UNIVERSITY OF ZAGREB
FACULTY OF ELECTRICAL ENGINEERING AND COMPUTING

MASTER THESIS No. 118

DEVELOPMENT AND EVALUATION OF AN AUGMENTED REALITY-BASED APPLICATION FOR COLLABORATIVE CYBERSECURITY TRAINING

Mirta Moslavac

Zagreb, June 2023

UNIVERSITY OF ZAGREB
FACULTY OF ELECTRICAL ENGINEERING AND COMPUTING

MASTER THESIS No. 118

DEVELOPMENT AND EVALUATION OF AN AUGMENTED REALITY-BASED APPLICATION FOR COLLABORATIVE CYBERSECURITY TRAINING

Mirta Moslavac

Zagreb, June 2023

UNIVERSITY OF ZAGREB
FACULTY OF ELECTRICAL ENGINEERING AND COMPUTING

Zagreb, 10 March 2023

MASTER THESIS ASSIGNMENT No. 118

Student:	**Mirta Moslavac (0036517647)**
Study:	Computing
Profile:	Computer Science
Mentor:	prof. Lea Skorin-Kapov

Title: **Development and Evaluation of an Augmented Reality-Based Application for Collaborative Cybersecurity Training**

Description:

Augmented Reality (AR) is a technology that enables the merging of the virtual and real worlds by displaying digital content in a real environment. This technology is increasingly being used in various fields, especially in education and training as a tool for creating interactive and visually appealing content for the purpose of acquiring new knowledge. Cybersecurity is a key topic in modern society, necessary for promoting the preservation of privacy, security, and trust in the use of today's information technologies. Consequently, it is becoming increasingly important to educate people on this topic. Augmented Reality can be utilized as an interactive learning medium for cybersecurity since it allows for the simulation of different attack scenarios, as well as the practice of protection and prevention procedures, through direct interaction with virtual objects. Your task is to implement a multi-user collaborative software solution in AR for cybersecurity training execution. Additionally, it is necessary to conduct a user study and investigate the Quality of Experience of the developed application based on the obtained data. All of the necessary literature and working conditions will be provided to you by the Department of Telecommunications.

Submission date: 23 June 2023

SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Zagreb, 10. ožujka 2023.

DIPLOMSKI ZADATAK br. 118

Pristupnica:	**Mirta Moslavac (0036517647)**
Studij:	Računarstvo
Profil:	Računarska znanost
Mentorica:	prof. dr. sc. Lea Skorin-Kapov

Zadatak: **Razvoj i evaluacija aplikacije za kolaborativni trening u području kibernetičke sigurnosti uporabom tehnologije proširene stvarnosti**

Opis zadatka:

Proširena stvarnost (engl. Augmented Reality, AR) tehnologija je koja omogućava spajanje virtualnog i stvarnog svijeta kroz prikaz digitalnih sadržaja u stvarnom okruženju. Ova tehnologija sve više nalazi primjene u raznim područjima, posebice u obrazovanju i treningu kao alat za stvaranje interaktivnog i vizualno privlačnog sadržaja u svrhu stjecanja novog znanja. Kibernetička sigurnost jedna od ključnih tema suvremenog društva. Nužna je u promicanju očuvanja privatnosti, sigurnosti i povjerenja u korištenju informacijske tehnologije današnjice, stoga je sve važnije educirati ljude o ovoj temi. Proširena stvarnost može se primijeniti kao imerzivno sredstvo za učenje o kibernetičkoj sigurnosti jer omogućava simuliranje različitih scenarija napada, kao i uvježbavanje postupaka zaštite i prevencije, kroz direktnu interakciju s virtualnim objektima. Vaš je zadatak implementirati višekorisničko kolaborativno programsko rješenje u proširenoj stvarnosti u svrhu provedbe treninga u području kibernetičke sigurnosti. Dodatno, potrebno je provesti korisničku studiju i izvršiti evaluaciju iskustvene kvalitete razvijene aplikacije na temelju dobivenih podataka. Svu potrebnu literaturu i uvjete za rad osigurat će Vam Zavod za telekomunikacije.

Rok za predaju rada: 23. lipnja 2023.

I am tremendously appreciative to my mentor, prof. Lea Skorin-Kapov, for her belief in my potential and the invaluable mentorship she has provided. Her guidance and support have opened doors to incredible opportunities that I deeply appreciate and cherish. I would like to also thank mag. ing. Sara Vlahović for her continued assistance and encouragement. Both of them have played vital roles in my academic growth, and I am truly fortunate to have had their guidance. Their contributions have not only shaped the past three years of my academic work but have also had a profound impact on my overall development as a researcher.

The most heartfelt thank you to my parents for showing me unwavering support not just for the past five years, but my entire life, especially during moments of zealous and ever-emerging aspirations that also accompanied my academic pursuits. To Cvetek, thank you for attentively yet cluelessly listening to my FER-related ramblings for the last five years. But, more importantly, thank you for being there for me through thick and thin for nearly a decade now – I am proud of each and every one of you and how much we have grown. Lara, you might be the worst partner in crime I could have asked for, but that makes it the best. Lastly, thank you to my two Legas who, through a serendipitous turn of events, showed me firsthand how life can change for the better within a year's time.

CONTENTS

Introduction **1**

1. Fundamental Theoretical Concepts **3**

2. Overview of Related Prior Research **7**

2.1. AR Training Solutions 7

2.2. Cybersecurity Training in VR 11

2.3. Cybersecurity Training in AR 14

3. Development of *SecuAR Together* **19**

3.1. Platform Choice 19

3.2. Used Technologies and Tools 20

3.3. Multiplayer Implementation 23

3.3.1. Networked User Connection and Synchronisation 23

3.3.2. Virtual Object Spatial Consistency 24

3.4. Scenario Descriptions 27

3.4.1. Scenario 0: Interaction Tutorial 28

3.4.2. Scenario 1: Password Break-In 29

3.4.3. Scenario 2: Password Creation and Analysis 34

3.5. Notable Mechanics 37

3.5.1. Preserving Game Object Transformation States 38

3.5.2. Analysing Passwords-Rule Relationships 39

3.5.3. Picking and Placing Rule Panels 41

3.6. Limitations 41

3.6.1. Anchoring Issues 42

3.6.2. Broken Synchronisation of Matched Rules 43

4. User Study **45**

4.1. Methodology 45

4.1.1. Experiment Design 45
4.1.2. Hardware and Software Set-Up 46
4.1.3. Procedure 47
4.1.4. Participants 48
4.1.5. Questionnaire 49
4.2. Results and Discussion 51
4.2.1. Application Experience 53
4.2.2. Collaborative Experience 54
4.2.3. Virtual Environment and Interaction Experience 58
4.2.4. General Outlook on XR and Training 62
4.2.5. Password Security Knowledge 63
4.2.6. Limitations 66

Conclusion **69**

References **70**

List of Figures **82**

List of Tables **83**

Abbreviations **84**

A. User Study Questionnaire **85**

INTRODUCTION

The existing landscape of cybersecurity training experiences is scarce in its offering of comprehensive solutions that effectively integrate augmented reality (AR) and cybersecurity principles [3, 99]. Moreover, there is a lack of AR-based cybersecurity solutions compatible with both mobile devices and head-mounted displays (HMDs). Nonetheless, in spite of these research and solution gaps, compelling justifications exist for the potential as to why AR can be a powerful tool for promoting cybersecurity awareness (CSA). AR offers an immersive experience by overlaying virtual elements onto the real world, further enhancing user engagement through the ability of active interaction with the augmented elements [11]. When it comes to CSA, the nature of AR can help users grasp complex concepts more effectively and make the learning process more engaging and enjoyable. In the form of an AR training scenario, users can directly experience the repercussions of their cybersecurity choices in real time, within their physical surroundings. This immersive experience can amplify the sense of realism, allowing users to truly grasp the tangible consequences of their actions. By providing an immersive and interactive learning experience, an AR training application can help bridge the gap between theoretical knowledge and practical application, fostering a culture of cybersecurity awareness and resilience.

Amongst the topical foci of currently available cybersecurity training solutions, password security emerges as a prominent area worthy of attention within the realm of AR training applications [96]. Its notable underrepresentation in this domain, coupled with its paramount importance, positions password security as an ideal subject for exploration and development within AR-based training platforms. Passwords are a fundamental aspect of digital security [101], and their importance cannot be overstated. However, despite their significance, many people still use weak passwords, reuse passwords across multiple accounts, or fall victim to phishing attacks that compromise their passwords. By focusing on password security, the application can address a topic that is both easy to understand and highly relevant in today's digital landscape. Password security is a universal concern that affects individuals, businesses, and organisations

across various sectors [57]. By educating users about the importance of strong and unique passwords, the risks of password reuse, and the techniques used by attackers to exploit weak passwords, an AR application can empower users to take proactive measures in order to protect their sensitive information in the future. Through the exploration of password-related concepts, a training application could lay the groundwork for users to develop a broader understanding of best practices in cybersecurity.

To address the aforementioned shortcomings, this thesis describes the development of *SecuAR Together*, an AR application that provides cybersecurity training in the field of password security with a focus on scenario-based and paired collaborative learning. To ensure accessibility for users across different platforms, the application supports multiple AR-capable devices, including HMDs and mobile phones. The application is further subjected to a comprehensive user study, aiming to examine various aspects related to the immersive and collaborative cybersecurity training. The user study aims to assess the overall user experience, considering factors such as interactivity, collaborativeness, and the impact of using different devices. In addition, the study seeks to evaluate the effectiveness of the training in enhancing participants' understanding and knowledge of password security principles.

The main focus of this thesis encompasses the following objectives:

1. review prior research concerning the enhancement of skill training and cybersecurity knowledge through the use of AR,
2. elaborate on the process involved in creating a collaborative cybersecurity training application that leverages AR and is supported across different devices, and
3. perform a quantitative user study to evaluate the efficacy and usability of the developed application.

These objectives are achieved in the six main chapters of the thesis. Following the introductory chapter, the subsequent chapter provides definitions to the the key concepts utilised within the thesis. The third chapter provides a comprehensive overview of previous work on the inclusion of extended reality (XR) technologies in the areas of training and cybersecurity. The following chapter delves into the process of developing a multi-device collaborative AR application for cybersecurity training. Additionally, the fifth chapter centres around a user study conducted to evaluate the aforementioned application. Ultimately, the thesis concludes by presenting a thorough summary and analysis of the achieved results. Furthermore, lists of references, figures, tables, and abbreviations employed throughout the thesis are also provided, along with the questionnaire form used in the study, which can be found in the appendix.

1. Fundamental Theoretical Concepts

An overview of the theoretical concepts that form the foundation for the research conducted in this thesis is given in Table 1.1, along with their descriptions. Definitions of concepts from various sources are provided in order to foster a shared understanding of these concepts, setting the stage for the remainder of the thesis. Notably, throughout the thesis, the term AR is used in alignment with the definition of mixed reality (MR) in the table, a conundrum formerly discussed by Billinghurst et al. [15].

Table 1.1: Descriptions of fundamental concepts referenced throughout the thesis

Theoretical Concept	**Description**
Augmented Reality (AR)	An environment containing both real and virtual sensory components. The Augmented Reality continuum runs from virtual content that is clearly overlaid on a real environment (Assisted Reality) to virtual content that is seamlessly integrated and interacts with a real environment (Mixed Reality) [44].
Mixed Reality (MR)	An environment containing both real and virtual components that are seamlessly integrated and interact with each other in a natural way [44].
Virtual Reality (VR)	An environment that is fully generated by digital means. To qualify as Virtual Reality, the virtual environment should differ from the local environment [44].
Extended Reality (XR)	An environment containing real or virtual components or a combination thereof, where the variable X serves as a placeholder for any form of new environment (e.g., Augmented, Mixed, Virtual) [44].

Continued on the next page

Table 1.1 – continued from the previous page

Theoretical Concept	**Description**
Immersion (adj. immersive)	A psychological state characterised by perceiving oneself to be enveloped by, included in, and interacting with an environment that provides a continuous stream of stimuli and experiences [43].
Cybersecurity	The process of protecting information by preventing, detecting, and responding to attacks [22].
Cybersecurity Awareness (CSA)	A learning process that sets the stage for training by changing individual and organisational attitudes to realise the importance of security and the adverse consequences of its failure [95]. The purpose of awareness presentations is to focus attention on security. Awareness presentations are intended to allow individuals to recognise IT security concerns and respond accordingly. In awareness activities, the learner is the information recipient, whereas the learner in a training environment has a more active role [94]. Awareness is used to reinforce the fact that security supports the mission of the organisation by protecting valuable resources. Awareness is also used to remind people of basic security practises [40].
Training	Teaching people the knowledge and skills that will enable them to perform their jobs more effectively [95]. Teaching people the skills that will enable them to perform their jobs more securely. This includes teaching people what they should do and how they should (or can) do it. Training can range from basic security practices to more advanced or specialised skills. Training is most effective when targeted to a specific audience [40].

Continued on the next page

Table 1.1 – continued from the previous page

Theoretical Concept	**Description**
Training Effectiveness	A measurement of what a student has learnt from a specific course or training event - learning effectiveness. A pattern of student outcomes following a specific course or training event - teaching effectiveness [95].
Gamification	Using game design elements in non-game contexts [12].
Game-Based Learning (GBL)	Learning that is facilitated by the use of a game. In addition to games, other game-like activities are often considered in relation to games-based learning: simulations aim to model realistic environments, virtual worlds offer interactive and explorative multi-user environments, role playing showcases different perspectives of imaginary situations, puzzles lack interaction and feedback, and stories are typically linear and noninteractive [81]. The theory of how learning occurs with the use of (primarily digital) games. Includes learning of some knowledge, skills, attitudes that happens with the deliberate use of digital games [12].
Serious Game	Synonym for GBL [81]. The term "serious game" is often mentioned in the literature as synonymous with the term "game-based learning." Game-based learning, however, can be seen as an approach to teaching in educational contexts [12]. With a specific learning goal in mind, a learning task is redesigned to make learning more interesting and effective. This involves the use of serious games in the learning process, seen as a tool of game-based learning [80]. A game designed specifically for purposes other than or in addition to pure entertainment [78].

Continued on the next page

Table 1.1 – continued from the previous page

Theoretical Concept	**Description**
Scenario-Based Learning (SBL)	A model of action-based learning: All learning that is orchestrated by some activity on the part of learners. Action-based learning models revolve around learners solving problems or addressing goals. The selection of authentic problem situations or scenarios that best represent reality is crucial for achieving desired learning outcomes [81].

2. Overview of Related Prior Research

2.1. AR Training Solutions

In recent years, XR technologies such as VR and AR have gained significant attention and have been applied to various domains, including medicine, military, psychology, and industrial maintenance. These immersive technologies offer unique opportunities to enhance training experiences, improve learning outcomes, and provide realistic simulations for trainees. The emphasis on exhibited prior research will predominantly be on AR, given its relevance in the research conducted within the context of this thesis.

AR training solutions have gained significant attention in the medical field, offering innovative approaches to enhance medical staff training and improve patient outcomes. In the domain of medical education, multiple studies have focused on evaluating the effectiveness and usability of AR training platforms. Sankaran et al. [77] conduct an evaluation of an MR training platform for sepsis prevention medical education, highlighting its potential to enhance clinical exposure for novice students. Similarly, Frøland et al. [34] investigate the application of MR for first aid trauma training, specifically focusing on wound treatment, and provided automated simulations and feedback to enhance individual training experiences. Liang et al. [52] explore the use of MR to enhance stroke assessment simulation experience for nursing school students, while Birt et al. [17] investigate the impact of mobile MR simulations on distance paramedic education. Developed by Bottino et al. [19], *Holo-BLSD* is an MR self-directed learning and evaluation training system for basic life support and defibrillation procedures, offering realistic haptic feedback, minimal instructor intervention, and comprehensive data logging for error identification and debriefing.

Expanding the scope to specific medical procedures, Eom et al. [29] introduce *NeuroLens*, an AR training solution for novice neurosurgeons, providing contextual guidance and improving the accuracy of catheter placement in external ventricular drain procedures. Abhari et al. [1] propose an XR system, offering both VR and AR modes,

for training neurosurgical residents in planning brain tumor resection, demonstrating improved performance and reduced time for clinically relevant tasks compared to conventional planning environments. Zhao et al. [100] present an MR training framework for neonatal endotracheal intubation, offering real-time guidance, automated assessment, and augmented feedback to enhance training effectiveness. Sielhorst et al. [85] introduce an MR extension to a birth simulator, allowing in-situ body visualisation and improving training efficiency. Rebol et al. [74] develop an MR system for remote training in central venous catheter placement, providing enhanced visual guidance compared to traditional video-based methods. Yong et al. [97] explore the application of AR in otologic and head and neck micro-surgical training, highlighting its potential to improve trainee learning outcomes. Wang et al. [92] develop an AR telemedicine platform for remote medical training, with a specific focus on ultrasound, comparing it to a traditional telemedicine setup.

In the context of assistance and real-time use, De Mauro et al. [28] showcase the first MR system integrated into a real microscope, specifically designed for training and intraoperative assistance in the field of neurosurgery. Maas et al. [54] present an XR telemedicine system that utilises both VR and AR to enable remote collaboration between expert and inexperienced physicians for ultrasound diagnostics and interventions in acute care settings.

Several studies have explored the application of AR to enhance patient rehabilitation processes. Jin et al. [47] develop an AR iOS application for gait rehabilitation in stroke patients, along with wireless sensors and a smart carpet for motion measurement. Sharma et al. [83] introduce an MR training application for upper limb amputees, incorporating additional tactile and proprioceptive feedback to improve performance, reduce prosthesis training time, and enhance completion rates. Evans et al. [31] investigate the use of MR with visual feedback as a method for rehabilitation during overground walking, specifically promoting goal-directed changes in walking behaviour. De Cecco et al. [27] present an MR framework for rehabilitation and skill assessment, enabling shared AR experiences between therapists and patients, fostering empathy, and enhancing patient engagement.

AR training solutions have also been explored in the field of veterinary training. Pan et al. [66] introduce an AR training solution that incorporates in-situ augmented data visualisation and context-aware light field displays, providing targeted teaching decisions and support by enabling real-time monitoring of students.

AR training solutions have also found applications in the military domain, offer-

ing innovative approaches to enhance training effectiveness and reduce costs. Schaffer et al. [79] propose the use of AR to enhance Marine Corps training by providing realistic pre-deployment training and utilising augmented training areas, which can replace live supporting forces and result in cost savings. Similarly, Piedimonte and Ullo [70] examine the applicability of MR in maintenance and training processes in the Italian Air Force, highlighting its potential to centralise resources, minimise expenses, and improve efficiency in remote guidance and assistance. Furthermore, Ai et al. [4] showcase an embedded military training system using MR, which enables the rapid development of mission-specific environmental models and synthetic characters. This system provides a realistic and adaptable training environment, allowing military personnel to acquire critical skills in a simulated setting. In evaluating different technologies for military training, Guzmán et al. [41] compare the effectiveness of MR and tablet technologies. They find that traditional tablet applications offer similar levels of situation awareness at reduced cost and increased usability compared to MR technologies.

In the field of psychology, AR training solutions have been explored to enhance various aspects of psychological interventions. Greenberg and Spitaletta [39] present the development of an MR social prosthetic system called *IN:URfACE*, which aims to enhance emotion recognition training and performance. This system overlays synchronised nonverbal signals onto the face of an interaction partner through an HMD. Chiam et al. [20] showcase an AR-enhanced solution for vocational rehabilitation in individuals with psychiatric and neurodevelopmental disabilities. This cost-effective training approach offers opportunities for skill development, social interaction, and potential re-employment. The training scenarios simulate real-world vocational settings, promoting skill acquisition and fostering social integration.

In the realm of industrial maintenance and assembly, extensive research has been done to explore the effectiveness and advantages of AR in enhancing training outcomes, offering realistic simulations, interactive guidance, and heightened user engagement. Besbes et al. [14] introduce an AR prototype for industrial maintenance training, utilising an HMD and a laser pointer for user interactions, with the aim of training users for specific maintenance tasks. Similarly, Aziz et al. [10] propose an MR training solution for engineering maintenance, with a focus on machine part maintenance and assembly, enhancing participant understanding. Wang et al. [91] explore the effectiveness of combining three-dimensional (3D) gestures and computer-aided design (CAD) models in an MR remote collaboration system for assembly training.

The study shows improved performance and user experience in the training process. Møsbæk and Bjørner [58] explore the application of AR in specific industrial context, examining an AR training application for field engineers in medical analyzer service and maintenance.

Furthermore, research has dedicated attention to evaluating the effectiveness of AR in industrial training, both in comparison to traditional methods and other XR technologies. Gonzalez-Franco et al. [38] investigate the effectiveness of MR as a training solution for complex manufacturing processes, comparing it to conventional face-to-face training. The study finds equivalent knowledge retention between MR and face-to-face training, but with potential cost reduction and improved safety. Daling et al. [23] compare AR and VR technologies for assembly of a pneumatic cylinder. The study examines usability, ergonomics, and perceived task load and found significant differences in usability, with a majority of participants preferring the VR system for industrial training purposes. However, no significant differences are observed in ergonomics and task load. A similar study by Daling et al. [24] investigates the effectiveness of AR and VR-based training compared to video-based training in manual assembly tasks. While no significant difference is found in objective performance, AR and video training received better subjective evaluations, suggesting that AR may be a more suitable alternative for achieving short- and long-term training success. Gavish et al. [35] evaluate the effectiveness of VR and AR training platforms for industrial maintenance and assembly tasks. The study highlights the advantages of AR in reducing errors and improving cognitive understanding, demonstrating its potential in improving training outcomes. Liu et al. [53] investigate the impact of VR and AR training on the effectiveness of professional maintenance personnel, with a specific focus on multi-level maintenance tasks. The study's findings show that AR outperforms VR and traditional training methods for such tasks, highlighting its superiority in training effectiveness.

In the realm of interactive learning and skill development, AR training solutions have been explored in various domains. Zhai et al. [98] propose an intelligent MR cooking system designed to address the memory and learning challenges faced by novice cooks in the kitchen. By leveraging MR presentation and focusing on five key aspects of cooking, this system aims to enhance the user experience and cooking effectiveness. Furthermore, Gonzalez et al. [37] conduct a comparative study between AR and desktop interfaces for authoring SBL content. Their findings reveal no significant differences in task completion time or perceived usability, indicating that AR

interfaces can provide comparable user experiences to traditional desktop interfaces in the context of SBL content creation.

In the context of music education, MR has also been utilised to enhance piano pedagogy. Birhanu and Rank [16] explore the use of MR in piano instruction, specifically focusing on notation literacy. Their application, called *KeynVision*, introduces beginners to octave scales, chords, and arpeggios through MR technology. Similarly, Gerry et al. [36] introduce *ADEPT*, an MR application for piano training that employs augmented embodiment, audio-visual perspective taking, and feedback to enhance motor learning and performance. In contrast to the previous solution, their approach emphasises muscle memory over symbolic musical notation.

2.2. Cybersecurity Training in VR

The field of immersive cybersecurity education and training has witnessed the emergence of VR technology as a powerful tool. In response to the ever-increasing complexity and sophistication of cyber threats, there is a pressing need for innovative approaches that effectively educate individuals and strengthen their cybersecurity knowledge and skills. This has prompted several research papers to explore the application of VR in the realm of cybersecurity, with the goal of developing effective training environments and tools. This section presents a diverse collection of studies that delve into the use of VR in cybersecurity education, encompassing serious games, role-playing games, and the consideration of integration of elements such as digital agents, haptic feedback, and immersive storytelling in order to further strengthen the effectiveness of acquiring cybersecurity knowledge through VR. These studies provide valuable insights into the potential of VR as a medium for enhancing cybersecurity awareness and knowledge.

Williams and El-Gayar [93] adopt SBL and gamification principles in the proposition of a collaborative VR cybersecurity escape room prototype. The application is structured as a serious game that integrates storytelling elements and incorporates essential cybersecurity skills, including social engineering and password security. Specifically, in terms of password security, participants engage in answering password recovery questions. The integration of VR technology in the development of role-playing games (RPG) for cybersecurity education is emphasised by Jin et al. [46]. They highlight the effectiveness of GBL in teaching cybersecurity principles and present various games, including two VR RPGs focusing on social engineering and secure online be-

haviour. The favourable reception and engagement exhibited by students indicate the effectiveness of these immersive games as tools for CSA training.

