a role-playing phishing simulation game. Conference on Human Factors in Computing Systems - Proceedings, 1–12. https://doi.org/10.1145/3290605.3300338

[16] Zhang-Kennedy, L., Baig, K., & Chiasson, S. (2017). Engaging children about online privacy through storytelling in an interactive comic. In Proceedings of the 31st British Computer Society Human Computer Interaction Conference (HCI '17). BCS Learning & Development Ltd., Swindon, GBR, Article 45, 1–11. DOI:https://doi.org/10.14236/ewic/HCI2017.45

[17] Malinverin, L., Valero, C., Schaper, M., & Pares, N. (2018). A conceptual framework to compare two paradigms of augmented and mixed reality experiences. Proceedings of IDC '18, June 19–22, 2018, Trondheim, Norway. https://doi.org/10.1145/3202185.3202750

[18] Shelton, B.E., & Hedley, N.R.(2002). Using augmented reality for teaching earth-sun relationships to undergraduate geography students. In the First IEEE International Workshop Augmented Reality Toolkit. doi: 10.1109/ART.2002.1106948

[19] Kirschner, P. A., Sweller, J., & Clark, R. E. (2006). Why minimal guidance during instruction does not work: An analysis of the failure of constructivist, discovery, problem-based, experiential, and inquiry-based teaching. Educational psychologist, 41(2), 75-86.

[20] Van Der Stappen, A., Liu, Y., Xu, J., Yu, X., Li, J., & Van Der Spek, E. D. (2019). MathBuilder: A collaborative AR math game for elementary school students. CHI PLAY 2019 - Extended Abstracts of the Annual Symposium on Computer-Human Interaction in Play, 731–738. https://doi.org/10.1145/3341215.3356295