Also building on the effectiveness of GBL, Veneruso et al. [90] introduce *CyberVR*, a VR game designed to educate users about cybersecurity. The game comprises six mini-games covering different cybersecurity topics and aims to raise awareness among players. A user study with 40 participants was conducted to evaluate the effectiveness of *CyberVR* compared to traditional textbook learning. The results indicate that CyberVR is equally effective, if not more, in teaching cybersecurity while being more engaging, showcasing the potential of *CyberVR* as an alternative learning tool for cybersecurity education.

Based on research comparing conventional cybersecurity training approaches and their VR counterparts, Ulsamer et al. [87] contrast the effectiveness of 360° VR video with traditional text-based e-learning methods. The study explores the use of immersive VR storytelling to improve knowledge and learning outcomes in cybersecurity, more precisely, social engineering. Notably, the participants in the study were unable to interact with the actors featured in the VR videos. The results reveal that users exposed to VR video outperform those exposed to traditional methods on an information security awareness test, demonstrating more sustainable learning. The story-based VR experience is found to be immersive and engaging, facilitating easier comprehension and application of knowledge. These findings suggest that immersive storytelling in VR video holds promise for enhancing knowledge and behaviour in social engineering. As a follow-up work by Fertig et al. [33], training within a fully interactable VR virtual environment is compared to video training for increasing knowledge in CSA. The study theoretically establishes the potential for sustainable knowledge enhancement through VR training. However, contrary to previous research, no sustainable increase in CSA knowledge is observed compared to video training.

Rana and Alhamdani [72] propose a framework to compare the efficacy of VR cybersecurity training with traditional video-based methods. Their framework involves developing a VR simulation and a video-based training format to teach physical cybersecurity concepts, followed by assessments through quizzes and surveys. The analysis of learning outcomes and participant feedback aims to evaluate the effectiveness and engagement of VR training in cybersecurity, contributing to a better understanding of the impact of VR in cybersecurity education. Based on the need to examine the effectiveness of VR cybersecurity training, the same authors present an ontology-based framework that integrates VR environments and interactive simulations. The

framework presented in Rana and Alhamdani [73] enhances VR cybersecurity training programmes and encompasses seven phases, ranging from module selection to its development and evaluation. By addressing the unique aspects of VR simulations and games, this research aims to augment the efficacy of cybersecurity training.

Bernsland et al. [13] showcase *CS:NO*, a VR prototype aimed at teaching cybersecurity basics. Alongside VR, haptic feedback is utilised to create an immersive learning environment where users can interact with virtual representations of data packets and explore abstract cybersecurity concepts such as encryption, decryption, firewalls, and malicious data. In order to provide haptic elements, they employ thermal sensors to enhance the sense of presence and provide multisensory experiences. This paper addresses the difficulties of visually representing abstract cybersecurity concepts in VR and introduces the initial design of CS:NO. Key elements of the design, including the network highway, firewall, data packet representation, as well as interactive decryption processes, are highlighted. The authors also explore the use of narrative design in the given context.

VRCyberEducation, an educational VR application developed by Klooster [50], is also dedicated to improving knowledge on cybersecurity basics, as well as reducing human errors in cybersecurity. The scenario-based application allows users to perform basic cybersecurity tasks and monitors their knowledge and behaviour, providing feedback upon completion. The evaluation reveals a significant improvement in cybersecurity performance among participants exposed to the VR application. Additionally, the application received above-average usability scores, highlighting its effectiveness as an educational tool in the field of cybersecurity.

Adinolf et al. [2] explore the potential of digital agents in VR environments for cybersecurity training and provide design insights classified as thematic, stylistic, and mechanical. The thematic findings suggest employing metaphors and narrative spaces instead of a direct cybersecurity presentation. Stylistically, a stylised or cartoon-like art style is recommended for both the environment and the agent to avoid the uncanny valley effect, emphasising non-verbal engagement. In the mechanical aspect, simple VR interactions such as pushing, grabbing, pointing, and throwing are suggested. Additionally, the agent can be used to mimic user actions or as a hint system.

Focusing on the application of VR cybersecurity training in specialised domains, Kasurinen [49] explore the usability issues of VR learning simulators for the prevention of cybersecurity threats in hospitals. The study focused on evaluating the usability

and user experience aspects of a mixed-method VR environment applied in the cybersecurity domain. Three scenario-based user interface solutions were tested: no VR, where participants used a computer to explore the implemented virtual environment and utilise the cybersecurity tools; semi-VR, where activities within the virtual environment were executed using a VR headset, while using cybersecurity tools separately on a computer; and full VR, where all activities were conducted within the VR environment. The findings indicate that the full VR approach offered the highest level of immersion and usability, enabling users to effectively complete tasks within the virtual environment. However, the study also acknowledges the importance of integrating real-life tools and ensuring tactile and responsive user interfaces.

Furthermore, Dattel et al. [26] present a study on the use of VR training to improve the identification of cyber threats in the field of naval operations. The developed application immerses participants in a simulated U.S. Navy destroyer environment where they encounter hacking incidents and must identify and mitigate cyber threats. The findings indicate that the trained shipmen showed significant advancements in their knowledge and performance in handling cyber threats, particularly early in the programme, compared to a control group.

Seo et al. [82] introduce the *CiSE-ProS* VR training programme designed to enhance physical cybersecurity education. The programme focuses on four scenarios set within a virtual data center environment and specifically targets high school students in institutions with limited access to physical data centers. The feedback from study participants highlighted their positive experiences with VR, emphasising the interactive, realistic, and immersive nature of the technology. Furthermore, participants demonstrated a strong retention of cybersecurity knowledge.

2.3. Cybersecurity Training in AR

In contrast to the extensive research and development of VR solutions in the field of cybersecurity, the exploration of AR in this domain has received relatively less attention. While VR has been extensively studied for its potential in enhancing cybersecurity training and education, the application of AR in cybersecurity is an emerging area that holds great promise. However, despite its potential benefits, the research and development of AR solutions in cybersecurity is still in the nascent stages. This section delves into the limited but notable research efforts that have been undertaken to explore the intersection of AR and cybersecurity, shedding light on the innovative applications, educational tools, and visualisation techniques.

Most notably, Alqahtani and Kavakli-Thorne [5] developed *CybAR*, an AR game designed to enhance cybersecurity awareness and knowledge acquisition. The game aims to educate users about various cyberattacks and ways to prevent them in an engaging and entertaining manner. The game incorporates real cybersecurity case studies, covering topics such as phishing, identity theft, ransomware, and social media-based attacks. Following a situated learning theory, *CybAR* emphasises collaborative problem-solving and integrates pedagogical approaches such as constructivist, game-based, and inquiry learning. Users engage in gamified tasks, earn points, receive feedback, and can compare their progress on leaderboards. The effectiveness of *CybAR* is evaluated through an experimental study involving 91 participants, demonstrating positive responses and increased awareness of cybersecurity practices.

Subsequently, the authors extend their investigations by conducting further research that specifically delves into distinct aspects of cybersecurity in conjunction with AR, as factors affecting user behaviour, acceptance of the game, decision-making styles, and the impact of gamification techniques, while leveraging the previously developed *CybAR* application as their experimental platform. In Alqahtani and Kavakli-Thorne [8], the authors focus on exploring factors influencing the acceptance of *CybAR*. It examines the relationship between attitudes, intentions, and actual behaviour, considering personality traits and cultural differences in order to identify predictors of *CybAR* usage and understand users' acceptance. They show that personality traits, such as agreeableness, conscientiousness, neuroticism, openness, and extraversion, play a role in the acceptance of *CybAR* by users. Alqahtani et al. [9] focuses on the specific impact of gamification factors on the acceptance of *CybAR* for CSA. It addresses the gap in understanding the factors that influence the acceptance of AR applications by analysing the effects of gamification in the context of cybersecurity. The study explores the relationship between gamification factors, user acceptance, and cybersecurity awareness in the context of the *CybAR* game. The findings demonstrate that the implementation of gamification techniques in *CybAR* significantly enhances users' acceptance of the game as a means of promoting cybersecurity awareness. Through the GBL approach, *CybAR* effectively educates users and effectively raises their understanding of cybersecurity issues. These results highlight the importance of developing augmented reality applications that prioritise user education and awareness in the realm of cybersecurity. The factors affecting users' cybersecurity behaviour by using *CybAR* are explored in Alqahtani and Kavakli-Thorne [7]. The researchers identify key elements that should be addressed in the game to prevent cybersecurity attacks and assess

that individual differences, such as demographic factors, personality traits, domain-specific risk-taking scale, and general decision-making style, significantly influence motivation and behaviour to avoid cybersecurity. Similarly, the work of Alqahtani and Kavakli-Thorne [6] investigates the role of decision-making styles in avoiding risky cybersecurity behaviour using *CybAR*. The study finds that decision-making styles significantly moderate the relationship between avoidance and cybersecurity avoidance behaviour. The rational decision-making style has been shown to have a strong influence on avoidance and cybersecurity avoidance behaviour, while dependent and avoidant styles have a lesser impact.

The work of Korkiakoski et al. [51] investigates the use of AR and gamification to enhance training and overall experience of using an ethical hacking game, where participants complete capture the flag (CTF)-style objectives by executing Linux terminal commands. A pilot study involving three cybersecurity experts and three cybersecurity novices was conducted to assess the game's impact on situational awareness and learning. The study employed dedicated questionnaires tailored for each group. Notably, an intriguing finding emerged as novice participants displayed noticeable progress over time, gradually catching up with the experts. This outcome highlights the potential of the AR application in equalising opportunities and promoting effective learning, regardless of participants' initial skill levels.

Another study that explores the intersection of AR, cybersecurity education, and gaming is conducted by Salazar et al. [76]. They introduce an AR-based serious game designed to enhance cybersecurity learning for high school students. It addresses the challenge of conveying complex cybersecurity concepts to this demographic via a presentation by allowing students to interact with tangible representations of cybersecurity concepts. The researchers propose two approaches to AR in the context of their application: AR lenses, where users view an augmented version of the real environment through a mobile platform, and AR mirror, where a fixed camera and display connected to a computer create an augmented reality effect. They employ the AR mirror paradigm using custom marker recognition algorithms, allowing users to interact with virtual objects and explore structures by rotating markers with their hands. The game focuses on key threats faced by high school students, such as identity theft and malware, and proposes countermeasures such as robust passwords and multi-layer security. The study's findings demonstrate that the serious game effectively reinforces understanding of cybersecurity concepts by providing users with tangible experiences and an interactive context for experimentation.

Tan [86] introduce an AR application for security officer training. Their approach utilises a marker-based system with QR codes and mobile device as an AR device. The study demonstrates the effectiveness of this approach in creating an immersive learning environment and employing scenario-based learning (SBL), allowing trainers to design customised training scenarios.

Shen et al. [84] aim to address the scarcity of cybersecurity professionals by employing AR to captivate middle school students and foster their interest in cybersecurity careers. Through the creation of interactive activities focused on steganography, phishing, and firewalls, the authors aim to make abstract cybersecurity concepts more accessible, enhancing student understanding and engagement. The research presents prototyped interactive cybersecurity activities and establishes design principles for the development of concrete and interactive educational content. The anticipated outcome of this research is to advance cybersecurity education and stimulate career interest among students. Notably, the same authors delve deeper into the concept of phishing in their following work (Chiou et al. [21]), where they develop a mobile AR-based cybersecurity education application. It is worth mentioning that this AR phishing prototype is the same one noted in the preceding paper. The paper presents related work on AR education and cybersecurity training for phishing, as well as discusses the design and prototype of the AR based phishing application. The goal is to provide remote access to cybersecurity education for school children and enable them to differentiate between malicious and genuine messages. The application involves students using iPad devices to discuss messages on a table and decide whether to open attachments or links based on their digital content.

Existing research efforts in AR visualisation focus on industrial applications and wireless network control, while limited work has been done in visualising network security data. Mattina et al. [56] propose a mobile phone AR platform for real-time and space-based visualisation of diverse security data. Two prototype applications been developed for visualising intrusion detection (*CovARVT*) and wireless association data (*ConnectAR*). These prototypes demonstrate the potential of AR in enhancing user situational awareness and threat response. The integration of AR in network security visualisation can provide analysts with new perspectives and aid in combating cyber threats effectively. However, further research is required to address the challenges and expand the scope of AR-based cybersecurity visualisation.

Similarly, Joshi [48] introduces an AR approach to enhancing the comprehension of data flow in cybersecurity for network operators and security analysts. The proposed solution integrates digital and physical components by mapping devices in the environment and augmenting device-specific information. Through the development of a mobile phone prototype application, the accompanying case study demonstrates the effectiveness of the visualisation method using adaptive interfaces and gesture controls. The application proves to be successful in enhancing threat mitigation by eliminating the need for manual localisation and enabling faster threat identification. In general, the study emphasises the potential of AR in enhancing situation awareness in the field of cybersecurity.

3. Development of *SecuAR Together*

The developed application is an immersive and collaborative training solution designed to enhance cybersecurity knowledge. It leverages AR technology to create a realistic and engaging learning environment. The application is specifically designed for use in pairs and each user has the flexibility to choose their preferred AR device to use this application on, including the HoloLens 2, an Android mobile phone, or an iOS mobile phone. However, it is important to note that the application has been primarily tested on the HoloLens 2 and Android devices, while its performance on iOS devices requires further evaluation.

The primary goal of *SecuAR Together* is to provide users with hands-on experiences and interactive simulations of real-life cybersecurity scenarios in AR, while leveraging a GBL approach combined with SBL at the same time. By immersing users in a virtual environment, the application aims to improve their understanding of cybersecurity concepts and foster a proactive mindset towards cyber threats. The application provides a dynamic training experience by combining educational content, interactive tasks, and collaborative features, organised into two distinct scenarios.

3.1. Platform Choice

The application aims to cater to a broad user base by targeting a range of AR-capable devices. This approach acknowledges that users may have varying levels of access to AR devices based on factors such as affordability, availability, or personal preferences. By accommodating multiple platforms, the application ensures that a wider audience can benefit from the training experience, regardless of the device they own or have access to. As mentioned, affordability is an essential consideration in this context. Mobile phones, often considered lower-end devices, are widely accessible to a significant portion of the population. By taking into account during application development that these devices are one type of possible end devices and ensuring a smooth ease of use on these devices, this opens up opportunities for widespread ap-

plication dissemination, even among individuals who may not have access to high-end AR hardware like HMDs. This inclusivity aligns with the aforementioned goal of promoting cybersecurity awareness and education to a broader audience, irrespective of their device limitations.

In spite of that, the disparity between the AR experience using an HMD, such as the HoloLens 2, and a mobile phone deserves attention and careful consideration [71]. The HoloLens 2 offers a hand gesture-based experience, eliminating the need for users to hold the device and enabling more seamless and natural interactions with the virtual environment. Furthermore, its ability to track head movement enhances the alignment of virtual objects with the user's perspective, creating a heightened sense of depth. In contrast, mobile phone users are limited to interacting with the virtual environment through a two-dimensional (2D) screen, introducing a physical barrier that impedes realistic interactions with virtual objects compared to the direct manipulation in a 3D space. However, depending on their screen size, mobile phones generally provide a slightly wider field of view (FoV) compared to the much more constricting and narrow FoV of the HoloLens 2 [59]. Moreover, the quality of the rendered virtual objects is much sharper and clearer on a mobile device, as the semi-transparent representation of virtual objects on the HoloLens 2, due to its optical see-through approach, can affect visual clarity. Figures 3.4a and 3.4b provide visual representations of the distinctions between the FoVs and renders of the two devices within the context of this application. These differences in device-specific user experience (UX) need to be taken into consideration when developing an AR application intended to be used on multiple platforms.

3.2. Used Technologies and Tools

Unity is a 2D and 3D cross-platform game engine developed by *Unity Technologies* [42]. Although the engine is written in C++, the scripting aspect of games developed in the engine is done in C#. Unity allows for seamless deployment of content across various platforms, including desktop, mobile, web, console, TV, VR and AR. For this application, version 2020.3.47f1 was chosen.

Mixed Reality Toolkit (MRTK2)[1] is an open-source development toolkit for MR application development by *Microsoft*. It is the successor to *HoloToolkit* released in 2017 [32]. Developed specifically for the Unity game engine, **MRTK-Unity** serves

[1] `https://learn.microsoft.com/en-us/windows/mixed-reality/mrtk-unity/mrtk2/`

as an adapted version of MRTK with pre-implemented core functionalities. Among its functionalities, MRTK-Unity provides a cross-platform input system and building blocks for spatial interactions and user interface (UI) elements. MRTK-Unity supports various devices, including Microsoft HoloLens 2, Windows Mixed Reality headsets, Meta Quest, and devices running on SteamVR via OpenXR. It seamlessly integrates with Android and iOS platforms via AR Foundation through the ARCore and ARKit XR plug-ins, respectively. Currently, MRTK3[2] is in its final stages of development. MRTK version 2.8.3 was used for this application.

In order to build applications targeted for HoloLens 2 and leverage AR capabilities such as spatial anchoring, the preferred XR plug-in within Unity is the Mixed Reality OpenXR plug-in. **OpenXR**[3], an open and royalty-free standard established by *Khronos*, provides a cross-platform Similarly, for Android-based AR application development, the recommended choice is **ARCore**[4], a cross-platform AR SDK offered by *Google*.

AR Foundation[5] is a framework within the Unity engine, which facilitates the development of multi-platform AR applications. AR Foundation seamlessly integrates with the native AR software development kit (SDK) of the target platform, granting the ability to create and distribute AR experiences across various platforms, such as the ARCore XR plug-in for Android, ARKit XR plug-in for iOS, and OpenXR plug-in for HoloLens 2, within a single Unity project. It is important to note that AR Foundation solely provides interfaces for AR features, necessitating the utilisation of separate provider plug-in packages specific to each platform. The version used was 4.2.7

Photon Unity Networking (PUN2)[6] is a Unity networking package, developed by *Photon Engine*, that improves upon and expands the capabilities of Unity's native networking system. By leveraging Photon's communication and matchmaking features, PUN2 provides developers with an application programming interface (API) that closely resembles Unity's built-in networking API. PUN2 is specifically designed to simplify the implementation of real-time and cross-platform multiplayer experiences,

[2] https://learn.microsoft.com/en-us/windows/mixed-reality/mrtk-unity/mrtk3-overview/
[3] https://www.khronos.org/openxr/
[4] https://developers.google.com/ar/
[5] https://docs.unity3d.com/Packages/com.unity.xr.arfoundation@5.0/
[6] https://www.photonengine.com/pun/

and provides seamless game object synchronisation, client-server model, and the aforementioned matchmaking features. The PUN2 version used during the development of the application was 2.33.3.

Azure Spatial Anchors (ASA) serves as a managed cloud-based solution and developer platform, empowering the creation of multi-user mixed reality experiences that are spatially aware [63]. It facilitates seamless Unity integration across a range of XR-capable devices, including HoloLens, iOS (ARKit), and Android (ARCore). The sevice enables users to collaboratively engage with immersive content in the context of their physical surroundings. ASA provides a versatile platform that empowers developers to create multi-user mixed reality applications, enable way-finding experiences, and integrate virtual content persistence into real-world environments. Different types of ASA SDK should be included into the Unity project in order to provide support for a specific platform. For this particular application, the Core, Android, and Windows SDKs (version 2.13.3) were incorporated.

The application development process employed two integrated development environments (IDEs), namely *JetBrains*' **Rider**[7] and *Microsoft*'s **Visual Studio 2022**[8]. On the one hand, Rider, version 2022.2.3, was used for Unity's scripting purposes for the application itself. On the other hand, Visual Studio, version 17.5.5, was also used to build and deploy the application on the HoloLens 2 device.

To obtain 3D models for the application, the **Unity Asset Store**[9] and **Sketchfab**[10] were utilised as valuable resources. The Unity Asset Store operates as a comprehensive marketplace, offering a wide range of pre-built assets, including 3D models and scripting elements. Additionally, Sketchfab provides a vast library of user-generated 3D models, offering a diverse selection of objects and environments.

[7] https://www.jetbrains.com/rider/
[8] https://visualstudio.microsoft.com/vs/
[9] https://assetstore.unity.com/
[10] https://sketchfab.com/

3.3. Multiplayer Implementation

This chapter addresses two pivotal aspects of multiplayer functionality in this application: networked collaboration and spatial consistency of objects in both the real and virtual world. To facilitate the collaborative aspect, the PUN2 networking framework is utilised, enabling seamless interaction and synchronisation among multiple users. Additionally, the ASA service is employed to anchor virtual content in real-world locations, ensuring spatial consistency across different devices. The integration of these technologies, their functionalities within the application, and the design considerations involved in their implementation are discussed in the remainder of the section.

3.3.1. Networked User Connection and Synchronisation

To support the collaborative aspect of the application, where two users join the application to participate in a single cybersecurity training session, it is important to have a reliable networking solution. Although Unity offers some built-in networking capabilities, they do not fully meet the requirements for seamless multiplayer interactions. To overcome these limitations, the application leverages PUN2, a simple networking framework that extends the native Unity functionality. It introduces the concept of client matchmaking into lobbies and rooms, allowing users to connect and synchronise their actions, interact with virtual objects and collaborate within a shared virtual environment [68]. The framework handles tasks such as player authentication, network latency management, and remote procedure calls (RPCs).

To meet the needs of the application, the free version of PUN2 is used, which supports up to 20 concurrent clients. This capacity is sufficient for the collaborative nature of the training sessions in pairs. The application utilises a centralised client-server architecture, facilitated by dedicated Photon servers situated in different geographic regions [68]. Specifically, the application designates the EU region to ensure that users who launch the application are seamlessly connected to the same lobby upon entering.

Within the application, a Photon room is established to facilitate a single cybersecurity training session. Room creation is initiated by the Master client, which is determined as the first user to enter the application among the two participants. The Master client assumes the role of Player 1, while the second user to join is regarded as a regular client, referred to as Player 2. The application establishes communication with the Photon Cloud service through the input of an App ID within the Unity project. This unique identifier is acquired through the registration process for a Photon account

and the subsequent creation of a dedicated "App" within the Cloud Dashboard.

Photon is utilised for user authentication, creating a Photon room to coordinate the two clients, managing object instantiation and destruction in various scenarios and facilitating RPCs to synchronise user actions. The primary namespace employed for the application's network code is `Photon.Pun`, with the occasional usage of the `Photon.Realtime` namespace. To invoke methods targeting one or both clients within the Photon room, RPCs were employed, allowing for the execution of methods marked with `[PunRPC]` through the specific `PhotonView` of the game object in question. The presence of the `PhotonView` component indicates that the object is a Photon networked object with a unique `viewID`. Examples of instances where RPC methods were used include switching between scenarios, verifying the entered password in Scenario 1, sharing individually entered passwords and performing password analysis in Scenario 2, as well as synchronising rule movement in Scenario 2.

3.3.2. Virtual Object Spatial Consistency

In order to enable real-time rendering of virtual content in specific real-world locations for multiple users, the utilisation of a tracking solution becomes imperative. Given the limitations encountered with marker-based AR tracking using Vuforia [59], a markerless approach was adopted to address these challenges effectively. ASA, a spatial anchor solution, emerged as the most suitable out-of-the-box service due to its simultaneous support for both HoloLens and mobile devices (Android and iOS), aligning with the targeted devices for the application. These devices employ visual simultaneous localisation and mapping (SLAM) algorithms to track feature points in captured images, resulting in a sparse local point cloud map [30], as depicted in Figure 3.1.

ASA operates by establishing a network environment that enables real-time rendering of content in specific real-world locations. To create or locate an anchor, the client SDK captures environment images, which are processed on the device to generate a sparse point cloud [61]. This point cloud, which contains visual characteristic hashes without pixel data, is securely transmitted and stored on the ASA cloud infrastructure within a designated geographic region. Anchors are isolated based on associated Azure accounts, ensuring access only for authorised applications. The sparse local maps are then matched with larger global maps stored in the cloud. ASA leverages device-specific AR trackers, utilising cameras to perceive the environment and track device movement in 6 degrees of freedom (6DoF) [61]. By designating anchor points

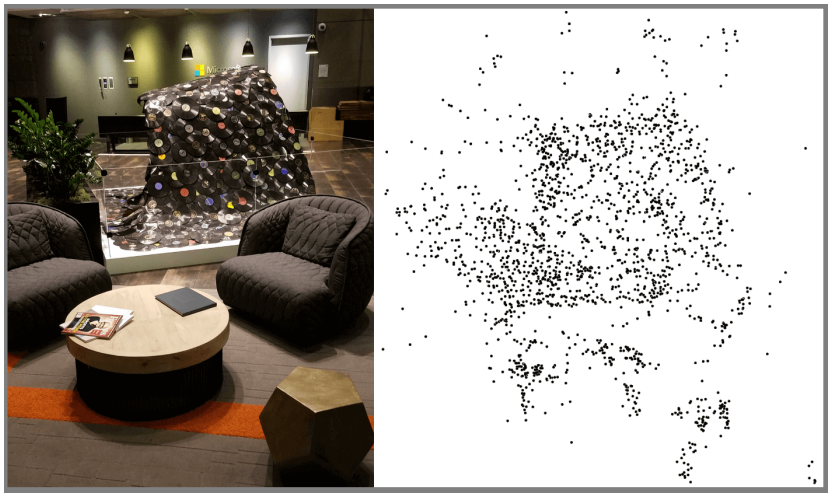


Figure 3.1: Real-life environment and the resulting sparse point cloud (source [61])

of interest, ASA captures and transmits environment data for storage. When another device queries the same anchor using a local map, its data are matched against the previously stored environment data in the cloud map. This process allows ASA to compute a reliable 6DoF pose, enabling the display of spatially anchored content at the correct physical location. Multiple devices can co-localise to the same anchor [30], visualising shared digital information from their own perspectives by leveraging the anchor's coordinate frame.

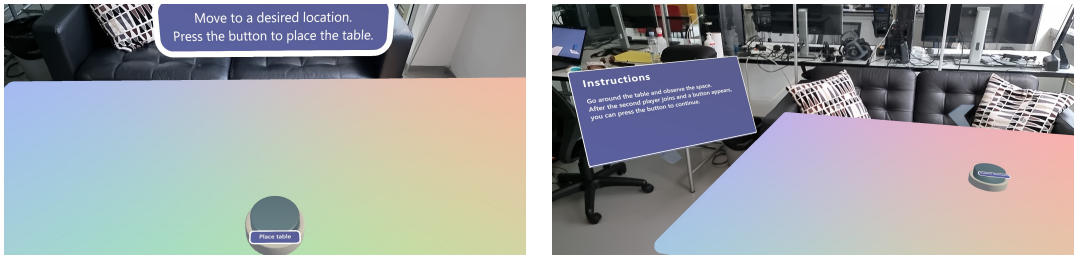
In the context of this application, session-based spatial anchors were employed, indicating that the anchors would cease to exist after the conclusion of a particular session. The utilisation of anchor persistence, wherein anchors created in one session can be located and accessed in subsequent sessions on the same or different devices [65], was intentionally disregarded. This decision was driven by the nature of the application, aiming to facilitate singular usage scenarios with new user pairs for each session, who could potentially occupy the same physical space as previous pairs. Consequently, the exclusion of anchor persistence ensures that each new pair could establish their own distinct anchor tailored to their specific requirements at a particular moment.

To incorporate the ASA service into a Unity application, several steps must be taken. Firstly, the relevant SDKs, depending on the targeted devices, must be loaded into the Unity project. Secondly, adjustments need to be made to the project settings to enable seamless integration with the ASA service. Additionally, an Azure account must be established through the Azure portal[11], providing the necessary foundation for utilising the ASA service. Within the Azure portal, a distinct "Spatial Anchor Account"

[11] `https://portal.azure.com/`

resource must be created, generating essential credentials such as the Account Domain and Access Key associated with the resource. This information is crucial for establishing a connection between the application and the Azure cloud service, supplied to the application through scripting in Unity.

The application utilises a single anchor, to be placed by Player 1 after entering the application (see Figure 3.2a). The anchor is visualised as the center of the table visible to both players, on which all the scenarios within the application are to take place. To ensure sufficient coverage of the surrounding real-life environment, Player 1 is encouraged to move around the table after its placement (see Figure 3.2b), following the general guidelines on ensuring a sufficient scan of the anchored area, provided by [62]. Once more than 80% of the area has been traversed (as indicated by the ASA SDK), the locally established anchor is officially placed and transmitted to the cloud. Consequently, the other player can retrieve this cloud-stored anchor by looking around the same area Player 1 scanned originally, aligning their own table's placement with the location of Player 1's table within their respective local space.



(a) Locally placing the spatial anchor **(b)** Capturing the surroundings of a spatial anchor

Figure 3.2: ASA set-up within the application

More technically, the application establishes communication with the ASA service by utilising the `SpatialAnchorManager` interface provided by the ASA SDK [64]. To create and locate anchors, an ASA session is initiated through the `StartSessionAsync()` method. If required, a session needs to be created first by invoking `CreateSessionAsync()`. The anchor in question is stored as a `CloudSpatialAnchor` object, which is linked to the platform-specific local anchor of `ARAnchor` type. The anchor can be assigned an expiration date or explicitly deleted, as implemented within this application. Furthermore, the application is required to collect environmental data, awaiting a signal from the dedicated `SpatialAnchorManager` indicating that a sufficient amount of scanning has been conducted. This signal is determined by checking the `IsReadyForCreate` property. Only when `IsReadyForCreate` becomes true can the potential cloud anchor (still local at this point) be saved to the cloud. Upon successful storage, an anchor ID

is generated, allowing it to be stored in the Photon Room properties. This enables the anchor to be used and discovered by every user within the room in the session, not just the creator of the anchor, in this case Player 1.

3.4. Scenario Descriptions

The application consists of two different cybersecurity awareness scenarios. In Scenario 1, users engage in an escape room-style challenge where they must decipher virtual clues to gain unauthorised access to a computer. Scenario 2 involves the generation of personal passwords, which are then evaluated against predefined password security rules. Users must correctly match their passwords to the corresponding rules based on whether each of the passwords meets the specified criteria. Preceding the two main scenarios is an introductory section, here named Scenario 0, included to familiarise users with the gestures and interactions specific to the device they are using and the application itself. This section is particularly useful for individuals who have not previously experienced AR or are unfamiliar with the unique interactions tailored for this application. Each scenario has an end goal, and, in case of Scenarios 0 and 1, once the objective is accomplished, Player 1 (the Master) is presented with a button to progress to the next scenario.

As mentioned in Section 3.3.2, all scenarios take place on a shared table object, the contents of which will be described separately for each scenario. In each scenario, users are presented with an instruction panel that contains the relevant information specific to that scenario. Each player exclusively sees their individual instruction panel located near their assigned position.

Additionally, a designated spot is assigned to each player, accompanied by a floating chevron guide. If a player moves too far away from the designated spot, the chevron guide is displayed to assist them in returning to the vicinity of their spot, as exemplified in Figure 3.3. Once the player is back within range, the chevron guide disappears.

While Player 1 need not move extensively from the initial location, Player 2 needs to change positions multiple times during certain stages of the scenarios, from being next to Player 1 to being on the opposite side of the table. Nevertheless, the users are still encouraged to move in both real and virtual space during the duration of the scenarios by the instruction panels and the study facilitator, particularly in Scenario 1. The positioning guides serve a dual purpose: they navigate the users to reposition due to changes in the virtual environment, as well as provide a reference for users who may lose track of the intended placement while exploring the virtual environment.

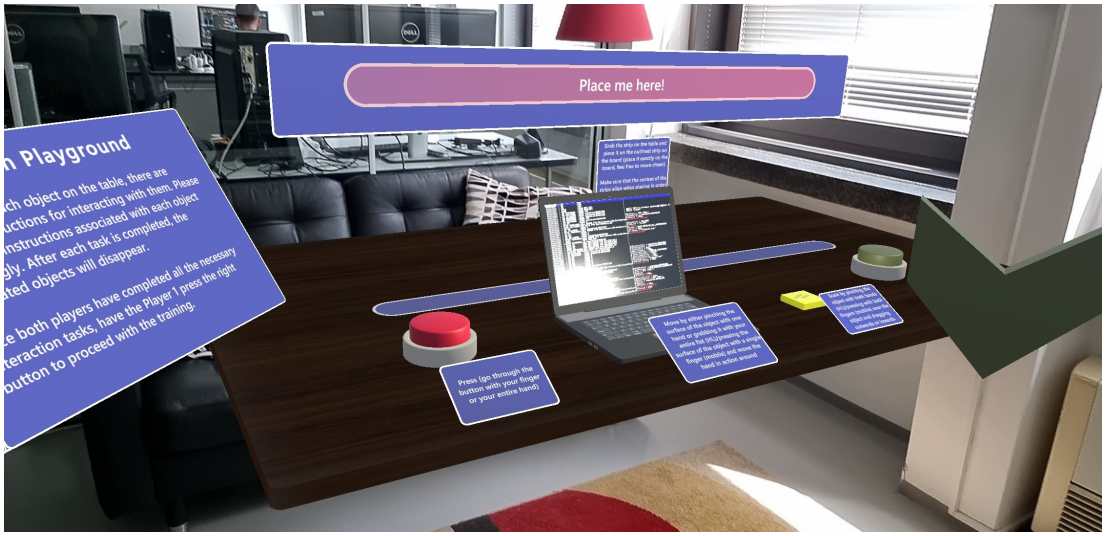


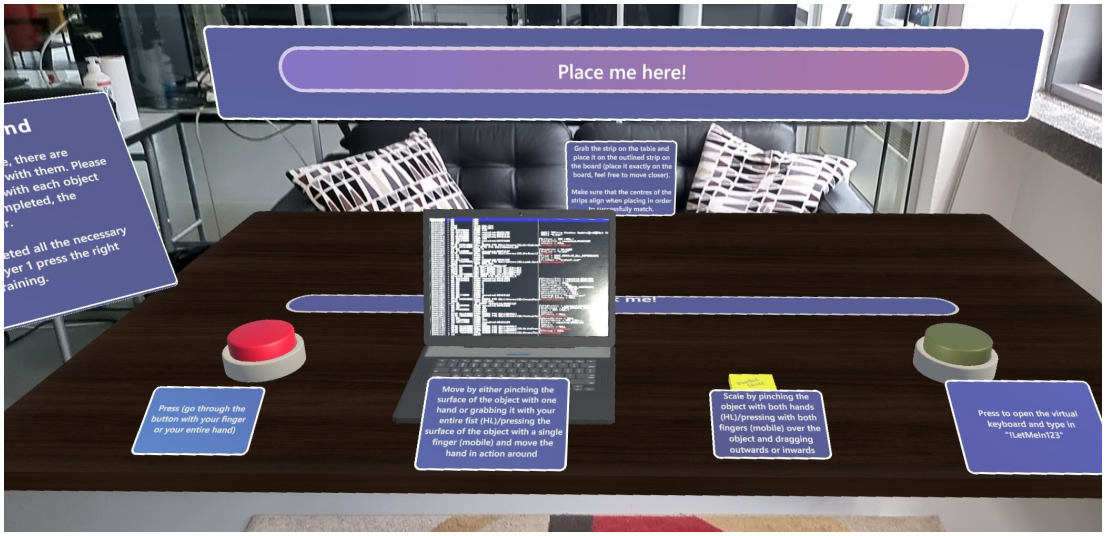
Figure 3.3: Chevron guide in Scenario 0 from Player 1's perspective

User-specific objects, such as buttons and the placement chevron, are assigned individual colours for each user. However, since these objects are not visible to the other user, they are unaware of the specific colours assigned to the other user's objects. On the other hand, shared buttons are assigned a distinct colour.

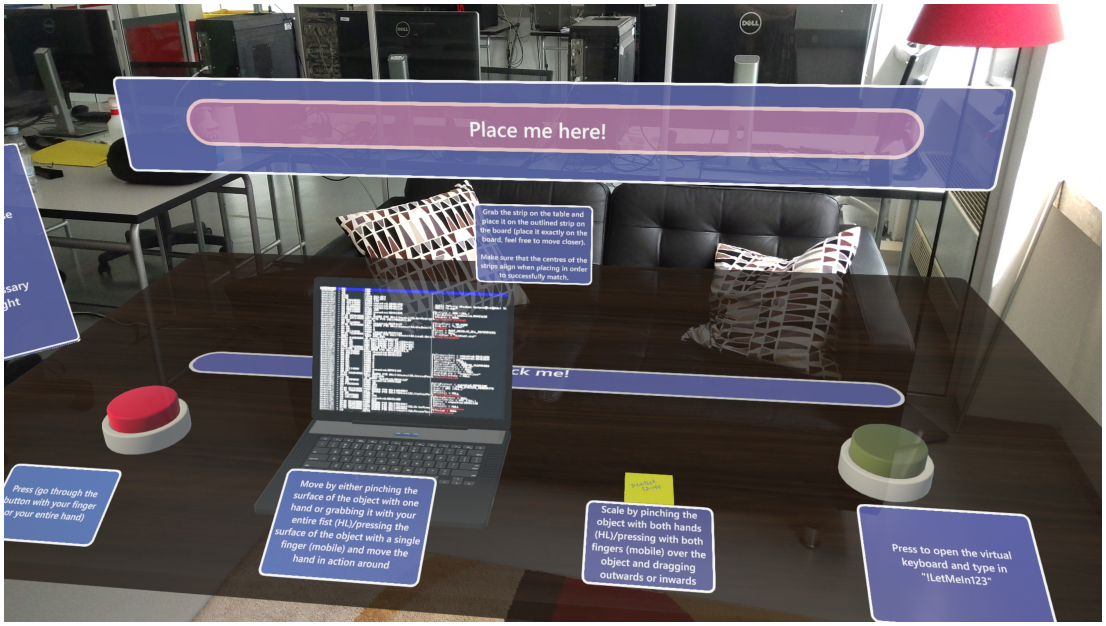
3.4.1. Scenario 0: Interaction Tutorial

In the introductory interaction tutorial, users are instructed to position themselves on the opposite sides of the table. A set of specific items representing various interactions is displayed in front of each user and each interaction is accompanied by a corresponding instruction to guide the user through its execution. To prevent visual clutter and minimise distractions, each user can only see the items relevant to their assigned interactions, meaning they cannot see the items with which the other person is supposed to interact. This design choice eliminates any irrelevant items that could potentially distract or overwhelm the user, allowing them to maintain their focus on the task at hand. The visual representation of the scenario within the application, from the point of view of Player 1, can be seen in Figure 3.4. Once an interaction is successfully completed, the associated items disappear, serving as a clear signal of achievement and enabling the user to seamlessly move on to the next interaction. Once both users have successfully completed all the designated interactions, Player 1 is presented with a button on the table, prompting them to proceed to the next scenario.

On the HoloLens 2, users are prompted to utilise both their hands in the physical 3D space to interact with virtual objects. This involves actions such as pressing, pinching,



(a) On an Android mobile phone



(b) On HoloLens 2

Figure 3.4: Representation of Scenario 0 from Player 1's perspective

and dragging. On the contrary, users of the mobile phone interact with virtual objects directly through the screen, using actions such as tapping, pinching, and sliding. The interactions covered in the tutorial are listed in Table 3.1.

3.4.2. Scenario 1: Password Break-In

This scenario is designed to provide users with a hands-on experience of exploring and investigating a simulated work environment while collaboratively solving a challenge. By engaging in the process of breaking into a work computer and deciphering

Table 3.1: Interactions featured in Scenario 0

Interaction	Description
Button pressing	Users press a designated button.
Object picking and translation (movement)	Users practice moving a virtual laptop by pinching/grabbing it with their fist (HoloLens 2) or tapping the screen (mobile phone) and not releasing the executed gesture while moving the hand in space.
Object scaling	Users scale a stack of sticky notes by pinching with two fingers and widening (enlarging) or tightening (shrinking) the gap between them.
Textual input via system keyboard	Users enter a predefined string on a keyboard interface depending on their device: HoloLens 2 users use a virtual 3D keyboard positioned in the spatial environment with pressable keys, while mobile phone users have a standard system 2D keyboard appearing from the bottom of the screen.
Picking and placing flat panel-like objects in 3D space	Users pick up a flat panel from the table and position it vertically on a board above the table, aligning it with the panel outline in all three spatial axes. HoloLens 2 users are additionally guided to position the ray emitted from any hand precisely on the panel and perform a pinching gesture to pick it up due to the relatively small height of the panel's collider.

the password, users can gain a deeper understanding of cybersecurity vulnerabilities, the importance of password security, and the significance of being vigilant in an office setting. This segment is designed in the style of an escape room, where participants must engage in a collaborative effort to gain unauthorised access to a colleague's work computer. The challenge involves discovering hidden clues within the work environment and deciphering the password based on these clues. Figure 3.5 showcases the scenario visualisation within the application, from Player 1's perspective.

In this scenario, collaboration between the two users is essential as they work together to explore the virtual work environment, analyse clues, and jointly decipher the password. By sharing their observations with their colleague, discussing potential connections between the clues, users can improve their chances of successfully breaking into the computer. The collaborative nature of the activity fosters teamwork, communication, and the utilisation of each user's unique perspectives and insights.

To maintain a clear and coherent user experience, both users are presented with the exact same virtual objects simultaneously. However, they are unable to observe

Figure 3.5: Representation of Scenario 1

the movement of objects performed by the other player. This intentional design choice aims to prevent potential confusion and disturbances that may arise from unexpected object movements within each user's view. Additionally, this approach addresses the possibility of spatial misalignment between the anchor location for each user, which determines the positioning of the rest of the objects in virtual space. If one user were to showcase a specific item to the other user, the latter may not perceive the item in the exact location as intended, leading to a disruption of the shared real and virtual space illusion. To compensate for this limitation, the scenario emphasises discussion between users to compensate for any lack of precise spatial alignment in the virtual environment. Notably, this scenario is more susceptible to offset issues compared to Scenario 2, where object movement synchronisation is enabled. This limitation is further elaborated on in Subsection 3.6.1.

The scenario employs gamification elements to enhance user engagement and experience. Interactive elements require users to physically manipulate objects and explore the virtual environment, fostering immersion and participation. A time pressure component, implemented through a countdown timer in the form of a clock on the table, adds a sense of urgency, prompting quick thinking and decision-making. The challenge timer had a duration of 8 minutes. Additionally, a hint system was implemented to support users during the challenge. To assist users in progressing through the challenge, hints were strategically incorporated. As the timer approached certain time intervals, specific hints were triggered to provide guidance. These hints were presented

in two formats: animated 3D warning signs appearing above the clues being hinted at, and objects themselves changing colour to yellow (e.g., sticky notes, calendar entries) in addition to the warning sign display. This combination of visual cues aimed to draw users' attention to relevant objects and provide additional assistance when needed. The clues hinted in such a way are the first six ones listed in the Table 3.2. However, the last two clues in the Table are objects which are not explicitly hinted at but rather rely on common computer behaviours and human carelessness regarding password security. Consecutive incorrect password attempts trigger a password hint, simulating typical system responses, while the placement of a sticky note with the complete password under the mousepad reflects the tendency of some individuals to leave passwords easily accessible in their immediate workspace. These elements add an additional layer of challenge and realism to the scenario. Figure 3.6 provides a visual representation of all the game objects mentioned as clues in the scenario.

Table 3.2: Password clues in Scenario 1

Clue	**Description**	**Hint Appearance**[1]
Dog figurine	A figurine of a Shiba Inu dog	50% of time left
Dog photo[2]	A photo of a dog of the same breed	40% of time left
Anniversary sticky note	A sticky note reminder to book a restaurant for the anniversary	30% of time left
Calendar	A calendar displaying all events	25% of time left
Vet appointment calendar entry	A calendar entry for a veterinarian appointment with the name "Indy"	20% of time left
Anniversary calendar entry	A calendar entry for the anniversary on June 6th	15% of time left
Login password hint	A password reminder in the login form on the computer	After three incorrect password attempts
Sticky note with password	A sticky note under the mousepad with the password "Indy0606"	-

[1] Specifies the condition or trigger for each hint's appearance.
[2] `https://www.reddit.com/r/shiba/comments/hlhb4t/ripley_had_a_little_vacation_in_puerto_backyardo/`

Figure 3.6: Clues in Scenario 1

In addition to the previously mentioned gamification elements, storytelling was employed in the instructions to enhance user immersion and engagement. By setting the scene and framing the challenge as uncovering a password left unattended by their co-worker named Lou, users are drawn into a narrative context. The use of storytelling adds a layer of intrigue and purpose to the task, making it more compelling for users to explore Lou's work desk for potential clues. Furthermore, the mention of time ticking and occasional hints appearing contributes to the sense of urgency and adventure, creating a gamified experience that motivates users to actively participate and test their luck in solving the challenge.

To attempt entering the password, users can utilise a button positioned on the desk, which opens a virtual keyboard specific to their respective device. If the correct password is entered, the work environment items vanish from the table, and a congratulatory message appears on a board above the table, acknowledging the successful break-in. Upon entering an incorrect password, users can continue exploring the same area and gather additional information about the password. They can make multiple attempts to enter the password, until eventually entering the correct one. However, if users fail to enter the correct password before the time expires, they are presented with a text board indicating their unsuccessful attempt and providing a list of the hints they may have overlooked to crack the password. In both cases of the end of Scenario 0, Player 1 is also presented with a button to proceed to the next scenario, which can be pressed when both users mutually agree to continue.

3.4.3. Scenario 2: Password Creation and Analysis

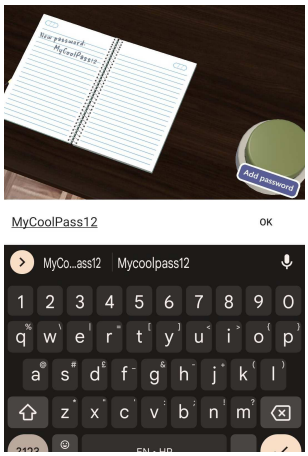
Scenario 2 of the application comprises two distinct parts. In the first part, users are tasked with generating their own passwords. The second part involves the analysis of the passwords entered by both users. The passwords are individually assessed against 12 password security rules. The objective is to associate each rule with the corresponding outcome for the respective passwords, determining whether each password conforms to the rule or not.

Collaboration plays a vital role in the second part of Scenario 2 as it enables users to combine their knowledge and perspectives to effectively evaluate the compliance of passwords with the given rules. By working together, users can share insights, discuss different interpretations, and ensure a comprehensive evaluation of passwords, ultimately fostering a deeper understanding of password creation and security. Also in the second part of Scenario 2, virtual object synchronisation is enabled to provide real-time visibility of the actions performed by the other player. This allows users to track the movement of the rules being selected, placed on the board, and determine which rules have yet to be matched and which have already been successfully matched.

In the creation part of the scenario, as visualised in Figure 3.7, the users are prompted to stand on the opposite sides of the table. Each user is assigned a dedicated button to generate their password, granting access to a virtual system keyboard for input. The entered password is simultaneously displayed in real-time on the notebook in front of each respective player. Figures 3.8a and 3.8b demonstrate an example of this behaviour when utilising an Android mobile phone and HoloLens 2, respectively, as the AR device. Importantly, users cannot view the password entered by the other user. Users have the freedom to revise and re-enter their passwords multiple times. Once both users have entered their passwords at least once, a new button appears only for Player 1 and they can proceed to the second part by pressing the button, provided that both users are content with their chosen passwords.

During the analysis part of the scenario, the users are required to stand together to effectively complete the task. A set of 12 password security rules is presented on the table as panels, as seen in Figure 3.9. Positioned above the table is a board that displays both entered passwords, with a separate board below it featuring slots for the rule panels. Each slot is colour-coded, with each half representing a password (left side for the Player 1's password, on the left, right side for the Player 2's password, on the right). The colour-coding indicates whether the corresponding password complies

Figure 3.7: Representation of password creation in Scenario 2



(a) On an Android mobile phone

(b) On HoloLens 2

Figure 3.8: Entering a password in Scenario 2

with the rule: green for compliance and red for non-compliance. In addition, indicators in the form of a tick or a cross mark are displayed alongside each rule slot, providing additional visual feedback for rule adherence. The relationships between the rules and passwords are represented in four colourways (see Figure 3.10a): green-green for compliance of both passwords, green-red for compliance of Player 1's password but not Player 2's, red-green for compliance of Player 2's password but not Player 1's, and red-red for non-compliance of both passwords. If multiple rules have the same relationship with the passwords, any of those rules can be placed in any available slot corresponding to that relationship type. Users can interact by dragging the rules from the table and placing them on a board, aligning them with the slots that signify their re-

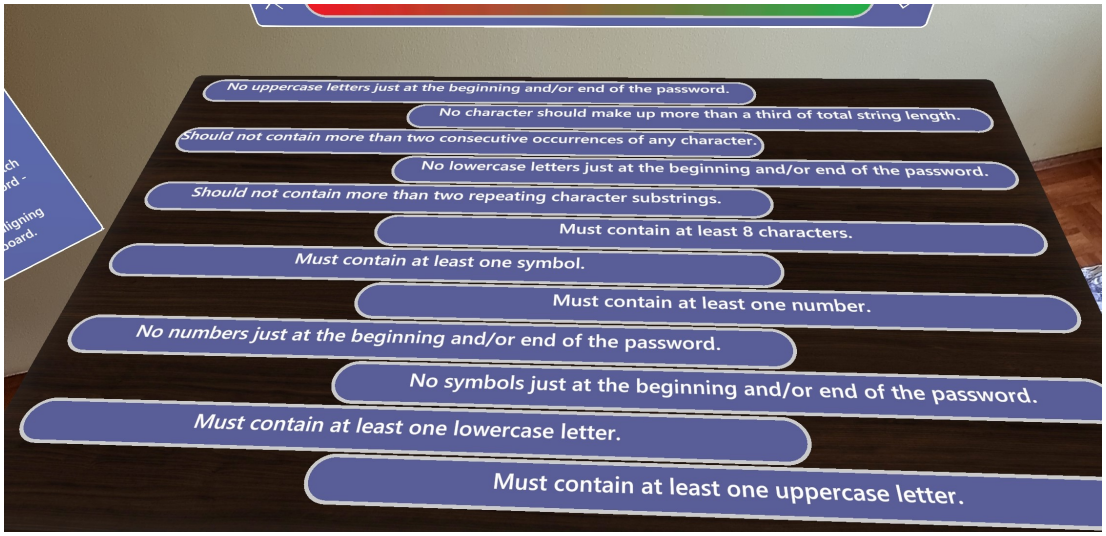


Figure 3.9: Password security rules in Scenario 2

lationships with the passwords, as depicted in Figure 3.10b. The rule attachment is an interaction mechanic introduced in Subsection 3.4.1 and further technically detailed in Subsection 3.5.3. Upon successful completion of matching all rules to their respective slots, the password analysis board is replaced by a congratulatory board, acknowledging the users' accomplishment in completing the task and the entire cybersecurity training in general.

The set of 12 password rules used to validate user-entered passwords, given in Table 3.3, are derived from the password heuristics utilised by Jayakrishnan et al. [45], where the majority of the rules have been adapted to suit the application's context. Due to the spatial constraints and potential overcrowding of the scene, the number of rules was restricted to 12 in the second part of the scenario. This decision was made to ensure that all rules could be effectively displayed on the table without overwhelming the visual clarity and organisation of the scene. Moreover, the choice not to include dictionary-based or predictable word pattern in the rule base is due to the impracticality of incorporating numerous available sources (e.g., dictionaries, databases of leaked passwords, keyboard pattern combinations, databases of common passwords with homograph substitutions) for run time optimisation and the challenge of selecting the most appropriate ones among a vast array of options. The implemented password rules focus primarily on identifying common patterns in password creation, such as inadequate length, absence of specific character categories, predictable arrangement of these categories, and the presence of repeated characters or substrings within the password.

(a) Initial state of the rule board **(b)** Rule board with most of the rules matched

Figure 3.10: Representation of password analysis in Scenario 2

3.5. Notable Mechanics

This chapter focuses on highlighting specific mechanics that were intentionally implemented to ensure the smooth functioning of the application. While the application incorporates various features to provide a comprehensive UX, these notable technical aspects were specifically designed to address key challenges and objectives within the application. The mechanics discussed include the preservation of original game object transformation states, the analysis of passwords-rule relationships, and the manipulation of rule panel objects through picking and placing. Each mechanic serves a specific purpose, such as maintaining spatial object consistency, validating password adherence to security rules, and facilitating the matching process between rules and designated slots. The implementation details and benefits of each mechanic are elaborated upon to provide a comprehensive understanding of their significance in the application.

3.5.1. Preserving Game Object Transformation States

Ensuring the preservation of the original transformation states of virtual objects after completing a transform interaction, including translation, rotation and scaling, is an important interaction mechanic, particularly in a multi-user environment. Once the gesture for transform manipulation is released, the virtual object smoothly transitions back to its original values of translation, rotation, and scale through interpolation. This mechanic becomes especially significant when considering the involvement of diverse devices like HoloLens 2 and Android phones with 2D screens. By addressing these conditions, the preservation of original transformation states enhances the overall user experience.

Firstly, the absence of true depth perception while using a 2D screen on a mobile phone poses challenges for users in accurately perceiving object placement and movement in 3D virtual space. By ensuring that virtual objects return to their original transformation state in the environment, the mechanic minimises the risk of inadvertently misplacing objects. This allows users to precisely locate objects after having finished interacting with them.

Secondly, in a collaborative environment where multiple users are simultaneously engaging with the application, maintaining the original transformation of objects promotes consistency and coordination. Users can easily comprehend and discuss the virtual objects based on their preserved original transformation state, as it remains consistent with the rest of the environment. This consistency reduces confusion and enhances the overall collaborative experience.

This preservation mechanic is applied across all three scenarios, with its impact being particularly noticeable in Scenario 1. This is attributed to the extensive number of interactions each user can have with numerous objects provided in the scenario. Additionally, in Scenario 2, the mechanic proves helpful when placing rules on the board. As previously discussed, users may encounter challenges initially when determining the correct depth for placing objects from the table onto the board. Furthermore, there is a possibility of unintentionally releasing the objects if the hand holding the rule disappears from the FoV of the AR device. This way, users can locate the object in the same position where they initially encountered it.

The implementation of this mechanic can be found in the script `MaintainOriginalTransform.cs`, which can be added as a component to any game object in the Unity project. By attaching this script, the object and its child

objects will retain their original transform even after being manipulated with. This functionality is achieved by utilising the `OnManipulationEnded` event triggered by the MRTK `ObjectManipulator` component, attached to the same game object, allowing for AR-based hand interactions with the object. Upon receiving the signal that the manipulation has ended, the script checks the current translation, rotation, and scale values against the original values and, using the MRTK `Interpolator` class, it smoothly interpolates towards the original values in each frame until the desired transform is reached.

3.5.2. Analysing Passwords-Rule Relationships

When a user enters a password in the password creation part of Scenario 2, as described in Subsection 3.4.3, the local password validation process is initiated. The objective of this process is to verify whether the entered password adheres to a predefined set of password security rules. This validation is performed by a script called `PasswordValidator.cs`, which listens for the `PlayerPasswordEntered` event triggered by the system keyboard input component when the user finishes entering a password.

The entered password is then compared against regular expressions representing the specific password rules listed in Table 3.3. Each rule has its own regular expression, and the password is checked against each of them to determine compliance. The results of each of these validations are stored locally for each entered password, while ensuring that duplicate entries do not trigger redundant validation.

To optimise network transfer, the passwords are validated locally, meaning that only the password itself and validation results need to be transmitted. This minimises the amount of data sent across the network, as only a string representing the password and a small number of boolean values indicating the validation outcomes are transferred. By storing the last entered and validated password for each user, the system keeps track of the most recent password input, enabling the distribution of only that password and its corresponding validation results across the network when required to proceed to the analysis phase of Scenario 2.

In the analysis phase, the rule panels on the table are shuffled, while ensuring that both users see the same rule in the same position. Simultaneously, the rule board is adjusted to match the entered passwords and their validation results. This dynamic adaptation ensures that the rule board accurately reflects the password analysis process

Table 3.3: Password rules, with respective regular expressions, used in Scenario 2

Password Security Rule	Regular Expression
Must contain at least 8 characters.	`^.{8,}$`
Must contain at least one lowercase letter.	`^(?=.*[a-z]).+$`
Must contain at least one uppercase letter.	`^(?=.*[A-Z]).+$`
Must contain at least one number.	`^(?=.*\d).+$`
Must contain at least one symbol.	`^(?=.*\W).+$`
Should not contain more than two consecutive occurrences of any character.	`^(?!.*(.)(\1\1)).*$`
Should not contain more than two repeating character substrings.	`^(?!.*(.{2,}).*\1.*\1)[\s\S]*$`
No character should make up more than a third of total string length.	`^(?!.*(.)(\1{2,})).*` `(?!.*(.)(\2{2,})).*$`
No lowercase letters just at the beginning and/or end of the password.	`^(?!^[a-z]$)(?!^[a-z][^a-z]*$)` `(?!^[a-z][^a-z]*[a-z]$)` `(?![^a-z]*[a-z]$).*$`
No uppercase letters just at the beginning and/or end of the password.	`^(?!^[A-Z]$)(?!^[A-Z][^A-Z]*$)` `(?!^[A-Z][^A-Z]*[A-Z]$)` `(?![^A-Z]*[A-Z]$).*$`
No numbers just at the beginning and/or end of the password.	`^(?!^[\d]$)(?!^[\d][^\d]*$)` `(?!^[\d][^\d]*[\d]$)` `(?![^\d]*[\d]$).*$`
No symbols just at the beginning and/or end of the password.	`^(?!^[\W]$)(?!^[\W][^\W]*$)` `(?!^[\W][^\W]*[\W]$)` `(?![^\W]*[\W]$).*$`

and serves as a visual framework for users to evaluate the compliance of the passwords with the established rules.

The dynamic adaptation is manifested through several visual cues on the rule board. This includes changing the colouring of the rule slots, adding mark indicators for each password next to each slot, and assigning each slot its corresponding passwords-rule relationship. These adjustments are crucial for the user's matching process, as they provide clear visual guidance for correctly placing the rule panels onto their designated slots.

3.5.3. Picking and Placing Rule Panels

The script `CheckRulePlacement.cs` is utilised as a component attached to each rule panel within the password analysis part of Scenario 2. Its primary purpose is to determine whether a given panel is within the proximity of a suitable slot on the rule board, corresponding to the relationship it represents between the rule in question and the two passwords under analysis.

During each frame update, the script checks whether the rule panel is currently being moved. When movement of a rule panel is detected, the panel is rotated to face the user and the script utilises an RPC mechanism to synchronise the transformation of the panel across all networked clients. This ensures that both the user who is currently moving the panel and the user who is not observing the same positional changes in real time. Subsequently, the script calculates the closest available slot placement based on the centre positions of the rule panel and each available slot on the rule board. If the closest slot is found to have the same passwords-rule relationship as the rule panel itself, the panel snaps into place, occupying that particular slot. This action is also propagated to the other user through an RPC. From that point on, both the rule and the slot become unavailable for further matching.

3.6. Limitations

In the pursuit of creating a robust and efficient application, it is important to acknowledge the observed issues and limitations that arise during its development and testing. Discussing and understanding these limitations is essential for guiding further development efforts, allowing for the refinement and improvement of the application in order to provide a more effective and efficient UX. Within the context of this application, there are two notable limitations that have the potential to negatively impact the UX. The first limitation involves difficulties that arise after obstructing anchored virtual elements, which can lead to a disjointed perception of the shared environment between users. The second limitation relates to the desynchronisation of rule matching in a shared virtual environment, possibly caused by the large number of RPCs being executed concurrently. Addressing the these issues remains an area for future work. Further investigation and efforts are needed to understand the specific factors causing these specific problems and find potential solutions for their mitigation or resolution.

3.6.1. Anchoring Issues

During the application testing phase, when one user of the pair used the HoloLens 2 and the other utilised an Android mobile phone, certain users experienced difficulties with the positioning of anchored items while using the Android device. These problems arose when the phone's camera was unintentionally covered, such as by the user's fingers or when the other walked in front of the camera, causing the mobile phone to lose sight of the real-world environment. Consequently, the anchoring of virtual items would freeze when obstructed, and even after removing the obstruction, the virtual objects would not reposition themselves correctly relative to the new camera perspective and the original anchor position. Instead, the anchor, and consequently the entire virtual environment, for that specific device would be placed in a new location in the real world based on the last-known anchor position which stayed frozen on the 2D screen of the phone during the camera obstruction period.

This resulted in a disjointed perception of the shared world between the two users. Even a slight offset between their virtual worlds could disrupt their understanding of a unified environment where both users should see the same objects in the same locations relative to the real environment. This became particularly problematic in Scenario 1, where multiple items were placed close together on a table. References to the location of specific items relative to the real environment would not accurately correspond between the users since their instances of the virtual world did not overlap but instead had an offset from each other. This offset, even if relatively small, caused irritation and discomfort for the users, as it undermined the sense of a shared environment that was intended to be achieved. In addition, users sporadically encountered situations where the entire virtual environment would unexpectedly drift away from them and fail to return, requiring them to restart the application. It is believed that this occurrence might have been triggered by the same obstacles, causing the ASA service to lose its tracking of the placed anchor and behaving in such an unpredictable manner. To address these issues, users were advised to avoid covering the camera and to refrain from obstructing each other's view.

Interestingly, HoloLens 2 users did not report experiencing such problems, although users with Android mobile phones did occasionally obstruct the HMD's capture of the real environment by walking in front of its cameras. One possible explanation for this discrepancy is that the HoloLens 2 offers more advanced tracking capabilities, and its dedicated hardware contributes to a more stable and reliable AR experience. Another factor could be the proximity of the obstructor to the mobile phone's camera,

which is much closer compared to the obstructor's proximity to the cameras of the HoloLens 2. This is because the HoloLens 2 is worn on the user's forehead, while the mobile phone is typically held at neck level, increasing the likelihood of obstructions interfering with the phone's cameras more than the HMD's cameras.

3.6.2. Broken Synchronisation of Matched Rules

In Scenario 2, when using the HoloLens 2 and an Android mobile phone together, the instances of the shared virtual environment for the two users may become desynchronised. To exemplify, the users are pursuing the actions instructed in the analysis part of Scenario 2 and while one user is matching rule panels on the table to slots on the rule board, the other user can observe the movement and matching of the panels, creating a sense of a shared environment. However, due to desynchronisation issues, when one user completes the matching aspect and their virtual environment switches to a congratulatory board, the other user may still have a few rules left to match, and still see the table with the leftover rules and the rule board with a few spots left blank.

This desynchronisation is suspected to be caused by interference due to a large number of RPCs that are executed during the process. RPCs containing information about the movement and transformation of the rule panels are sent every frame when the movement is active. Additionally, an RPC is issued when a rule panel has been matched and should no longer be available for matching. However, this single RPC may not always arrive on time for the receiving user. As a result, the user who successfully performs the matching executes all the appropriate actions, while the other user may not receive the crucial RPC indicating that a panel has been matched. Instead, the observing user may receive an RPC indicating that the panel has been released by the other user. While this information is technically correct, the user lacks the RPC regarding the matching of the rule panel to the board. As a consequence, the panel returns to its original position on the table, remaining unmatched for the observing user.

The PUN2 communication protocol chosen within the Unity project is the User Datagram Protocol (UDP). However, the large volume of different messages being sent simultaneously over UDP may contribute to some messages being ignored or lost, including the RPC message about matching the rule to the board. This issue could possibly be mitigated by switching from UDP to Transmission Control Protocol (TCP). However, Photon's official documentation recommends adhering to the default UDP [69] option, since Photon utilises something that is called reliable UDP. This protocol

establishes a connection between the server and the clients, assigning sequence numbers to messages that require acknowledgement at the receiving end [67]. Messages are sent repeatedly until acknowledged or the connection times out. Therefore, Photon's reliable UDP protocol aims to ensure message reliability, but some other factor might be contributing to the described problem. Factors such as network latency, congestion, implementation issues, inconsistent network conditions, and application-specific complexities can all impact the reliable delivery of messages. Thorough analysis and troubleshooting are necessary to identify and address the underlying cause of desynchronisation.

If ruling out the protocol issue, there are several other potential causes for the desynchronisation observed in the scenario. Another possible cause could be related to network latency and inconsistent network conditions. Variations in network speed and stability can result in delays or interruptions in message transmission, leading to discrepancies between users' virtual environments. Additionally, congestion in the network could affect the timely delivery of RPCs, causing desynchronisation between the actions performed by one user and the observations of the other. Implementation issues within the application, such as inefficient handling of RPCs or synchronisation logic, could also contribute to the problem. Furthermore, application-specific complexities, such as unoptimised management of multiple simultaneous interactions, could introduce observed synchronisation challenges.

It is important to note that during testing both the HoloLens 2 and the Android mobile phone were connected to the same shared Wi-Fi hotspot. This hotspot was created using another Android mobile phone with an active mobile Internet connection. This setup introduces additional factors that can contribute to the desynchronisation issue. The stability and performance of the mobile internet connection, including factors such as signal strength and bandwidth limitations, may impact the reliability and timeliness of message delivery between devices. Therefore, the characteristics of the Wi-Fi hotspot and the mobile internet connection should also be considered when investigating and troubleshooting the desynchronisation problem.

4. User Study

In the scope of this thesis, a user study was conducted to investigate the practicality of developing an immersive and collaborative cybersecurity training solution that could be seamlessly deployed on a range of AR-capable devices, encompassing both the lower end, such as a mobile phone, and the higher end, exemplified by the HoloLens 2. The proposed concept is exemplified through the application *SecuAR Together*, described extensively prior in the thesis. By targeting devices across different availability and affordability ranges, the study aims to evaluate the viability and effectiveness of a unified application on various AR platforms. To address these goals, the study addresses the following research questions (RQs):

RQ1: *How do users perceive the overall application, considering factors such as enjoyment and the provided educational value?*,

RQ2: *Are there any discernible differences in the quality of experience (QoE) and UX between HMD and mobile phone users?*,

RQ3: *How do users assess the virtual environment and interaction experience within the application?*,

RQ4: *What is the impact of collaboration on QoE and UX?*,

RQ5: *What are users' attitudes towards incorporating XR technologies into everyday life and various types of training?*, and

RQ6: *Does the usage of SecuAR Together lead to a change in users' knowledge of password security compared to their prior knowledge, and if so, how?*

4.1. Methodology

4.1.1. Experiment Design

Each study trial included a pair of participants, one of whom used an MR HMD, while the other used an Android mobile phone during the trial. The study adopted a

mixed study approach, incorporating aspects from both a between- and within-subjects design [89]. The within-subjects aspect of the study focused on the content and tasks within the application itself. Regardless of the device used, all participants went through the same application and experienced the identical set of tasks. This design choice allowed comparisons of elements within the application that were independent of the specific device. The between-subjects aspect involved assigning each participant in the examined pair per session a different AR device, effectively dividing the participants into two groups: one group using the HoloLens 2 and the other group using a mobile phone. Each group exclusively used their assigned device throughout the study. This between-subjects design allowed for a comparison of the participants' experiences between the two device types. By incorporating both the between-subjects and within-subjects aspects, the study aimed to investigate the effects of device type on the participants' experiences while executing the same tasks within the application.

4.1.2. Hardware and Software Set-Up

The study was conducted in a designated laboratory room, where each participant was equipped with an individual desktop computer and one of two AR-capable devices: HoloLens 2 and Huawei Mate 20 X. An illustration of the set-up using both devices can be see in Figure 4.1. In order for the tested application, which was extensively detailed in the previous chapter (Chapter 3), to function as intended, an Internet connection was required. Both devices were connected to the Internet via a shared Wi-Fi hotspot, facilitated by another Android mobile phone with an active mobile Internet connection. Participants accessed the questionnaires through an online form hosted on the Google Forms[1] platform.

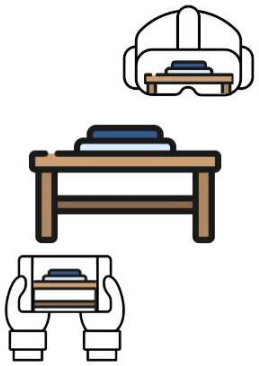


Figure 4.1: Illustration of the dual AR device set-up

[1] `https://www.google.com/forms/`

HoloLens 2 is an MR HMD, released by *Microsoft* in 2019. It operates independently without the need for external computing power or constant connection to a power source. With its optical see-through display, HoloLens 2 allows users to perceive their surroundings in real time through a semi-transparent screen [59]. This unique feature enables users to seamlessly integrate virtual objects into their environment. Additionally, the HoloLens 2 incorporates advanced capabilities such as spatial mapping, which allows the device to understand and interact with the physical space, and intuitive hand gesture recognition, eliminating the need for controllers when interacting with virtual objects.

Huawei Mate 20 X is a smartphone released by *Huawei* in 2018. It runs on the Android operating system and features a powerful processor and a high-resolution display. It utilises the ARCore platform, as well as its Depth API[2], enabling advanced AR features such as markerless tracking. Similar to other mobile AR systems, the interaction with virtual objects is primarily achieved through touch gestures on the device's screen. Users can tap, swipe, or pinch to manipulate and control virtual objects within the AR environment.

4.1.3. Procedure

The participants were assigned in pairs to arrive at the study location simultaneously, following hourly time slots, as each trial required an approximate duration of one hour. Upon their arrival, participants were introduced to the details of the research study and provided with a consent form to sign. Following the completion of the consent process, participants were directed to their computers, where they were asked to fill out the initial three sub-questionnaires, as described in Subsection 4.1.5. Participants subsequently received instructions on how to use the assigned AR hardware and the application they were about to use. A visual representation of the study procedure is depicted in Figure 4.2. Once finished with using the application, the participants were prompted to fill out the rest of the sub-questionnaires on their respective computers. The participants were informed that the study facilitator would be readily available to address any questions, concerns, or technical issues that may arise during the entire duration of the study.

[2] `https://developers.google.com/ar/develop/depth`

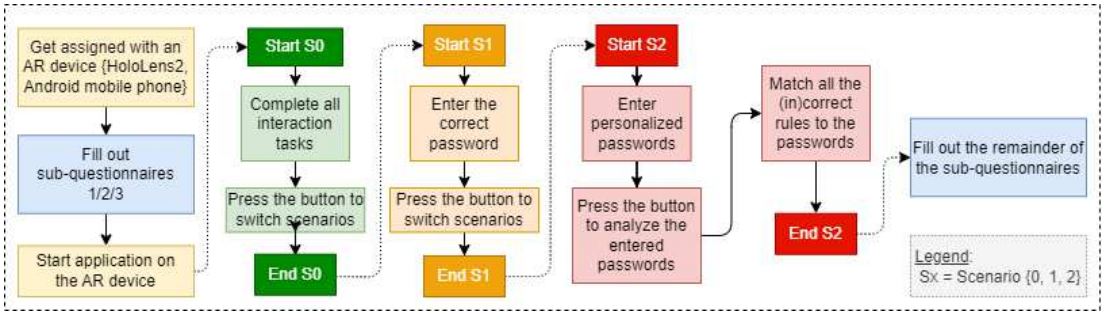


Figure 4.2: Procedure outline of the study

4.1.4. Participants

The research study included the voluntary participation of 18 subjects, with 11 identifying as *female* and 7 as *male*. The age range of the participants spanned from 22 to 24, with a mean age of 22.89 (median 23). Out of the 18 participants, 14 of them have an academic background or job in computer science, computer engineering, information technology, or a related field. Participants self-reported their familiarity with AR, that is, the frequency of using AR throughout their lifetime, as shown in Table 4.1. In case of prior experience (11 participants), they were also prompted to specify the context in which they had encountered the technology (see Table 4.2) and which AR devices they have used (see Table 4.3). One participant had already participated in an immersive XR training experience, albeit not related to cybersecurity, while another participant had participated in a real-life simulation cybersecurity training, but without the immersive aspect.

Table 4.1: Prior AR usage frequency among study participants

AR Usage Frequency	User Count
Never	7
Once	4
A few times	3
A few times a year	2
Monthly	1
Once or more times a week	1

Participants were also prompted to self-report on their cybersecurity behaviour and habits, prior to engaging in the AR training. The results revealed a varied level of self-perceived cybersecurity knowledge, with a third of the participants either disagreeing or remaining neutral about their expertise in this domain. When it comes to password management practices, a significant majority of the participants (55.6%) reported changing their passwords only when prompted, indicating a reactive approach

Table 4.2: Contexts in which study participants have previously encountered AR

AR Context	User Count
Work	1
School	4
Communication	2
Games	5
Other forms of entertainment	4

Table 4.3: AR devices which study participants have previously used

AR Device	User Count
Mobile phone	9
HMD	7
Heads-up display (HUD)	2

rather than a proactive one. Moreover, 38.9% of participants acknowledged changing passwords sometimes without being prompted, suggesting a slight inclination towards proactive behaviour. Half of the participants revealed that they have had at least one of their passwords compromised in the past. In particular, the questionnaire revealed a concerning trend of password reuse among all participants, as every participant admitted to reusing passwords for multiple accounts sometimes in their lifetime. While a substantial proportion of participants expressed relative confidence in creating strong passwords, a notable number remained neutral, suggesting room for improvement in password creation skills. Interestingly, despite the reliance on memorisation as the primary method of recalling passwords (72.2%), a half of the participants report using password management tools. However, one participant revealed they still resort to writing passwords down on paper, which poses a security risk.

4.1.5. Questionnaire

To facilitate this study, a comprehensive self-report questionnaire was developed, consisting of 78 questions. The entire questionnaire is given in the Appendix A. The questionnaire encompassed various question types:

- binary (Yes/No),
- multiple-choice (both single and multiple select, some with an open-ended "write-your-own-answer" option),
- 5-point Likert scales, and
- open-ended questions (optional, for further elaboration on previous responses).

The questionnaire consisted of several sub-questionnaires:

1. a demographic questionnaire,
2. a cybersecurity awareness/previous training experience questionnaire,
3. a pre-training password questionnaire,
4. an AR system comparison questionnaire,
5. a collaboration questionnaire,
6. a questionnaire regarding the application itself
7. a general AR usage questionnaire, and
8. a post-training password questionnaire.

Each participant completed the first three sub-questionnaires prior to using the application, whereas the rest was completed afterwards.

The questionnaire consists of a mixture of questions sourced from related research and newly developed question items. A careful selection of questions was made from existing questionnaires designed for specific areas of related research [18, 25, 55, 60, 75]. These questions were then adapted to suit the context and objectives of this study. This allowed the utilisation of already explored assessments that were relevant to the study's focus.

However, given the unique combination of elements in the study, including the integration of AR technology, cybersecurity training with an emphasis on password security, collaborative interactions, and the utilisation of multiple AR devices, there was a lack of pre-existing questionnaires specifically designed for this particular research context. To address this gap, self-developed question items were incorporated to capture the unique aspects of interest that were not adequately covered by existing sources. This approach of combining already established and new questions ensured a comprehensive assessment of the targeted research areas and provided insights specific to the study's objectives.

Both the pre-training and post-training questionnaires encompassed a set of 10 identical questions, requiring participants to evaluate pairs of passwords and determine their relative level of security or if they are equally secure, adopting a question pattern similar to the one presented by Ur [88]. This deliberate design of having both

a pre- and post-training sub-questionnaire allowed for the measurement of changes in participants' responses as an indicator of the training's effectiveness. One instance of the questions provided is (the corrected answer was not highlighted):

> **Compare the provided security level between these two passwords:**
> **P1:** ***12345678!*** **P2:** ***AbCdEfGhIjKlMnOp!***
>
> A. P1 is more secure.
>
> B. Both passwords are equally secure.
>
> **C. P2 is more secure.**

The list of passwords for each question, along with an indication of which of the two passwords is considered more secure, is given in Table 4.4. It is important to note that the determination of password safety is solely based on the rules outlined in Table 3.3. Other factors, such as the avoidance of dictionary words, which are generally regarded as poor practice, are not taken into consideration in this context. Therefore, it should be acknowledged that the relative safety of the passwords may differ if additional criteria, such as the exclusion of dictionary words, were considered.

4.2. Results and Discussion

In this study, the collected data was subjected to statistical analysis using the R programming language, inside the R Studio IDE[3]. All aspects were evaluated using a statistical significance level of 0.05 to ensure a comprehensive analysis. To assess the normality assumption, the Shapiro-Wilk test was performed on the responses of each applicable question. It is important to note that due to the relatively small sample size, it was expected that the data would violate the normality assumption. As expected, most of the questions tested breached the normality assumption. As a result, non-parametric tests were used for subsequent analyses to account for these violations of normality.

However, to proceed with further analysis, the assumption of equal variances was examined using the Levene's test. It was chosen since it does not assume that the underlying data come from a normal distribution. Interestingly, the results indicated that the assumption of equal variances was met for an overwhelming amount of questions, when observing the HoloLens 2 group and the mobile phone group separately.

[3] `https://posit.co/products/open-source/rstudio/`

Table 4.4: Correct passwords in the password security pre- and post-questionnaires

Password 1 (P1)	**Password 2 (P2)**
PurpleSunset789!	Sunshine123!
Choice explanation: P1 has a longer length and a better combination of uppercase and lowercase letters.	
Password123!	987654321!
Choice explanation: P1 has a longer length, includes a mixture of uppercase and lowercase letters, numbers, and a special character, as well as does not follow a predictable pattern.	
MySecretWord2023!	ABCDEFGH!
Choice explanation: P1 has a longer length, includes a mixture of uppercase and lowercase letters, numbers, and a special character, as well as does not follow a predictable pattern.	
TrickyP@ssw0rd!	P@ssw0rd123!
Choice explanation: P1 has a longer length and includes multiple special characters.	
PurpleGiraffe876!	Password987!
Choice explanation: P1 has a longer length and a better combination of uppercase and lowercase letters.	
12345678!	**AbCdEfGhIjKlMnOp!**
Choice explanation: P2 has a longer length, includes a mixture of uppercase and lowercase letters, and follows a less predictable pattern.	
MyDogSpot#1	CorrectHorseBatteryStaple
Choice explanation: P1 is shorter, but includes a variety of character types.	
Qwerty123!	ZXCVBNM456!
Choice explanation: P1 is shorter, but includes a mixture of uppercase and lowercase letters and numbers.	
MyFavoriteColorIsBlue!	**5tarW@rsFan!**
Choice explanation: P2 is shorter, but it includes a mixture of character types.	
Tr0ub4dor&3!	**$ecur3P@$$w0rd!**
Choice explanation: P2 has a longer length and includes a larger mixture of character types.	

This finding provides assurance that the groups exhibit similar variability, despite the deviation from normality.

Subsequently, all questions posed to participants after using the application were subjected to the Mann-Whitney U test to examine the significance of differences in responses between the HoloLens 2 and mobile phone groups. This non-parametric

test was chosen because of the observed violation of the normality assumption, while the assumption of homoscedasticity was satisfied. The Mann-Whitney U test allows for the comparison of medians between two independent groups without relying on the assumption of normal distribution. This analysis was performed only for data of ordinal nature, such as responses based on the Likert scale, to gain insight into potential variations in response patterns between the two groups. The test was performed with continuity correction due to tied values present in the responses. The only two questions that exhibited significance difference on the AR device variable were:

- *To what extent did the virtual objects give the impression of being displayed on a screen (2D) or create the perception of being situated in physical space (3D)?* and
- *To what extent did the gesture interactions for button pressing feel intuitive/natural?*

The following subsections showcase box plots that provide a graphical representation of the participants' responses. These box plots are presented for the entire participant group (N=18) as well as for each subgroup based on the AR device used, namely HoloLens 2 (N=9) and mobile phone (N=9). The purpose of this subdivision is to identify differences or similarities in the participants' experiences based on the specific AR device utilised during the training, yielding a more nuanced understanding of the impact of device choice on their overall experience.

4.2.1. Application Experience

All participants expressed their enjoyment in using the application, indicating a positive user experience (see Figure 4.3a). Furthermore, all but one participant reported a positive level of satisfaction in the acquisition of cybersecurity knowledge through the application (see Figure 4.3b). Regarding the overall comments about the application, several strengths were highlighted, including the educational and entertaining nature of Scenario 1, which effectively showcased the ease of piecing together a password based on contextual clues. One user mentioned that the collaborative aspect of the application could have been further emphasised to make communication between users essential rather than voluntary. Some participants experienced anchor and synchronisation issues, which have already been elaborated on in more detail in Subsection 4.2.6, indicating potential areas for improvement in terms of technical performance.

Regarding the presence of gamification elements (see Figure 4.3c), the results indicate that the majority of participants (88.9%) perceived these elements as enhancing

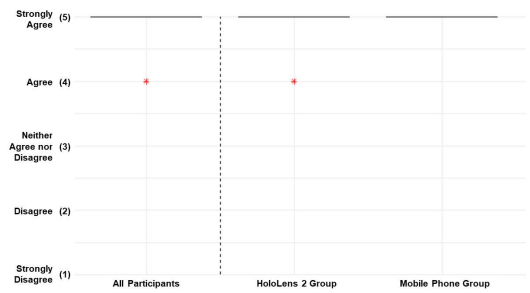
their learning experience during the training. Analysis of the participant's responses to the information provided on specific scenarios and their contexts (see Figure 4.3d) revealed that two-thirds of the participants were completely or relatively satisfied with the amount of information and context provided during application use. When talking about specific game elements that provided instructions and further context, participants found the instruction panels, which contained information on how to navigate and interact with the application, with 94.4% acknowledging that they served as good guidance. The chevron placement guides were perceived as valuable guidance by 55.6% of participants, while a third of the participants noticed them but did not pay significant attention. In Scenario 1, 55.6% of the participants found the object hints to be helpful, while 38.9% did not notice them at all. It should be noted that this latter group included participants who successfully entered the correct password before the halfway mark when the hints were meant to appear.

As all participants successfully entered the correct password in Scenario 1, it was expected that they would agree that sufficient time was provided for the task, and the majority indeed agreed (see Figure 4.3e). Furthermore, the use of storytelling (see Figure 4.3f) in Scenario 1 was well-received, with 50% of participants mainly agreeing and 44.4% completely agreeing that it enhanced their engagement in the task.

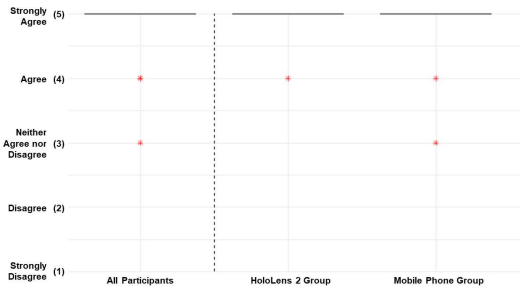
In Scenario 2, the majority of participants (61.1%) intentionally created a different password than they normally would. Factors that influenced this decision included the presence of another person (83.3%), the prompts from Scenario 1 (33.3%), and increased awareness of password generation issues (50%). This demonstrates that the collaborative nature of the application and the impact of the training on participants' awareness influenced their password creation choices. Furthermore, 55.6% of the participants created a completely new password using their usual approach, while 38.9% used a different approach, suggesting that the training encouraged most of the participants to create new passwords and some to reconsider their usual password choices.

4.2.2. Collaborative Experience

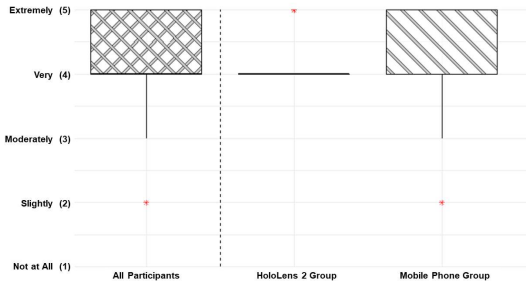
When asked about their enjoyment of the collaboration aspect of the application, the majority of the participants (83.3%) agreed that they enjoyed collaborating with their partner (see Figure 4.4a), indicating that the collaborative elements of the application were well-received and contributed to a positive user experience. The ease of collaboration in Scenario 1 was perceived positively by an overwhelming majority of participants (88.9%) (see Figures 4.4c), whereas Scenario 2 received a lower per-



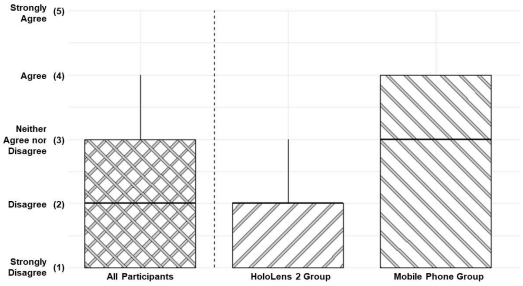
(a) *I enjoyed using this application.*



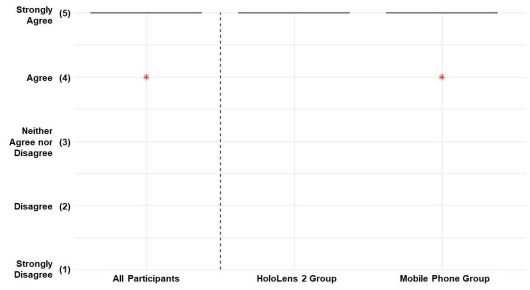
(b) *I enjoyed acquiring cybersecurity knowledge through the use of this application.*



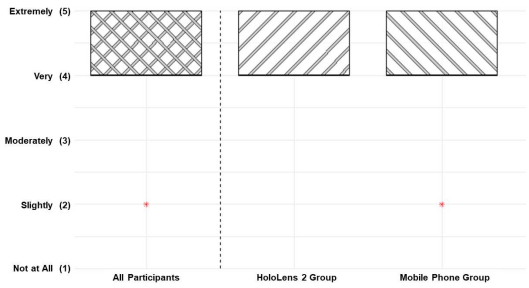
(c) *To what extent do you feel that the presence of gamification elements enhanced your learning during the training?*



(d) *I would have preferred the application to provide more detailed information about the specific scenarios and their respective contexts.*



(e) *There was enough time given in Scenario 1.*



(f) *To what extent did the utilisation of storytelling in Scenario 1 enhance your engagement with the assigned task?*

Figure 4.3: Box plots for questions on the general application experience

centage than Scenario 1, while still being the majority (66.67%) (see Figures 4.4d). The lower percentage for Scenario 2 compared to Scenario 1 is potentially rooted in the synchronisation issues participants experienced specifically in that scenario (see Subsection 4.2.6.

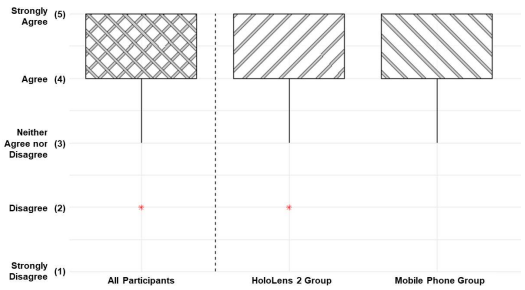
In terms of the sense of shared environment, participants expressed mixed opinions (see Figure 4.4e). These findings suggest that the application may have been more successful in fostering a shared experience for certain participants than for others. Examination of the responses among different groups of AR devices did not reveal any discernible differences in the data, indicating that the disparity in experience can-

not be attributed to a specific AR device used, based on the data obtained in this study. Further research incorporating a larger sample size and questions related to this issue is required in order to explore the underlying factors that are related to a sense of shared environment in this context.

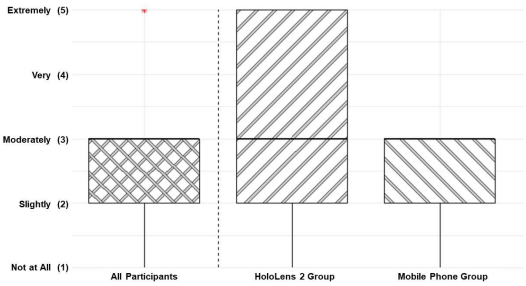
The impact of collaboration on learning effectiveness was also evaluated (see Figure 4.4f), and half of the participants strongly agreed that having a partner during cybersecurity training helped them learn more effectively, compared to doing it alone. However, a third of participants remained neutral regarding the statement. Although this might suggest that collaborative immersive training has the potential to enhance the learning experience and facilitate knowledge acquisition, it should be noted that participants were not exposed to such training individually, without collaboration capabilities. Thus, their prediction of improved learning effectiveness when collaborating serves as an indication rather than a definitive confirmation.

Moreover, participants demonstrated a belief in the overall effectiveness of collaboration in immersive training (see Figure 4.4g). In particular, when examining the groups individually, mobile phone users displayed a high degree of agreement, with almost unanimous agreement with the statement. In contrast, HoloLens 2 users exhibited a wider range of opinions, spanning from strong agreement to strong disagreement. This discrepancy suggests that the perceived impact of collaboration in immersive training may vary depending on the type of AR device used, but any conclusion is again limited due to the small number of samples per device.

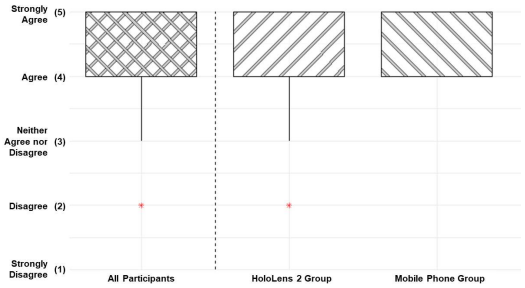
Participants were also asked about the necessity of using the same type of device in collaborative AR experiences, and their responses varied (see Figure 4.4h). While almost two-thirds (61.11%) agreed that users should be using the same type of device, the remaining participants expressed disagreement or neutrality. When asked to elaborate on their choices further, participants expressed a range of opinions. On the one hand, some participants strongly agreed that users should be using the same type of device, emphasising the importance of consistency for a more immersive and cohesive experience. They believed that having the same equipment would enhance the sense of shared environment and facilitate collaboration. On the other hand, participants who disagreed or expressed neutrality mentioned different factors to consider. They noted that using different devices could add variety, fun, or practicality to the collaborative experience. Some participants recognised that collaboration could still occur effectively despite the use of different devices. They highlighted the importance of implementing effective synchronisation of the virtual environment and providing sensory feedback about the presence of other participants, rather than solely relying on device



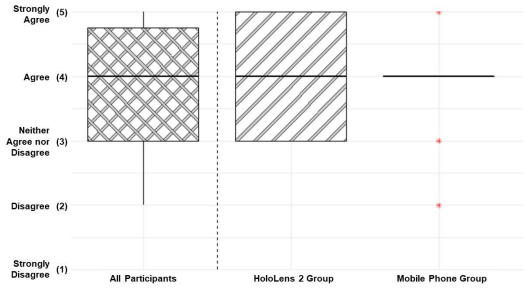
(a) *I enjoyed the collaboration aspect of this application.*



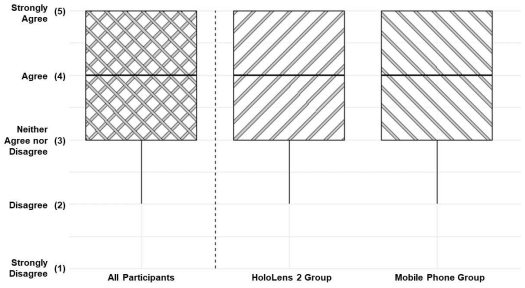
(b) *To what extent did the setup of the application help you perceive the actions taken by your partner within the application?*



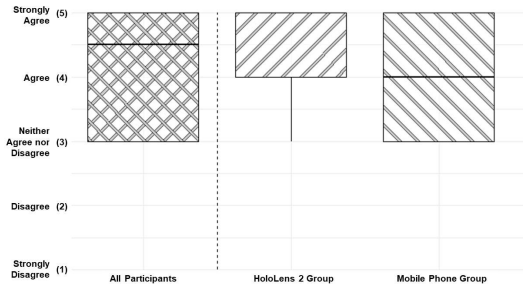
(c) *It was easy to collaborate on the assigned task.* (Scenario 1)



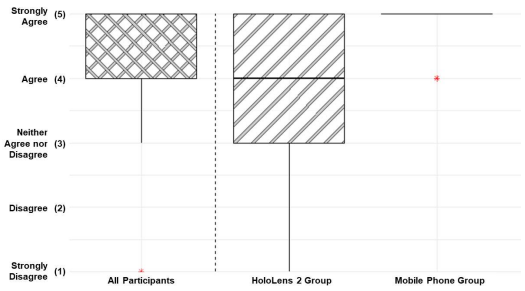
(d) *It was easy to collaborate on the assigned task.* (Scenario 2)



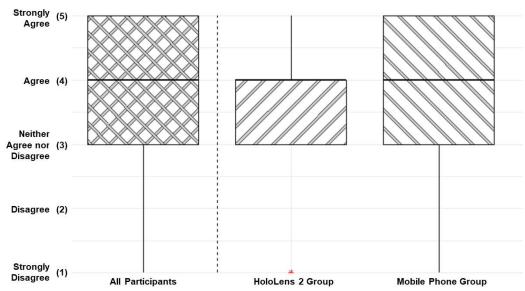
(e) *I felt a strong sense of shared environment with my partner, as if we were observing the same virtual objects in the exact same positions within the physical world.*



(f) *I found that having a partner during this cybersecurity training helped me learn more effectively compared to doing it alone.*



(g) *I believe that collaboration enhances the effectiveness of any type of immersive training compared to individual efforts.*



(h) *I think that users should be using the same type of device in collaborative AR experiences.*

Figure 4.4: Box plots for questions on the collaboration experience

uniformity. These findings suggest that participants' perspectives on device uniformity are influenced by considerations of immersion, practicality, collaborative functionality, and application design. They state that, while device uniformity may contribute to a seamless collaborative experience, it is not the sole determining factor.

4.2.3. Virtual Environment and Interaction Experience

Participants were asked to assess the level of realism of the virtual environment they were exposed to (see Figure 4.5a). While a majority of participants agreed (61.1%) that the virtual environment appeared real, a notable percentage disagreed or expressed neutral views (38.9%). Regarding the participants' sense of direct contact with the virtual environment (see Figure 4.5b), specifically their ability to physically touch and hold virtual objects, the majority of participants (66.7%) agreed with this statement. However, a third of the participants expressed either negative or neutral views, highlighting the existing gap between the cohesion of the physical and virtual elements. To bridge this gap, efforts have been made to incorporate haptic feedback and other sensory elements into the experience.

Furthermore, participants' responses regarding the perception of virtual objects being displayed on a screen (2D) or situated in physical space (3D) yielded mixed results (see Figure 4.5c). Through a majority (61.1%) perceived the virtual objects as 3D in real space, a significant proportion (38.8%) felt that the objects were somewhat 2D, approaching a 3D experience but not fully attaining it. It is important to note that the experiences varied between HoloLens 2 and mobile device users. Somewhat expected, due to the way that the virtual content is presented to the user, HoloLens 2 users primarily experienced the virtual objects in a 3D sense, while mobile device users reported perceiving the objects as mostly 2D.

When considering the level of distraction caused by the device's visual representation (see Figure 4.5d), almost two-thirds (61.1%) of participants reported slight to moderate distraction, indicating that the visual representation of the virtual environment may have affected participants' focus to some extent during the assigned tasks. Participants attributed this distraction primarily to device-specific factors, with limited FoV being the most significant contributor mentioned by the majority of participants (81.3%). Other factors mentioned included display rendering quality (25%) and lag (12.5%). When observing on a device-specific level, the results for each device are given in the Table 4.5. Notably, despite the larger FoV of the mobile phone used compared to the HoloLens 2, as described in Subsection 4.1.2, both groups identified the

Table 4.5: Visual device-specific factors serving as a distraction while executing assigned tasks

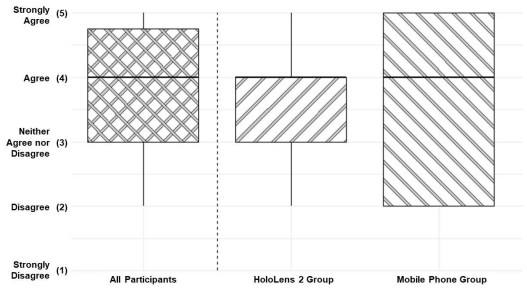
	AR device	
Factor	**HoloLens 2**	**Mobile phone**
Narrow FoV	6	7
Render quality	3	1
Lag	0	2
Unaccustomedness to AR	2	0

FoV as the main distraction. Also described in that Subsection is the lower visual quality of the rendered by the HoloLens 2 due to its approach to AR. This discrepancy in visual quality was reflected in the feedback from HoloLens 2 users, with a third of them expressing that the render quality was a distraction. In contrast, only one participant using the mobile phone device reported this issue.

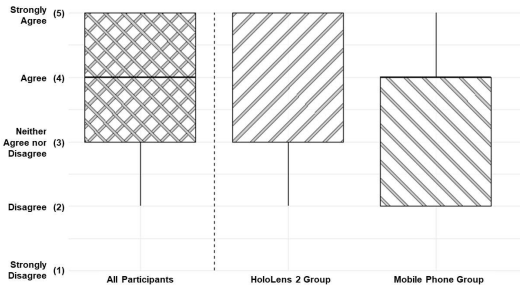
Participants were asked to provide an overall rating for the visual design of the application and appearance of the virtual environment (see Figure 4.5e). All participants expressed a positive attitude towards the visual design, with 44.4% of participants rating the experience as excellent and 55.6% as above average.

Participants were also asked on specific interactions with the virtual environment exhibited in the application and the mechanics tied to those interactions. In terms of concentration on the assigned tasks rather than concentrating on the mechanisms used to perform those tasks (see Figure 4.5f), a majority of participants (66.7%) reported being able to concentrate very well, indicating that the application's design and interaction mechanisms effectively facilitated task-focused engagement. However, a small percentage of participants (22.2%) indicated slight or moderate difficulty in focusing solely on the assigned tasks. This finding highlights the importance of optimising the interaction mechanisms to minimise any additional cognitive load associated with focusing on the means rather than the desired outcomes. By streamlining the interaction process, the application can enable users to concentrate more effectively on their goals.

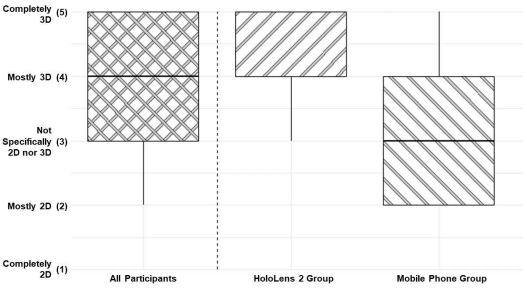
In terms of relying on pointing with their fingers in real space while using the application, participants were evenly split. However, when considering the usage patterns at the device level, two-thirds of HoloLens 2 users reported using pointing gestures during their interaction with the application. In contrast, a third of mobile phone users indicated using pointing gestures throughout their use of the application. Participants also provided an overall rating for the interaction experience (see Figure 4.5g), with over a half (55.6%) rating the experience as excellent and a third as above average.



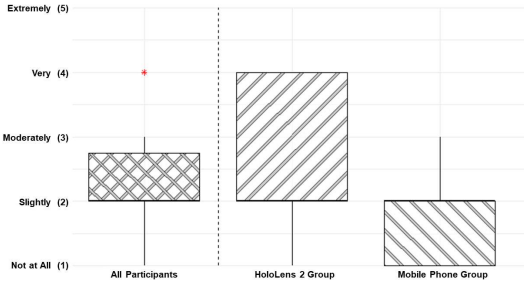
(a) *The virtual environment appeared real.*



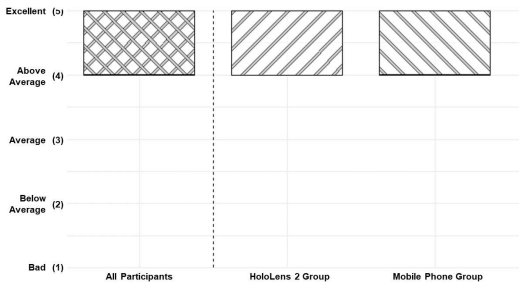
(b) *I felt in direct contact with the virtual environment.*



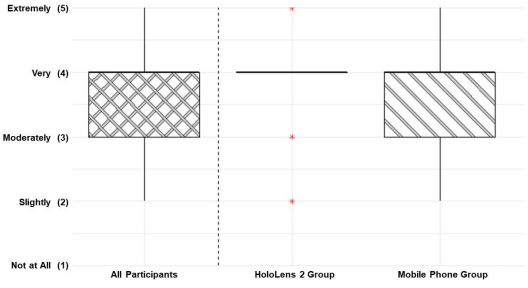
(c) *To what extent did the virtual objects give the impression of being displayed on a screen (2D) or create the perception of being situated in physical space (3D)?*



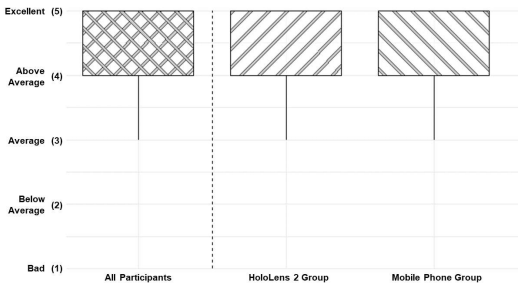
(d) *To what extent did the device's visual representation of the virtual environment distract you from completing the assigned tasks?*



(e) *Please provide your feedback on the visual design and appearance of the virtual environment in the application.*



(f) *To what extent were you able to concentrate on the assigned tasks rather than on the mechanisms used to perform those tasks?*



(g) *Please provide an overall rating for the interaction experience in the application.*

Figure 4.5: Box plots for questions on the virtual environment and user interactions

Figure 4.6 illustrates the participants' perceptions regarding the intuitive and natural feel of specific interactions. The questionnaire included seven distinct interactions, which were categorised into two groups based on the AR device employed. This categorisation was implemented to facilitate a thorough analysis of how each device influenced the perceived intuitiveness of each interaction. This categorisation allowed for a detailed examination of how each device influenced the perceived intuitiveness of each interaction, considering divergent gestures and execution approaches to each interaction inherent to each device.

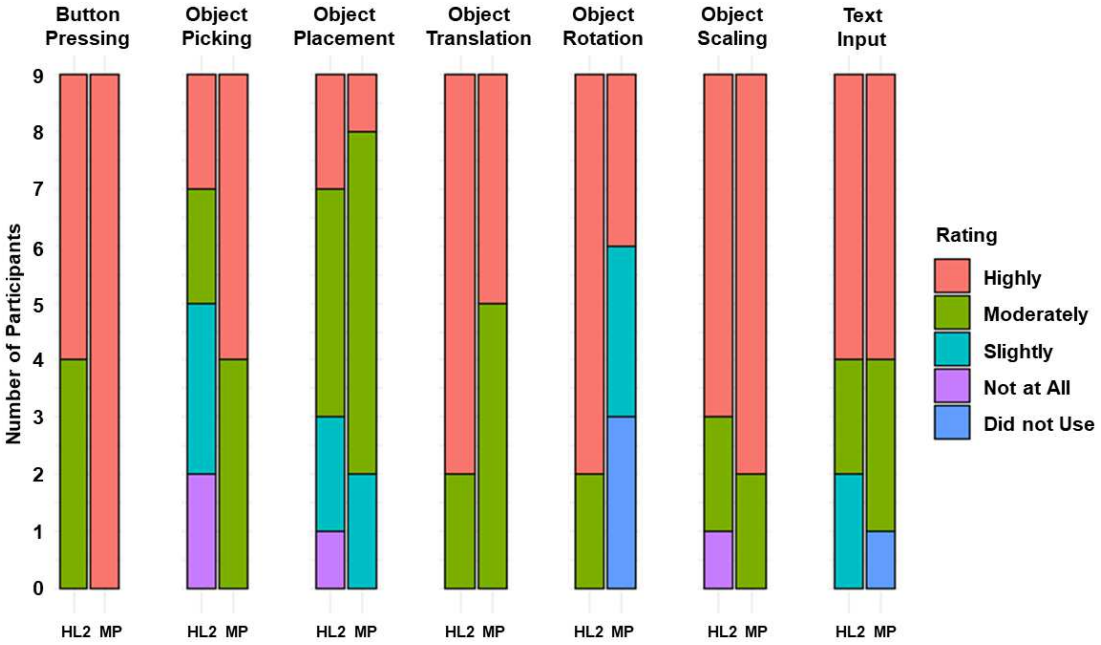


Figure 4.6: Interaction intuitiveness for the HoloLens 2 (HL2) and mobile phone (MP) groups

Regarding button pressing, mobile phone users reported no lack of intuitiveness, while the majority (55.6%) of HoloLens 2 users also found completely intuitive. However, a notable portion (44.4%) of HoloLens 2 users encountered some challenges, albeit to a lesser extent. In terms of object picking, mobile phone users generally did not express significant issues with intuitiveness. However, within the HoloLens 2 group, participants reported a wide range of perceived intuitiveness. Approximately 44.4% indicated minimal to moderate lack of intuitiveness, while 55.6% attributed strong or complete lack of intuitiveness to the interaction. Notably, HoloLens 2 users encountered difficulties when picking panel-like rule objects due to the objects' flat profile and relatively small colliders in terms of height, making it challenging to grasp the panel when in close proximity. Regarding object placement, both groups reported varying levels of lack of intuitiveness. Multiple participants, particularly in the HoloLens 2 group, specifically mentioned issues related to the rule panels during the study trials.

However, the lack of unison ratings for intuitiveness was less pronounced compared to the previous interaction.

In terms of object translation, HoloLens 2 users generally had a slightly better experience, with a majority of users perceiving the interaction as highly intuitive. In contrast, although the majority of mobile phone users also rated the interaction positively, a few expressed moderate issues with intuitiveness. Overall, the ratings for this interaction remained at good levels of intuitiveness in both groups. For object rotation, the HoloLens 2 group did not encounter significant problems and found the interaction intuitive. In contrast, mobile phone users reported either no difficulties or sufficient issues that affected the perceived intuitiveness of the interaction. It is worth noting that a third of mobile phone users did not even use the rotation interaction, which may be attributed to the lack of exposure to the interaction in the Scenario 0. However, other participants in both groups were able to discover the rotation interaction easily by executing other interactions, such as scaling. Regarding object scaling, the overwhelming majority in both groups rated the interaction as highly intuitive. However, a single participant in the HoloLens 2 group reported no intuitiveness at all for this interaction.

In terms of text input, slightly over half of the participants in both groups (55.6%) perceived the interaction as completely intuitive. The remaining participants expressed varying degrees of intuitiveness, with 22.2% of HoloLens 2 users reporting moderate intuitive tendencies and the remaining 22.2% indicating weaker intuitiveness. Among mobile phone users, most reported moderate intuitive tendencies, while one user did not utilise the keyboard feature.

4.2.4. General Outlook on XR and Training

Participants exhibited a positive attitude towards immersive learning experiences (see Figure 4.7a), with all but one participant agreeing that they would pay more attention to acquiring new skills if they were presented in a immersive manner similar to this application. When asked about the perceived effectiveness of immersive experiences compared to traditional learning approaches (see Figure 4.7b), participants demonstrated a favourable view of XR technologies. More than two-thirds of participants (72.2%) agreed that immersive experiences are more effective learning methods compared to textbooks, videos, or traditional lectures. While participants acknowledged the benefits of XR in terms of learning, there was also a degree of skepticism regarding the complete replacement of traditional learning methods (see Figure 4.7c). A considerable portion of participants (44.4%) expressed a certain level of disagreement that

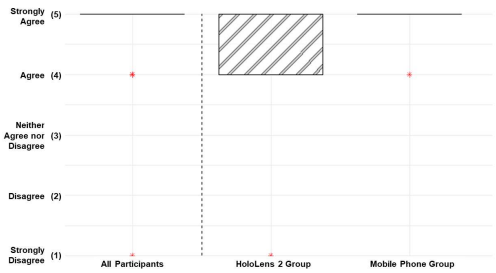
immersive experiences could entirely replace skill acquisition from traditional sources, while almost a third (27.8%) remained undecided on the idea, suggesting that participants still recognise the value of traditional educational resources alongside the usage of XR. However, a considerable proportion (72.2%) agreed or strongly agreed that immersive experiences could serve as an extension or addition to gaining skillsets from traditional sources (see Figure 4.7d).

In terms of incorporating XR into everyday life (see Figure 4.7e), a two-thirds of participants either agreed or strongly agreed that they would like to integrate AR applications into their routines. However, the last third of the participants expressed disagreement or uncertainty towards the concept. Although the participants acknowledge the appeal of XR technologies, based on previous responses, these technologies need not be suitable for everyone in their daily lives. When it comes to incorporating AR applications similar to the developed application into various types of training, participants expressed a slightly stronger inclination (see Figure 4.7f). The findings indicate that a significant majority of participants (77.8%) expressed agreement or strong agreement towards the integration of AR applications into any type of training. This suggests a higher level of receptiveness among participants in leveraging XR technologies to enhance training experiences across a wide range of domains, as opposed to the previously discussed utilisation of XR for non-training-related everyday tasks.

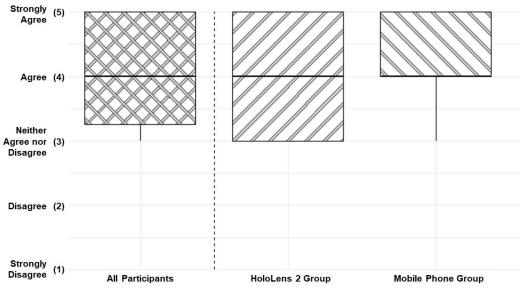
4.2.5. Password Security Knowledge

During the study trial, participants were asked twice, before and after training, to compare the relative security level between two passwords and determine which one offers greater security, based on the predefined criteria outlined earlier in the thesis. The options presented to the participants included answers indicating that the first password is more secure, the second password is more secure, and both passwords are equally secure. To investigate the impact of AR cybersecurity training on participants' performance, an analysis of the trends in correct question answering was conducted, encompassing data collected both before and after exposure to the training. The corresponding graphical representation of these trends can be observed in Figure 4.8.

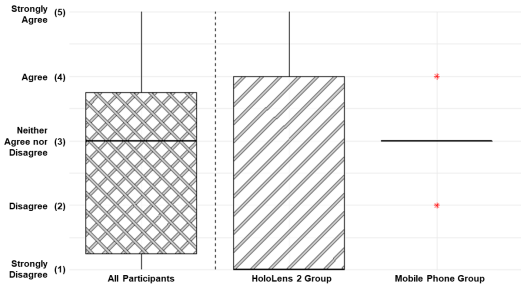
When considering only the guidelines provided in the application, the participants consistently demonstrated improved performance in selecting the correct answers between two password options, with the exception of one question. Furthermore, it is worth highlighting that Question 7 exhibited a notable increase of 7 correct answers, and Question 8 showed a significant improvement of 6 correct answers after the train-



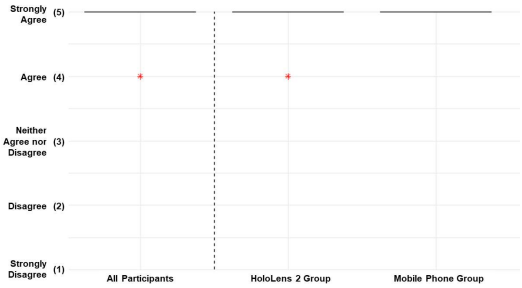
(a) *I would pay more attention to acquiring new skills if they were presented in an immersive manner, similar to this application.*



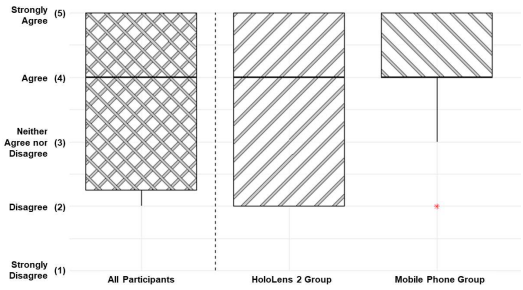
(b) *I believe that immersive experiences are a more effective learning method compared to textbooks, videos, or traditional lectures.*



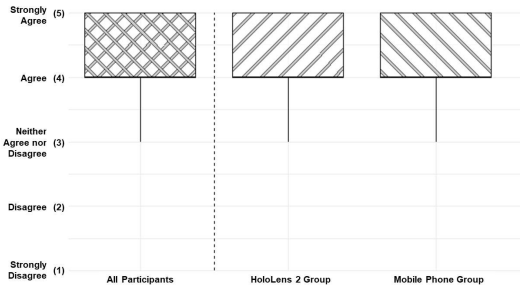
(c) *I think that immersive experiences have the potential to completely replace the acquisition of skillsets from textbooks, videos, or traditional lectures.*



(d) *I think that immersive experiences can serve as an extension of/addition to gaining skillsets from a textbook, video or a traditional lecture.*



(e) *I would generally like to incorporate the use AR applications in my everyday life.*



(f) *I would generally like to incorporate the use AR applications similar to this one in any type of training.*

Figure 4.7: Box plots for questions on the general outlook of participants on XR and trainings

ing. These findings might suggest a substantial enhancement in participants' ability to evaluate password security in those specific scenarios. However, a closer examination of the questions and responses reveals that participants may have overly adapted their perceptions of password security based on the explicit rules presented in the application, which is to be expected, but not ideal. It is important to note that the application did not cover certain rules such as avoiding common words and more complex predictable patterns in password creation, which participants might have been aware of before taking part in the study. Since these rules were not explicitly addressed in the

Figure 4.8: Correct answer trends for each question in pre- and post-training questionnaires

application, participants may have considered them to be of less importance and therefore less secure compared to the emphasised rules. To avoid this, a wider coverage of password security rules should be incorporated within the application.

In contrast, Question 6 exhibited a decrease in the number of correct answers from the pre-training to post-training phase. Prior to using the application, a significant majority of participants (88.9%) expressed the belief that the second password, `AbCdEfGhIjKlMnOp!`, which is the correct password, was more secure. Only two participants considered both passwords, `12345678!` and `AbCdEfGhIjKlMnOp!`, to be equally secure. Surprisingly, after the training, two participants who had initially identified the second password as more secure switched their response to indicating that both passwords were equally secure. This change in perception is somewhat perplexing since the second password aligns with the criteria of being longer and incorporating different character groups, including both uppercase and lowercase letters, as opposed to the first password which consists only of numbers, alongside both containing a special character.

Based on the analysis of the questionnaire responses, several questions exhibited a notable tendency among participants to believe that both passwords were equal in strength. For instance, prior to the training, approximately half of the participants in Question 7 indicated that both passwords held the same level of security. However, after being exposed to the training, there was a shift in perceptions. While a third of the participants still held the belief that both passwords were equally secure, the

majority of participants, along with one individual who initially considered the first password to be more secure, changed their stance and recognised the second password as the correct and more secure option. Another example is evident in Question 8, where a higher number of participants in the post-training questionnaire expressed the belief that both passwords were correct than in the pre-training one. This aligns with the previously discussed indication of participants shifting their perception of the first password's strength, recognising it as the correct option, after undergoing the training.

The observed patterns in accurate responses indicate an overall generally positive impact of AR cybersecurity training on participants' comprehension of password security, specifically regarding password strength. The majority of the questions saw an increase in correct answers after the training, suggesting an improvement in participants' ability to evaluate the security level of passwords. Nonetheless, as discussed previously, various factors may have influenced participants' final choices, highlighting the need for further evaluation and refinement of the questions assessing the participants' comprehension of password security and the existing rules, as well as the inclusion of more rules, presented to the users in the training to ensure consistent and comprehensive knowledge acquisition across all areas of password security.

4.2.6. Limitations

This study aims to provide insight into the efficacy of immersive cybersecurity training, including a collaborative framework and the use of various AR devices. However, it is important to acknowledge certain limitations that may impact the interpretation of the study findings. One significant limitation is the relatively small sample size of 18 participants in total. When dividing the participants further into groups based on the AR devices used, each group consists of only 9 participants per device. This limited sample size raises concerns about the generalisability and statistical significance of the results. Therefore, caution should be exercised when drawing conclusions from this study. Future research with larger and more diverse participant groups is warranted to further validate and expand upon the findings.

Furthermore, it is important to consider the limitations associated with the questionnaire used in this study. The questionnaire was nonstandardised, comprising a combination of questions derived from previous research and original inquiries. While this approach allowed for customisation and exploration of specific aspects related to immersive cybersecurity training, the lack of standardisation may introduce variability

in how participants interpret and respond to the questionnaire items, potentially influencing the accuracy and reliability of the gathered data. Future research in the field of AR training with a collaborative aspect would benefit from the use of a standardised assessment survey. However, it is important to acknowledge that developing a comprehensive and validated questionnaire specifically tailored to the niche context of AR collaborative training may pose certain challenges. The development and validation of such a specialised questionnaire would require careful consideration and examination of the unique characteristics and requirements of AR training environments. Therefore, it is recommended that further investigation be conducted to explore the feasibility and potential benefits of developing a standardised questionnaire that specifically addresses the intricacies and nuances of AR collaborative training.

Moreover, with regard to the questionnaire employed, it is important to recognise that the study relied primarily on subjective participant feedback. While attempting to mitigate potential biases by using mostly close-ended questions, subjective measures are still vulnerable to individual biases, subjective interpretations of questions, and variations in participants' ability to accurately articulate their experiences. To enhance the objectivity of future evaluations, incorporating objective measures alongside subjective assessments could provide a more comprehensive understanding of the effectiveness and impact of immersive cybersecurity training. Objective measures, such as performance metrics (task completion time, task accuracy) and physiological indicators (heart rate, cognitive load), could provide a more comprehensive understanding of training effectiveness. However, selecting appropriate objective measures becomes challenging when comparing different AR devices. Consistency and standardisation of measures across devices are essential to ensure meaningful conclusions. Thus, careful consideration is needed to identify objective measures that capture relevant aspects of the training experience uniformly across different AR platforms.

An oversight has been detected in the questionnaire related to a specific question. The question *To what extent did the application setup contribute to your perception of your partner's actions within the application?* (see Figure 4.4b) failed to differentiate between Scenario 1 and Scenario 2, despite the need for separate assessments. It is noteworthy that in Scenario 1, the user is unable to observe their partner's manipulation of virtual objects, whereas Scenario 2 incorporates real-time synchronisation, allowing users to witness each other's movements and placement of rule panels. Consequently, the current formulation of the question lacks coherence as it fails to acknowledge the divergent nature of these scenarios in terms of perceiving the other user's actions. This ambiguity compromises the usability of both the question and its corresponding re-

sponses, as participants struggle to give a response to a question that encompasses contrasting situations. Several participants expressed concerns about the logical consistency of the question during the study. For future research employing this question in the context of this particular application, it is recommended to split it into two separate questions, asking the same question, but for Scenario 1 and Scenario 2 separately.

As mentioned in Subsection 3.6, the application itself features a few limitations in the form of bugs. The presence of these bugs could have presented challenges and uncertainties during the study, potentially affecting the participants' experience and, consequently, their responses. Specifically, issues related to obstructing anchored virtual elements and desynchronisation of rule matching in the shared virtual environment may have impacted the participants' engagement and the overall effectiveness of their immersive cybersecurity training. Participants might have encountered these issues while using the application, leading to disruptions and inconsistencies in their immersive cybersecurity training process. Therefore, it is important to acknowledge the potential influence of these application limitations on the study outcomes and participants' feedback. Addressing these bugs in future iterations of the application is crucial to enhance the overall UX, improve reliability, and ensure consistent participant responses for future studies.

CONCLUSION

This thesis presents the design and implementation of *SecuAR Together*, a collaborative cybersecurity training application for multiple AR platforms, along with its evaluation. The application offers two interactive scenarios focusing on password security principles and provides hands-on learning opportunities. Despite the presence of several bugs and limitations, the application shows potential for enhancing user experience. Future refinements of the application should address these issues to improve reliability and maximise the impact of immersive cybersecurity training. The application possesses the potential for further expansion in terms of the number and the range of scenarios implemented. While the focus on password security could be retained, it can also be extended to encompass various other domains of cybersecurity, creating a comprehensive training system for cybersecurity. The user study conducted provides insights into the training experience, revealing positive user experiences and satisfaction with acquiring cybersecurity knowledge through the application. Collaboration within the application is well-received by the majority, although perceptions of a shared environment vary among participants. Opinions diverge regarding the necessity of device uniformity in collaborative augmented reality experiences. The virtual environment is generally regarded as realistic, although some participants perceive the virtual objects as partially 2D. Device-specific virtual environment rendering tends to cause minimal distraction, primarily due to limited FoV. Also observed are significant enhancements in participants' knowledge of password strength after using *SecuAR Together*. However, the study had limitations, such as a small sample size and nonstandardised questionnaire, suggesting the need for future research with larger and more diverse groups and the use of standardised assessment surveys. Objective measures should also be incorporated alongside subjective assessments to provide a comprehensive evaluation of training outcomes. Despite these limitations, the study highlights the potential of interactive and collaborative AR-based training for enhancing password security awareness and calls for further development and refinement of the training framework to improve the user experience and effectiveness in future studies.

REFERENCES

[1] Kamyar Abhari, John SH Baxter, Elvis CS Chen, Ali R Khan, Terry M Peters, Sandrine De Ribaupierre, Roy Eagleson. Training for Planning Tumour Resection: Augmented Reality and Human Factors. *IEEE Transactions on Biomedical Engineering*, 62(6):1466–1477, 2014.

[2] Sonam Adinolf, Peta Wyeth, Ross Brown, Roger Altizer. Towards Designing Agent Based Virtual Reality Applications for Cybersecurity Training. U *Proceedings of the 31st Australian Conference on Human-Computer-Interaction*, pages 452–456, 2019.

[3] Anastasios Agrianidis. Information Security Training and Serious Games, 2021.

[4] Zhuming Ai, Mark A Livingston, Jonathan W Decker. Mission Specific Embedded Training Using Mixed Reality. Technical report, U.S. Naval Research Laboratory, 2011.

[5] Hamed Alqahtani Manolya Kavakli-Thorne. Design and Evaluation of an Augmented Reality Game for Cybersecurity Awareness (CybAR). *Information*, 11 (2):121, 2020.

[6] Hamed Alqahtani Manolya Kavakli-Thorne. Does Decision-Making Style Predict Individuals' Cybersecurity Avoidance Behaviour? U *HCI for Cybersecurity, Privacy and Trust: Second International Conference, HCI-CPT 2020, Held as Part of the 22nd HCI International Conference, HCII 2020, Copenhagen, Denmark, July 19–24, 2020, Proceedings 22*, pages 32–50. Springer, 2020.

[7] Hamed Alqahtani Manolya Kavakli-Thorne. Exploring Factors Affecting User's Cybersecurity Behaviour by Using Mobile Augmented Reality App (CybAR). U *Proceedings of the 2020 12th International Conference on Computer and Automation Engineering*, pages 129–135, 2020.

[8] Hamed Alqahtani Manolya Kavakli-Thorne. Factors Affecting Acceptance of a Mobile Augmented Reality Application for Cybersecurity Awareness. U *Proceedings of the 2020 4th International Conference on Virtual and Augmented Reality Simulations*, pages 18–26, 2020.

[9] Hamed Alqahtani, Manolya Kavakli-Thorne, Majed Alrowaily. The Impact of Gamification Factor in the Acceptance of Cybersecurity Awareness Augmented Reality Game (CybAR). U *HCI for Cybersecurity, Privacy and Trust: Second International Conference, HCI-CPT 2020, Held as Part of the 22nd HCI International Conference, HCII 2020, Copenhagen, Denmark, July 19–24, 2020, Proceedings 22*, pages 16–31. Springer, 2020.

[10] Faieza Abdul Aziz, AS Alsaeed, Shamsuddin Sulaiman, MK Ariffin, Muhammad Faris Al-Hakim. Mixed Reality Improves Education and Training in Assembly Processes. *Journal of Engineering and Technological Sciences*, 52(4): 598–607, 2020.

[11] Ronald T Azuma. A Survey of Augmented Reality. *Presence: teleoperators & virtual environments*, 6(4):355–385, 1997.

[12] Katrin Becker. What's the Difference Between Gamification, Serious Games, Educational Games, and Game-Based Learning. *Acad. Lett*, 209:1–4, 2021.

[13] Melina Bernsland, Arvin Moshfegh, Kevin Lindén, Stefan Bajin, Luis Quintero, Jordi Solsona Belenguer, Asreen Rostami. CS:NO–An Extended Reality Experience for Cyber Security Education. U *ACM International Conference on Interactive Media Experiences*, pages 287–292, 2022.

[14] Bassem Besbes, Sylvie Naudet Collette, Mohamed Tamaazousti, Steve Bourgeois, Vincent Gay-Bellile. An Interactive Augmented Reality System: A Prototype for Industrial Maintenance Training Applications. U *2012 IEEE international symposium on mixed and augmented reality (ISMAR)*, pages 269–270. IEEE, 2012.

[15] Mark Billinghurst, Adrian Clark, Gun Lee, et al. A Survey of Augmented Reality. *Foundations and Trends® in Human–Computer Interaction*, 8(2-3):73–272, 2015.

[16] Amare Birhanu Stefan Rank. KeynVision: Exploring Piano Pedagogy in Mixed

Reality. pages 299–304, 10 2017. ISBN 978-1-4503-5111-9. doi: 10.1145/3130859.3131336.

[17] James Birt, Emma Moore, Michael A Cowling. Piloting Mobile Mixed Reality Simulation in Paramedic Distance Education. U *2017 IEEE 5th International Conference on Serious Games and Applications for Health (SeGAH)*, pages 1–8. IEEE, 2017.

[18] Felix Bork, Alexander Lehner, Ulrich Eck, Nassir Navab, Jens Waschke, Daniela Kugelmann. The Effectiveness of Collaborative Augmented Reality in Gross Anatomy Teaching: A Quantitative and Qualitative Pilot Study. *Anatomical Sciences Education*, 14(5):590–604, 2021.

[19] Andrea Giuseppe Bottino, Pier Luigi Ingrassia, Fabrizio Lamberti, Fernando Sal-Vetti, Francesco Strada, Antony Vitillo. Holo-BLSD: An Augmented Reality Self-Directed Learning and Evaluation System for Effective Basic Life Support Defibrillation Training. U *IMSH Conference, Los Angeles, CA*, 2018.

[20] Brian Soon Wei Chiam, Ivy Mun Wah Leung, Oran Zane Devilly, Clemen Yun Da Ow, Frank Yunqing Guan, Bhing Leet Tan. Novel Augmented Reality Enhanced Solution Towards Vocational Training for People with Mental Disabilities. U *2021 IEEE International Symposium on Mixed and Augmented Reality Adjunct (ISMAR-Adjunct)*, pages 195–200. IEEE, 2021.

[21] Yan-Ming Chiou, Chien-Chung Shen, Chrystalla Mouza, Teomara Rutherford. AAugmented Reality-Based Cybersecurity Education on Phishing. U *2021 IEEE International Conference on Artificial Intelligence and Virtual Reality (AIVR)*, pages 228–231. IEEE, 2021.

[22] Critical Infrastructure Cybersecurity. FFramework for Improving Critical Infrastructure Cybersecurity. *URL: https://nvlpubs. nist. gov/nistpubs/CSWP/NIST. CSWP*, 4162018, 2018.

[23] Lea M Daling, Anas Abdelrazeq, Ingrid Isenhardt. A Comparison of Augmented and Virtual Reality Features in Industrial Trainings. U *Virtual, Augmented and Mixed Reality. Industrial and Everyday Life Applications: 12th International Conference, VAMR 2020, Held as Part of the 22nd HCI International Conference, HCII 2020, Copenhagen, Denmark, July 19–24, 2020, Proceedings, Part II 22*, pages 47–65. Springer, 2020.

[24] Lea M Daling, Marisa Tenbrock, Ingrid Isenhardt, Sabine J Schlittmeier. Assemble It Like This!–Is AR- or VR-Based Training an Effective Alternative to Video-Based Training in Manual Assembly? *Applied Ergonomics*, 110:104021, 2023.

[25] Dragos Datcu, Stephan G Lukosch, Heide K Lukosch. A Collaborative Game to Study Presence and Situational Awareness in a Physical and an Augmented Reality Environment. *J. Univers. Comput. Sci.*, 22(2):247–270, 2016.

[26] Andrew R Dattel, Trevor Goodwin, Harry Brodeen, Daniel Friedenzohn, Omar Ochoa, Hui Wang, Peiheng Gao, Syaza Haris, Irfan Parkar. Using Virtual Reality for Training to Identify Cyber Threats in the Bridge of a Ship. U *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, svezak 66, pages 1957–1961. SAGE Publications Sage CA: Los Angeles, CA, 2022.

[27] Mariolino De Cecco, Alessandro Luchetti, Isidro Butaslac III, Francesco Pilla, Giovanni Maria Achille Guandalini, Jacopo Bonavita, Monica Mazzucato, Kato Hirokazu. Sharing Augmented Reality between a Patient and a Clinician for Assessment and Rehabilitation in Daily Living Activities. *Information*, 14(4): 204, 2023.

[28] Alessandro De Mauro, Jörg Raczkowsky, Reiner Wirtz, Mark Eric Halatsch, Heinz Wörn. Augmented Microscope System for Training and Intra-Operative Purposes. U *Modeling Simulation and Optimization-Focus on Applications*. IntechOpen, 2010.

[29] Sangjun Eom, David Sykes, Shervin Rahimpour, Maria Gorlatova. NeuroLens: Augmented Reality-Based Contextual Guidance through Surgical Tool Tracking in Neurosurgery. U *2022 IEEE International Symposium on Mixed and Augmented Reality (ISMAR)*, pages 355–364. IEEE, 2022.

[30] Delmerico et al. *Enabling Interaction Between Mixed Reality and Robots via Cloud-Based Localization*. Microsoft, 2020. URL `https://www.microsoft.com/en-us/research/blog/enabling-interaction-between-mixed-reality-and-robots-via-cloud-based-localization/`, last accessed: 22.05.2023.

[31] Emily Evans, Megan Dass, William M Muter, Christopher Tuthill, Andrew Q Tan, Randy D Trumbower. A Wearable Mixed Reality Platform to Augment

Overground Walking: A Feasibility Study. *Frontiers in Human Neuroscience*, 16, 2022.

[32] Kurtis Eveleigh David Kline. *HoloToolKit 2017 vs MixedRealityToolkit v2*. Microsoft, 2019. URL `https://github.com/microsoft/MixedRealityToolkit-Unity/wiki/HoloToolKit-2017-vs-MixedRealityToolkit-v2/`, last accessed: 22.05.2023.

[33] Tobias Fertig, David Henkelmann, Andreas Schütz. 360 Degrees of Security: Can VR Increase the Sustainability of ISA Trainings? U *Proceedings of the 55th Hawaii International Conference on System Sciences*, 2022.

[34] Tord Hettervik Frøland, Ilona Heldal, Elisabeth Ersvær, Gry Sjøholt. State-of-the-Art and Future Directions for Using Augmented Reality Head Mounted Displays for First Aid Live Training. U *2020 International Conference on e-Health and Bioengineering (EHB)*, pages 1–6. IEEE, 2020.

[35] Nirit Gavish, Teresa Gutiérrez, Sabine Webel, Jorge Rodríguez, Matteo Peveri, Uli Bockholt, Franco Tecchia. Evaluating Virtual Reality and Augmented Reality Training for Industrial Maintenance and Assembly Tasks. *Interactive Learning Environments*, 23(6):778–798, 2015.

[36] Lynda Gerry, Sofia Dahl, Stefania Serafin. ADEPT: Exploring the Design, Pedagogy, and Analysis of a Mixed Reality Application for Piano Training. U *16th sound and music computing conference*, pages 241–249. Sound and Music Computing Network, 2019.

[37] Andres Vargas Gonzalez, Senglee Koh, Katelynn Kapalo, Robert Sottilare, Patrick Garrity, Mark Billinghurst, Joseph LaViola. A Comparison of Desktop and Augmented Reality Scenario Based Training Authoring Tools. U *2019 IEEE International Symposium on Mixed and Augmented Reality (ISMAR)*, pages 339–350. IEEE, 2019.

[38] Mar Gonzalez-Franco, Rodrigo Pizarro, Julio Cermeron, Katie Li, Jacob Thorn, Windo Hutabarat, Ashutosh Tiwari, Pablo Bermell-Garcia. Immersive Mixed Reality for Manufacturing Training. *Frontiers in Robotics and AI*, 4:3, 2017.

[39] Ariel M Greenberg Jason A Spitaletta. Mixed Reality Social Prosthetic System.

[40] Barbara Guttman Edward A Roback. *An Introduction to Computer Security: The NIST Handbook*, svezak 800. Diane Publishing, 1995.

[41] Betsy Guzmán, Sarah Deresky, Sabrina Taylor, Hawk Wimmer, Ali Momen, Chad Tossell, Michael Boyce, Joel Cartwright, Charles Amburn, Ben Sawyer. Evaluating Mixed Reality and Tablet Technologies in Military Planning. U *2022 Systems and Information Engineering Design Symposium (SIEDS)*, pages 310–314. IEEE, 2022.

[42] John K Haas. A History of the Unity Game Engine. *Diss. Worcester Polytechnic Institute*, 483(2014):484, 2014.

[43] International Telecommunication Union. ITU-T Recommendation G.1035 – Influencing Factors on Quality of Experience for Virtual Reality Services. 2021.

[44] International Telecommunication Union. ITU-T Recommendation P.1320 – QoE Assessment of Extended Reality (XR) Meetings. 2022.

[45] Gokul Chettoor Jayakrishnan, Gangadhara Reddy Sirigireddy, Sukanya Vaddepalli, Vijayanand Banahatti, Sachin Premsukh Lodha, Sankalp Suneel Pandit. Passworld: A Serious Game to Promote Password Awareness and Diversity in an Enterprise. U *Proceedings of the Sixteenth USENIX Conference on Usable Privacy and Security*, pages 1–18, 2020.

[46] Ge Jin, Manghui Tu, Tae-Hoon Kim, Justin Heffron, Jonathan White. Game Based Cybersecurity Training for High School Students. U *Proceedings of the 49th ACM Technical Symposium on Computer Science Education*, pages 68–73, 2018.

[47] Yu Jin, João Monge, Octavian Postolache, Wangqiang Niu. Augmented Reality with Application in Physical Rehabilitation. U *2019 International Conference on Sensing and Instrumentation in IoT Era (ISSI)*, pages 1–6. IEEE, 2019.

[48] Tapas Dipakkumar Joshi. *A Mixed-Reality Approach for Cyber-situation Awareness*. Doktorska disertacija, 2017.

[49] Jussi Kasurinen. Usability Issues of Virtual Reality Learning Simulator in Healthcare and Cybersecurity. *Procedia computer science*, 119:341–349, 2017.

[50] Lara Klooster. VR CyberEducation: Improving the Human Factor in Cybersecurity through an Educational Virtual Reality Program, July 2022. URL `http://essay.utwente.nl/93717/`.

[51] Mikko Korkiakoski, Anssi Antila, Jouni Annamaa, Saeid Sheikhi, Paula Alavesa, Panos Kostakos. Hack the Room: Exploring the Potential of an Augmented Reality Game for Teaching Cyber Security. U *Proceedings of the Augmented Humans International Conference 2023*, pages 349–353, 2023.

[52] Ci-Jyun Liang, Charles Start, Hanna Boley, Vineet R Kamat, Carol C Menassa, Michelle Aebersold. Enhancing Stroke Assessment Simulation Experience in Clinical Training Using Augmented Reality. *Virtual Reality*, 25:575–584, 2021.

[53] Xiao-Wei Liu, Cheng-Yu Li, Sina Dang, Wei Wang, Jue Qu, Tong Chen, Qing-Li Wang. Research on Training Effectiveness of Professional Maintenance Personnel Based on Virtual Reality and Augmented Reality Technology. *Sustainability*, 14(21):14351, 2022.

[54] Stefan Maas, Peter Kopacsi, Peter Kovacs, Arnaud Bosteels. A Mixed Reality Telemedicine System for Collaborative Ultrasound Diagnostics and Ultrasound-Guided Interventions. *AboutOpen*, 9(1):15–20, 2022.

[55] Wannisa Matcha Dayang Rohaya Awang Rambli. Preliminary Investigation on the Use of Augmented Reality in Collaborative Learning. U *Informatics Engineering and Information Science: International Conference, ICIEIS 2011, Kuala Lumpur, Malaysia, November 14-16, 2011, Proceedings, Part IV*, pages 189–198. Springer, 2011.

[56] Brendan Mattina, Franki Yeung, Alex Hsu, Dale Savoy, Joseph Tront, David Raymond. MARCS: Mobile Augmented Reality for Cybersecurity. U *Proceedings of the 12th Annual Conference on Cyber and Information Security Research*, pages 1–4, 2017.

[57] Kevin F McCrohan, Kathryn Engel, James W Harvey. Influence of Awareness and Training on Cyber Security. *Journal of internet Commerce*, 9(1):23–41, 2010.

[58] Liana-Dorina Møsbæk Thomas Bjørner. An Augmented Reality Training Application for Service and Maintenance of a Medical Analyzer: A UX Approach to Usefulness and User Satisfaction. U *2022 8th International Conference of the Immersive Learning Research Network (iLRN)*, pages 1–8. IEEE, 2022.

[59] Mirta Moslavac. Development of an Augmented Reality-Based Prototype Application for Learning How to Play the Piano Using the HoloLens 2 Platform, 2021.

[60] Susanna Nilsson, Björn JE Johansson, Arne Jönsson. A Co-Located Collaborative Augmented Reality Application. U *Proceedings of the 8th International Conference on Virtual Reality Continuum and Its Applications in Industry*, pages 179–184, 2009.

[61] pamistel et al. *Frequently Asked Questions About Azure Spatial Anchors*. Microsoft. URL https://learn.microsoft.com/en-us/azure/spatial-anchors/spatial-anchor-faq/, last accessed: 22.05.2023.

[62] pamistel et al. *Create an Effective Anchor Experience by Using Azure Spatial Anchors*. Microsoft, 2022. URL https://learn.microsoft.com/en-us/azure/spatial-anchors/concepts/guidelines-effective-anchor-experiences/, last accessed: 10.06.2023.

[63] pamistel et al. *Azure Spatial Anchors Overview*. Microsoft, 2022. URL https://learn.microsoft.com/en-us/azure/spatial-anchors/overview/, last accessed: 22.05.2023.

[64] pamistel et al. *Tutorial: Step-by-Step Instructions to Create a New HoloLens Unity App Using Azure Spatial Anchors*. Microsoft, 2023. URL https://learn.microsoft.com/en-us/azure/spatial-anchors/tutorials/tutorial-new-unity-hololens-app/, last accessed: 10.06.2023.

[65] pamistel et al. *TTutorial: Share Spatial Anchors Across Sessions and Devices*. Microsoft, 2023. URL https://learn.microsoft.com/en-us/azure/spatial-anchors/tutorials/tutorial-share-anchors-across-devices/, last accessed: 01.06.2023.

[66] Xingyu Pan, Mengya Zheng, Xuanhui Xu, Abraham G Campbell. Knowing Your Student: Targeted Teaching Decision Support Through Asymmetric Mixed Reality Collaborative Learning. *IEEE Access*, 9:164742–164751, 2021.

[67] *Analyzing Disconnects*. Photon, . URL https://doc.photonengine.com/pun/v1/troubleshooting/analyzing-disconnects/, last accessed: 15.06.2023.

[68] *Photon Unity Networking for Unity Multiplayer Games - PUN2*. Photon, . URL https://www.photonengine.com/pun/, last accessed: 10.06.2023.

[69] *Setup And Connect*. Photon, . URL https://doc.photonengine.com/pun/current/getting-started/initial-setup/, last accessed: 15.06.2023.

[70] Pompeo Piedimonte Silvia Liberata Ullo. Applicability of the Mixed Reality to Maintenance and Training Processes of C4I Systems in Italian Air Force. U *2018 5th IEEE International Workshop on Metrology for AeroSpace (MetroAeroSpace)*, pages 559–564. IEEE, 2018.

[71] Sai Vijay Pola. Evaluating the User Experience of Microsoft HoloLens and Mobile Device Using an Augmented Reality Application, 2019.

[72] Shaila Rana Wasim Alhamdani. Exploring the Need to Study the Efficacy of VR Training Compared to Traditional Cybersecurity Training. *International Journal of Computer and Information Engineering*, 15(1):10–17, 2021.

[73] Shaila Rana Wasim Alhamdani. A VR Cybersecurity Training Knowledge-Based Ontology. *open science index 16 2022*, 2:5, 2022.

[74] Manuel Rebol, Krzysztof Pietroszek, Claudia Ranniger, Colton Hood, Adam Rutenberg, Neal Sikka, David Li, Christian Gütl. Mixed Reality Communication for Medical Procedures: Teaching the Placement of a Central Venous Catheter. U *2022 IEEE International Symposium on Mixed and Augmented Reality (ISMAR)*, pages 346–354. IEEE, 2022.

[75] Holger Regenbrecht Thomas Schubert. Measuring Presence in Augmented Reality Environments: Design and a First Test of a Questionnaire. *arXiv preprint arXiv:2103.02831*, 2021.

[76] Mikel Salazar, José Gaviria, Carlos Laorden, Pablo G Bringas. Enhancing Cybersecurity Learning Through an Augmented Reality-Based Serious Game. U *2013 IEEE global engineering education conference (EDUCON)*, pages 602–607. IEEE, 2013.

[77] Naveen Kumar Sankaran, Harris J Nisar, Ji Zhang, Kyle Formella, Jennifer Amos, Lisa T Barker, John A Vozenilek, Steven M LaValle, Thenkurussi Kesavadas. Efficacy Study on Interactive Mixed Reality (IMR) Software with Sepsis Prevention Medical Education. U *2019 IEEE Conference on Virtual Reality and 3D User Interfaces (VR)*, pages 664–670. IEEE, 2019.

[78] Ben Sawyer. Serious Games: Improving Public Policy Through Game-Based Learning and Simulation. 01 2002.

[79] Richard Schaffer, Sean Cullen, Phe Meas, Kevin Dill. Mixed and Augmented Reality for Marine Corps Training. U *Virtual, Augmented and Mixed Reality. Systems and Applications: 5th International Conference, VAMR 2013, Held as Part of HCI International 2013, Las Vegas, NV, USA, July 21-26, 2013, Proceedings, Part II 5*, pages 310–319. Springer, 2013.

[80] Claudia Schrader. Serious Games and Game-Based Learning. U *Handbook of Open, Distance and Digital Education*, pages 1–14. Springer, 2022.

[81] Norbert M Seel. *Encyclopedia of the Sciences of Learning*. Springer Science & Business Media, 2011.

[82] Jinsil Hwaryoung Seo, Michael Bruner, Austin Payne, Nathan Gober, Donald McMullen, Dhruva K Chakravorty. Using Virtual Reality to Enforce Principles of Cybersecurity. *The Journal of Computational Science Education*, 10(1), 2019.

[83] Avinash Sharma, Christopher L Hunt, Asheesh Maheshwari, Luke Osborn, Gyorgy Lévay, Rahul R Kaliki, Alcimar B Soares, Nitish Thakor. A Mixed-Reality Training Environment for Upper Limb Prosthesis Control. U *2018 IEEE Biomedical Circuits and Systems Conference (BioCAS)*, pages 1–4. IEEE, 2018.

[84] Chien Chung Shen, Yan-Ming Chiou, Chrystalla Mouza, Teomara Rutherford. Work-in-Progress-Design and Evaluation of Mixed Reality Programs for Cybersecurity Education. U *2021 7th International Conference of the Immersive Learning Research Network (iLRN)*, pages 1–3. IEEE, 2021.

[85] Tobias Sielhorst, Tobias Obst, Rainer Burgkart, Robert Riener, Nassir Navab. An Augmented Reality Delivery Simulator for Medical Training. U *International workshop on augmented environments for medical imaging-MICCAI Satellite Workshop*, svezak 141, pages 11–20, 2004.

[86] Kenneth Tan. Implementing Augmented Reality Scenario-Based Learning: Impact Study in the Security Industry. *International Multidisciplinary Research Journal*, 1:1–4, 2021.

[87] Philipp Ulsamer, Andreas Schütz, Tobias Fertig, Lisa Keller. Immersive Storytelling for Information Security Awareness Training in Virtual Reality. 2021.

[88] Blase Eric Ur. Supporting Password-Security Decisions with Data. 2016.

[89] Gary R VandenBos. *APA Dictionary of Psychology*. American Psychological Association, 2007.

[90] Silvestro V Veneruso, Lauren S Ferro, Andrea Marrella, Massimo Mecella, Tiziana Catarci. CyberVR: An Interactive Learning Experience in Virtual Reality for Cybersecurity Related Issues. U *Proceedings of the International Conference on Advanced Visual Interfaces*, pages 1–8, 2020.

[91] Peng Wang, Xiaoliang Bai, Mark Billinghurst, Shusheng Zhang, Sili Wei, Guangyao Xu, Weiping He, Xiangyu Zhang, Jie Zhang. 3DGAM: Using 3D Gesture and CAD Models for Training on Mixed Reality Remote Collaboration. *Multimedia Tools and Applications*, 80:31059–31084, 2021.

[92] Shiyao Wang, Michael Parsons, Jordan Stone-McLean, Peter Rogers, Sarah Boyd, Kristopher Hoover, Oscar Meruvia-Pastor, Minglun Gong, Andrew Smith. Augmented Reality as a Telemedicine Platform for Remote Procedural Training. *Sensors*, 17(10):2294, 2017.

[93] Tania Williams Omar El-Gayar. Design of a Virtual Cybersecurity Escape Room. U *National Cyber Summit (NCS) Research Track 2021*, pages 60–73. Springer, 2022.

[94] Mark Wilson, Joan Hash, SP NIST. SP 800-50: Building an Information Technology Security Awareness and Training Program. 2003. *National Institute of Standards and Technology*.

[95] Mark Wilson, Dorothea E de Zafra, Sadie I Pitcher, John D Tressler, John B Ippolito. Information Technology Security Training Requirements: A Role-and Performance-Based Model. Technical report, National Institute of Standards and Technology, 1998.

[96] Mark Wilson, Joan Hash, et al. Building an Information Technology Security Awareness and Training Program. *NIST Special publication*, 800(50):1–39, 2003.

[97] Michael Yong, Julie Pauwels, Frederick K Kozak, Neil K Chadha. Application of Augmented Reality to Surgical Practice: A Pilot Study Using the ODG R7 Smartglasses. *Clinical Otolaryngology*, 45(1):130–134, 2020.

[98] Ke-yu Zhai, Yi-ming Cao, Wen-jun Hou, Xue-ming Li. Interactive Mixed Reality Cooking Assistant for Unskilled Operating Scenario. U *Virtual, Augmented and Mixed Reality. Industrial and Everyday Life Applications: 12th International Conference, VAMR 2020, Held as Part of the 22nd HCI International Conference, HCII 2020, Copenhagen, Denmark, July 19–24, 2020, Proceedings, Part II 22*, pages 178–195. Springer, 2020.

[99] Leah Zhang-Kennedy Sonia Chiasson. A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education. *ACM Computing Surveys (CSUR)*, 54(1):1–39, 2021.

[100] Shang Zhao, Xiao Xiao, Qiyue Wang, Xiaoke Zhang, Wei Li, Lamia Soghier, James Hahn. An Intelligent Augmented Reality Training Framework for Neonatal Endotracheal Intubation. U *2020 IEEE International Symposium on Mixed and Augmented Reality (ISMAR)*, pages 672–681. IEEE, 2020.

[101] Moshe Zviran William J Haga. Password Security: An Empirical Study. *Journal of Management Information Systems*, 15(4):161–185, 1999.

List of Figures

3.1. Real-life environment and the resulting sparse point cloud (source [61]) 25
3.2. ASA set-up within the application 26
3.3. Chevron guide in Scenario 0 from Player 1's perspective 28
3.4. Representation of Scenario 0 from Player 1's perspective 29
3.5. Representation of Scenario 1 31
3.6. Clues in Scenario 1 33
3.7. Representation of password creation in Scenario 2 35
3.8. Entering a password in Scenario 2 35
3.9. Password security rules in Scenario 2 36
3.10. Representation of password analysis in Scenario 2 37

4.1. Illustration of the dual AR device set-up 46
4.2. Procedure outline of the study 48
4.3. Box plots for questions on the general application experience 55
4.4. Box plots for questions on the collaboration experience 57
4.5. Box plots for questions on the virtual environment and user interactions 60
4.6. Interaction intuitiveness for the HoloLens 2 (HL2) and mobile phone (MP) groups 61
4.7. Box plots for questions on the general outlook of participants on XR and trainings 64
4.8. Correct answer trends for each question in pre- and post-training questionnaires 65

List of Tables

1.1. Descriptions of fundamental concepts referenced throughout the thesis 3

3.1. Interactions featured in Scenario 0 30
3.2. Password clues in Scenario 1 32
3.3. Password rules, with respective regular expressions, used in Scenario 2 40

4.1. Prior AR usage frequency among study participants 48
4.2. Contexts in which study participants have previously encountered AR 49
4.3. AR devices which study participants have previously used 49
4.4. Correct passwords in the password security pre- and post-questionnaires 52
4.5. Visual device-specific factors serving as a distraction while executing assigned tasks 59

ABBREVIATIONS

2D	*Two-Dimensional*
3D	*Three-Dimensional*
6DoF	*6 Degrees of Freedom*
API	*Application Programming Interface*
AR	*Augmented Reality*
ASA	*Azure Spatial Anchors*
CAD	*Computer-Aided Design*
CSA	*Cybersecurity Awareness*
CTF	*Capture the Flag*
FoV	*Field of View*
GBL	*Game-Based Learning*
HMD	*Head-Mounted Display*
IDE	*Integrated Development Environment*
MR	*Mixed Reality*
MRTK(2)	*Mixed Reality Toolkit (v2)*
PUN2	*Photon Unity Networking v2*
QoE	*Quality of Experience*
RPC	*Remote Procedure Call*
RQ	*Research Question*
RPG	*Role-Playing Game*
SBL	*Scenario-Based Learning*
SDK	*Software Development Kit*
SLAM	*Simultaneous Localisation and Mapping*
TCP	*Transmission Control Protocol*
UDP	*User Datagram Protocol*
UI	*User Interface*
UX	*User Experience*
VR	*Virtual Reality*
XR	*Extended Reality*

Appendix A
User Study Questionnaire

Collaborative Cybersecurity Training Study

A questionnaire as a part of the study for my Master's thesis titled *Development and Evaluation of an Augmented Reality-Based Application for Collaborative Cybersecurity Training* at the Faculty of Electrical Engineering and Computing, University of Zagreb, in AY 22/23.

* Indicates required question

Demographic Questionnaire

1. Name and Surname *

_____

2. Gender *

Mark only one oval.

- ◯ Female
- ◯ Transgender Female
- ◯ Male
- ◯ Transgender Male
- ◯ Non-Binary
- ◯ Gender-Fluid
- ◯ Prefer Not to Answer
- ◯ Other: _____

3. Age *

_____

4. Prior Experience with Augmented Reality (AR) *

Mark only one oval.

- ◯ No experience – never tried AR
- ◯ Only tried AR once
- ◯ Used AR a few times
- ◯ Use AR a few times per year
- ◯ Use AR monthly
- ◯ Experienced – use AR approximately 1 or more times per week

5. If you have prior experience, in which context have you encountered AR?

Tick all that apply.

- ☐ Work
- ☐ School
- ☐ Communication
- ☐ Games
- ☐ Other forms of entertainent
- ☐ Other: _____

6. If you have prior experience, what type(s) of AR devices have you used?

Tick all that apply.

- ☐ Mobile phone
- ☐ Head-mounted display (HMD) - e.g., Meta Quest or HoloLens headsets, ...
- ☐ Head-up display (HUD) - e.g., in a car
- ☐ Other: _____

7. Are you currently doing your university studies in or do you have a degree or job in computer science, computer engineering, information technology, or a related field? *

Mark only one oval.

- Yes
- No

General Knowledge Overview

8. Select the degree of agreement with the statement: *
I am well-versed in cybersecurity.

Mark only one oval.

	Strongly disagree
1	
2	
3	
4	
5	Strongly agree

9. Complete the statement: *
I change my passwords...

Mark only one oval.

- ◯ Never
- ◯ When prompted
- ◯ Sometimes, without being prompted
- ◯ Regularly, without being prompted

10. Select if the statement applies to you or not: *
One or more of my passwords were compromised sometimes in the past.

Mark only one oval.

- ◯ Yes
- ◯ No

11. Select if the statement applies to you or not: *
In my lifetime, I have reused the same password for two or more accounts at least once.

Mark only one oval.

- ◯ Yes
- ◯ No

12. Select the degree of agreement with the statement: *
I have relative confidence that I can create strong passwords.

Mark only one oval.

	Strongly disagree					Strongly agree
	1	2	3	4	5	

13. Which of the following statements reflect your daily behaviour related to passwords? *

Tick all that apply.

- [ ] I use a password manager (standalone or in my browser) to automatically enter my passwords for me.
- [ ] I type the entire password from memory.
- [ ] I write my passwords down on a piece of paper.
- [ ] I store my passwords digitally (e.g., in a file or on my phone).
- [ ] I first have to look up a password and then type it in.

14. Have you ever taken part in **any VR/AR training** experiences? *

Mark only one oval.

- Yes
- No

15. Have you ever taken part in a **cybersecurity training** (need not be VR/AR)? *

Mark only one oval.

- ◯ Yes
- ◯ No

16. If so, which type?

Tick all that apply.

- ☐ Textual
- ☐ Audio
- ☐ Video
- ☐ Real-life scenario simulation
- ☐ VR/AR
- ☐ Other: _____

17. If you've taken part in some other type of immersive training (VR/AR), describe briefly what it was?

_____

18. How were you assessed after taking part in these immersive training(s)?

Tick all that apply.

- ☐ Yes/No questions
- ☐ Multi-choice question quiz
- ☐ Short-form open-ended questions
- ☐ Real-life scenario simulation
- ☐ Oral exam
- ☐ Other: _____

Pre-Training Questionnaire

The following 10 questions require you to assess pairs of passwords and determine their relative security level, or if they are equally secure.

19. Compare the provided security level between these two passwords: *
P1: **PurpleSunset789!**
P2: **Sunshine123!**

Mark only one oval.

- ◯ P1 is more secure
- ◯ Both passwords are equally secure
- ◯ P2 is more secure

20. Compare the provided security level between these two passwords: *
P1: **Password123!**
P2: **987654321!**

Mark only one oval.

- ◯ P1 is more secure
- ◯ Both passwords are equally secure
- ◯ P2 is more secure

21. Compare the provided security level between these two passwords: *
P1: **MySecretWord2023!**
P2: **ABCDEFGH!**

Mark only one oval.

- ◯ P1 is more secure
- ◯ Both passwords are equally secure
- ◯ P2 is more secure

22. Compare the provided security level between these two passwords: *
P1: **TrickyP@ssw0rd!**
P2: **P@ssw0rd123!**

Mark only one oval.

- ◯ P1 is more secure
- ◯ Both passwords are equally secure
- ◯ P2 is more secure

23. Compare the provided security level between these two passwords: *
P1: **PurpleGiraffe876!**
P2: **Password987!**

Mark only one oval.

- ◯ P1 is more secure
- ◯ Both passwords are equally secure
- ◯ P2 is more secure

24. Compare the provided security level between these two passwords: *
P1: **12345678!**
P2: **AbCdEfGhIjKlMnOp!**

Mark only one oval.

- ◯ P1 is more secure
- ◯ Both passwords are equally secure
- ◯ P2 is more secure

25. Compare the provided security level between these two passwords: *
P1: **MyDogSpot#1**
P2: **CorrectHorseBatteryStaple**

Mark only one oval.

- ◯ P1 is more secure
- ◯ Both passwords are equally secure
- ◯ P2 is more secure

26. Compare the provided security level between these two passwords: *
P1: **Qwerty123!**
P2: **ZXCVBNM456!**

Mark only one oval.

- ◯ P1 is more secure
- ◯ Both passwords are equally secure
- ◯ P2 is more secure

27. Compare the provided security level between these two passwords: *
P1: **MyFavoriteColorIsBlue!**
P2: **5tarW@rsFan!**

Mark only one oval.

- ◯ P1 is more secure
- ◯ Both passwords are equally secure
- ◯ P2 is more secure

28. Compare the provided security level between these two passwords: *
P1: **Tr0ub4dor&3!**
P2: **$ecur3P@$$w0rd!**

Mark only one oval.

- P1 is more secure
- Both passwords are equally secure
- P2 is more secure

Time to try out the Cybersecurity Awareness Training Application!

29. Select the device you were assigned: *

Mark only one oval.

- HoloLens 2
- Mobile phone

Questionnaire after Using the Application - System Comparison

30. Select the degree of agreement with the statement: *
The virtual environment appeared real.

Mark only one oval.

Strongly disagree

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

Strongly agree

31. Select the degree of agreement with the statement: *
I felt in direct contact with the virtual environment. (e.g., I felt like I could physically touch and hold the virtual objects.)

Mark only one oval.

Strongly disagree

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

Strongly agree

32. To what extent did the virtual objects give the impression of being displayed on a screen (2D) or create the perception of being situated in physical space (3D)? *

Mark only one oval.

	Completely 2D
1	
2	
3	
4	
5	
	Completely 3D

33. To what extent did the device's visual representation of the virtual environment distract you from completing the assigned tasks? *

Mark only one oval.

Not at all

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

Extremely

34. If affected, what influenced the distraction?

Tick all that apply.

- [ ] Limited field of view (extent of the observable virtual environment seen at any given moment)
- [ ] Display/render quality
- [ ] Lag (i.e., low number of frames-per-second, ...)
- [ ] Other: _____

35. Please provide your feedback on the visual design and appearance of the virtual environment in the application. *

Mark only one oval.

Bad

1

2

3

4

5

Excellent

36. To what extent were you able to concentrate on the assigned tasks rather than on the mechanisms used to perform those tasks? *

Mark only one oval.

	Not at all					Extremely
	1	2	3	4	5	

37. To what extent did the gesture interactions for ... feel intuitive/natural? *

Mark only one oval per row.

	Not at all	Slightly	Moderately	Highly	Did not use
Button pressing	◯	◯	◯	◯	◯
Object picking	◯	◯	◯	◯	◯
Object placing (rule placement on the board)	◯	◯	◯	◯	◯
Object translation (movement)	◯	◯	◯	◯	◯
Object rotation	◯	◯	◯	◯	◯
Object scaling	◯	◯	◯	◯	◯
Text input (keyboard usage)	◯	◯	◯	◯	◯

38. Select if the statement applies to you or not: *
I often relied on pointing (with fingers in the real space) while using the application.

Mark only one oval.

◯ Yes

◯ No

39. Please provide an overall rating for the interaction experience in the application. *

Mark only one oval.

Bad

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

Excellent

Questionnaire after Using the Application - Collaboration

40. Select the degree of agreement with the statement: *
I enjoyed the collaboration aspect of this application.

Mark only one oval.

Strongly disagree

1
2
3
4
5

Strongly agree

41. To what extent did the setup of the application help you perceive the actions taken by your partner within the application? *

Mark only one oval.

	Not at all				Extremely
	1	2	3	4	5

42. Select the degree of agreement with the statement for **Scenario 1**: *

It was easy to collaborate on the assigned task.

Mark only one oval.

Strongly disagree

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

Strongly agree

43. Select the degree of agreement with the statement for **Scenario 2**: *
It was easy to collaborate on the assigned task.

Mark only one oval.

Strongly disagree

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

Strongly agree

44. Select the degree of agreement with the statement: *

I felt a strong sense of shared environment with my partner, as if we were observing the same virtual objects in the exact same positions within the physical world.

Mark only one oval.

Strongly disagree

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

Strongly agree

45. Select the degree of agreement with the statement: *

I found that having a partner during this cybersecurity training helped me learn more effectively compared to doing it alone.

Mark only one oval.

Strongly disagree

1

2

3

4

5

Strongly agree

46. Select the degree of agreement with the statement: *
I believe that collaboration enhances the effectiveness of any type of immersive training compared to individual efforts.

Mark only one oval.

Strongly disagree

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

Strongly agree

47. Select the degree of agreement with the statement: *
I think that users should be using the same type of device in collaborative AR experiences.

Mark only one oval.

Strongly disagree

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

Strongly agree

48. Please provide an explanation to your previous answer.

Questionnaire after Using the Application - Application Details

49. To what extent do you feel that the presence of gamification elements enhanced your learning during the training? *

Mark only one oval.

	Not at all
1	
2	
3	
4	
5	
	Extremely

50. Were the instruction panels of any help while using the application? *

Mark only one oval.

- I did not notice them at all.
- I noticed them, but did not pay attention to them.
- They were an inconvenience/annoying.
- They served as a good guidance.

51. Were the placement guides (the floating chevrons) of any help while using the application? *

Mark only one oval.

- I did not notice them at all.
- I noticed them, but did not pay attention to them.
- They were an inconvenience/annoying.
- They served as a good guidance.

52. Were the objects hints in Scenario 1 of any help while using the application? *

Mark only one oval.

- I did not notice them at all.
- I noticed them, but did not pay attention to them.
- They were an inconvenience/annoying.
- They served as a good guidance.

53. Select the degree of agreement with the statement: *
I would have preferred the application to provide more detailed information about the specific scenarios and their respective contexts.

Mark only one oval.

Strongly disagree

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

Strongly agree

54. Did you manage to crack the password in Scenario 1? *

Mark only one oval.

◯ Yes

◯ No

55. Select the degree of agreement with the statement: *
There was enough time given in Scenario 1.

Mark only one oval.

Strongly disagree

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

Strongly agree

56. To what extent did the utilization of storytelling in Scenario 1 enhance your engagement with the assigned task? *

Mark only one oval.

Not at all

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

Extremely

57. In Scenario 2, I knowingly created a different password than I would have usually. *

Mark only one oval.

◯ Yes

◯ No

58. If yes, what influenced your decision to create a different one than usual?

Tick all that apply.

☐ The presence of another person who was also creating a password.

☐ The first scenario prompted me to create a stronger password compared to my typical choice.

☐ The theme of the application raised my awareness about password generation issues.

59. Did you use reuse or modify a previously used password in Scenario 2? *

Tick all that apply.

- [ ] I reused a password I was already using.
- [ ] I modified a password I was already using.
- [ ] I created an entirely new password, using the same general approach I usually do.
- [ ] I created an entirely new password, and I used a different approach than I normally do.

60. Do you have any comments about the application (strengths, weaknesses, something could have been left out, something was missing, ...)

Questionnaire after Using the Application - Immersive vs Traditional

Immersive experience - VR/AR application

61. Select the degree of agreement with the statement: *
I enjoyed using this application.

Mark only one oval.

Strongly disagree

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

Strongly agree

62. Select the degree of agreement with the statement: *
I enjoyed acquiring cybersecurity knowledge through the use of this application.

Mark only one oval.

Strongly disagree

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

Strongly agree

63. Select the degree of agreement with the statement: *

I would pay more attention to acquiring new skills if they were presented in an immersive manner, similar to this application.

Mark only one oval.

Strongly disagree

1

2

3

4

5

Strongly agree

64. Select the degree of agreement with the statement: *

*I believe that immersive experiences are **a more effective learning method** compared to textbooks, videos, or traditional lectures.*

Mark only one oval.

Strongly disagree

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

Strongly agree

65. Select the degree of agreement with the statement: *

*I think that immersive experiences have the potential to **completely replace** the acquisition of skillsets from textbooks, videos, or traditional lectures.*

Mark only one oval.

Strongly disagree

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

Strongly agree

66. Select the degree of agreement with the statement: *

*I think that immersive experiences can serve as **an extension of/addition to** gaining skillsets from a textbook, video or a traditional lecture.*

Mark only one oval.

Strongly disagree

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

Strongly agree

67. Select the degree of agreement with the statement: *

I would generally like to incorporate the use AR applications in my everyday life.

Mark only one oval.

Strongly disagree

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

Strongly agree

68. Select the degree of agreement with the statement: *
I would generally like to incorporate the use AR applications similar to this one in any type of training.

Mark only one oval.

Strongly disagree

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

Strongly agree

Post-Training Questionnaire

The following 10 questions require you to assess same pairs of passwords as in the pre-training questionnaire and determine their relative security level, or if they are equally secure.

69. Compare the provided security level between these two passwords: *
P1: **PurpleSunset789!**
P2: **Sunshine123!**

Mark only one oval.

◯ P1 is more secure

◯ Both passwords are equally secure

◯ P2 is more secure

70. Compare the provided security level between these two passwords: *
P1: **Password123!**
P2: **987654321!**

Mark only one oval.

- ◯ P1 is more secure
- ◯ Both passwords are equally secure
- ◯ P2 is more secure

71. Compare the provided security level between these two passwords: *
P1: **MySecretWord2023!**
P2: **ABCDEFGH!**

Mark only one oval.

- ◯ P1 is more secure
- ◯ Both passwords are equally secure
- ◯ P2 is more secure

72. Compare the provided security level between these two passwords: *
P1: **TrickyP@ssw0rd!**
P2: **P@ssw0rd123!**

Mark only one oval.

- ◯ P1 is more secure
- ◯ Both passwords are equally secure
- ◯ P2 is more secure

73. Compare the provided security level between these two passwords: *
P1: **PurpleGiraffe876!**
P2: **Password987!**

Mark only one oval.

- P1 is more secure
- Both passwords are equally secure
- P2 is more secure

74. Compare the provided security level between these two passwords: *
P1: **12345678!**
P2: **AbCdEfGhIjKlMnOp!**

Mark only one oval.

- P1 is more secure
- Both passwords are equally secure
- P2 is more secure

75. Compare the provided security level between these two passwords: *
P1: **MyDogSpot#1**
P2: **CorrectHorseBatteryStaple**

Mark only one oval.

- P1 is more secure
- Both passwords are equally secure
- P2 is more secure

76. Compare the provided security level between these two passwords: *
P1: **Qwerty123!**
P2: **ZXCVBNM456!**

Mark only one oval.

- ◯ P1 is more secure
- ◯ Both passwords are equally secure
- ◯ P2 is more secure

77. Compare the provided security level between these two passwords: *
P1: **MyFavoriteColorIsBlue!**
P2: **5tarW@rsFan!**

Mark only one oval.

- ◯ P1 is more secure
- ◯ Both passwords are equally secure
- ◯ P2 is more secure

78. Compare the provided security level between these two passwords: *
P1: **Tr0ub4dor&3!**
P2: **$ecur3P@$$w0rd!**

Mark only one oval.

- ◯ P1 is more secure
- ◯ Both passwords are equally secure
- ◯ P2 is more secure

End of the Questionnaire!

Thank you for participating in the study 😊

Development and Evaluation of an Augmented Reality-Based Application for Collaborative Cybersecurity Training

Abstract

This Master's Thesis introduces *SecuAR Together*, a collaborative cybersecurity training application that leverages augmented reality (AR) technology to provide users with interactive hands-on learning experiences. Through two scenarios, the application focuses on enhancing users' understanding of password management and strong password generation principles. The application is compatible with various AR platforms, such as HoloLens 2 and smartphones, enabling a wide range of users to engage in immersive cybersecurity training. The thesis also presents a user study (N=18) that assessed the impact of *SecuAR Together* on users' password security knowledge and overall user experience. Pairs of participants were exposed to the application, after which their subjective assessments were collected. Pre- and post-training evaluations were conducted to measure the learning outcomes related to password strength. The research findings reveal positive user attitude towards the application, indicating the potential of collaborative AR-based training to improve password security awareness. Participants demonstrate improved knowledge and understanding of password security after using *SecuAR Together*. However, the study acknowledges limitations such as the small sample size and the use of a nonstandardised questionnaire, which may affect the generalisability and reliability of the results. Overall, this research highlights the potential of interactive AR-based training in enhancing cybersecurity awareness, emphasising the need for continued development and evaluation in cybersecurity education.

Keywords: AR, MR, XR, Mixed Reality, Cyber Awareness, Password Security

Razvoj i evaluacija aplikacije za kolaborativni trening u području kibernetičke sigurnosti uporabom tehnologije proširene stvarnosti

Sažetak

Ovaj diplomski rad predstavlja *SecuAR Together*, kolaborativnu aplikaciju za trening o kibernetičkoj sigurnosti koristeći tehnologiju proširene stvarnosti kako bi se korisnicima pružila interaktivna praktična iskustva učenja. Kroz dva scenarija, aplikacija se usredotočuje na poboljšanje korisničkog razumijevanja upravljanja lozinkama i načela generiranja jakih lozinki. Aplikacija je kompatibilna s raznim AR platformama, poput HoloLensa 2 i pametnih telefona, omogućujući širokom rasponu korisnika sudjelovanje u imerzivnom treningu o kibernetičkoj sigurnosti. Rad također predstavlja korisničko istraživanje (N=18) koje procjenjuje utjecaj aplikacije *SecuAR Together* na korisničko znanje o sigurnosti lozinki i cjelokupno korisničko iskustvo. Parovi sudionika bili su izloženi aplikaciji, nakon čega su prikupljene njihove subjektivne procjene. Provedene su evaluacije prije i poslije treninga kako bi se izmjerili ishodi učenja koji se odnose na jačinu lozinki. Rezultati istraživanja otkrivaju pozitivan stav korisnika prema aplikaciji, ukazujući na potencijal kolaborativnog treninga temeljenog na proširenoj stvarnosti za poboljšanje svijesti o sigurnosti lozinki. Sudionici pokazuju poboljšano znanje i razumijevanje sigurnosti lozinki nakon korištenja aplikacije. Međutim, istraživanje osvješćuje ograničenja poput male veličine uzorka i korištenja nestandardiziranog upitnika, što može utjecati na generalizaciju i pouzdanost rezultata. Ovo istraživanje općenito naglašava potencijal interaktivnog treninga temeljenog na proširenoj stvarnosti u jačanju svijesti o kibernetičkoj sigurnosti, naglašavajući potrebu za kontinuiranim razvojem i evaluacijom u obrazovanju o kibernetičkoj sigurnosti.

Ključne riječi: AR, MR, XR, miješana stvarnost, kibernetička svjesnost, sigurnost lozinki