Two-Factor Authentication in VR using Near-Range Extended Reality and Smartphones

by

© Aiur Nanzatov

A Project Report submitted to the

School of Graduate Studies

in partial fulfillment of the

requirements for the degree of

Master of Science

Supervisor: Dr. Oscar Meruvia-Pastor

Department of Computer Science

Memorial University of Newfoundland

May 2025

St. John's Newfoundland

Acknowledgements

I extend my heartfelt gratitude to my supervisor, Dr. Oscar Meruvia-Pastor, for your patience, guidance, and unwavering support. Your extensive knowledge and meticulous editing have greatly benefited my work, and I am deeply thankful that you took me on as a student and continued to believe in me throughout the years.

I also wish to thank, Dr. Lourdes Pena-Castillo, for your encouraging words and thoughtful, detailed feedback, which have been invaluable to my research; for the immense help with the statistical data analysis.

A special thanks to the user study participants who generously dedicated their time to participate in my study, making this project possible.

I am immensely grateful to my family, for your endless support.

Lastly, I am profoundly grateful to Ms. Brianna Rachel McDonald, for the thoughts and ideas provided during the research and for the help you've provided during the development.

Abstract

Modern smartphones have a wide variety of authentication and authorization measures: from drawing a simple pattern to a fingerprint scan system. However, the whole “password” is always contained inside of the device’s memory. In case of information leak the possible malefactor/attacker has access to the whole password, therefore information security is at risk. Enhancing security measures is essential to develop a robust tool that ensures the safety of both head-mounted devices and smartphones. Users wearing headsets are vulnerable to real-world security threats, such as unauthorized individuals attempting to access their personal information or belongings. Furthermore, the necessity of removing the headset to interact with the smartphone can lead to potential security breaches. Thus, it is crucial to address these vulnerabilities to protect users effectively, both in VR and the immediate environment. This thesis proposes a novel approach to two-step authentication by ”splitting” the password authentication process between two independent devices. In this method, one half of the password is displayed on a smartphone screen, while the other half is delivered through a head-mounted device (HMD). This design ensures that only an individual with access to both devices can successfully combine the two halves to form the complete password. The research suggests that this dual-authentication measure could effectively enhance security in systems that utilize both HMDs and smartphones simultaneously.

A prototype was developed and tested, enabling users to interact with their smartphone content in a virtual reality (VR) environment. This system facilitates authentication through various challenges, such as CAPTCHA, numeric passwords, or game-like interfaces, requiring users to input specific passwords. Success in these tasks hinges on the effective communication and combination of inputs from both the HMD and smartphone, making it impossible to bypass the authentication process without both devices.

The findings of this research are supported by two publications detailing the experiments and user studies conducted on the password-splitting method and the integration of smartphone content into the VR setting.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

The origin of augmented reality (AR) and virtual reality (VR) can be traced as far back as 1838, when Charles Wheatstone invented the stereoscope. This technology used an image for each eye to create a 3D image for the viewer [3]. Since then, the technology has evolved at a rapid pace, but has stayed on the fringes of society. However, in the past few years, as graphics and computing technologies have evolved, AR and VR have experienced a renaissance [4, 5]. Nowadays Head-Mounted Devices (HMDs) provide a user with variety of opportunities, ranging from such significant and important matters as surgical operations [6], medicine or teaching [7], to much more entertaining: video games, music, sports or theater [8, 9]. As VR technology becomes more accessible, applications making use of it require an increased level of security. For example, some video games contain in-game purchases, or access to some event in VR might need to ensure the person has identified properly before being allow to take part in the event.

Since any approach to authentication/authorization solution has its own drawbacks and advantages, there is an active discussion of whether some of them are better or worse in terms of efficiency, safety, robustness, simplicity in usage, etc. The objective of this research is to develop a prototype application based on a specific approach: the division of an existing password into two complementary segments. These segments are designed to be disclosed only through human recognition. Even if a machine (decoder) acquires both segments of the code, it will remain unable to decipher the password, as the process requires genuine human cognition to solve the underlying ”riddle.”

Exempli gratia, imagine if the standard CAPTCHA, sometimes described as a reverse Turing test [10], had half of its digital/word/picture code hidden inside of another device, which is not connected to the smartphone and, hence, only the human can juxtapose and compare, which parts of the code fit the correct answer and thereby can pass the authorization. This research posits that satisfactory results can be achieved that are comparable to existing security measures. Furthermore, by considering user studies focused on the effectiveness and comfort of the user experience, the overall utility of this approach can be thoroughly analyzed. Nowadays authentication methods have undergone significant enhancements, reflecting a constant arms race between security developers and cyber attackers [11, 12, 13, 14, 15, 16]. Both hackers and automated security attack systems have made considerable strides, necessitating the continuous development of innovative protection mechanisms[17, 18, 19, 20]. This situation underscores the need for security solutions that are not only robust but also user-friendly. Effective authentication systems must strike a balance between strong protection and ease of use, ensuring a seamless and secure user experience.

As technology advances, safeguarding user access and credentials requires increasingly sophisticated strategies [16, 21]. In the context of online security, two-step authentication has emerged as an efficient and secure way to validate someone's identity [22]. One of the main benefits of two-step authentication is the increased level of security that comes from the fact that part of the information needed to validate the user's identity is sent to an alternative device and so the user must be in possession of two separate devices to authenticate. In the context of utilizing VR headsets, users encounter distinct challenges due to their inability to perceive their real-world surroundings while immersed in the VR environment.

Two-step authentication is difficult in VR because users are usually not able to see their real-world surroundings and, for instance, operate or see their smartphones. This study introduces the use of NRXR for authentication purposes, a technique designed to implement two-step authentication in the context of extended reality systems and smartphones. The proposed method enables users to complete an authentication challenge via their smartphones without removing their HMDs, utilizing Near-Range Extended Reality technology. The term extended reality (XR) is used here as an umbrella term that has emerged in recent years to encompass the general category of Virtual, Augmented, and Mixed Reality systems. Considering that users of Near-Range Extended Reality (NRXR) may alternately experience full VR, Mixed Reality (MR), or Augmented Virtuality (AV) for objects located in close proximity, this technique is designated as Near-Range Extended Reality (NRXR).

1.1 Near-Range Extended Reality and Cyber-Security

With the emergence of the latest generation of Virtual Reality HMDs, including the Meta Quest 3, Varjo XR4, and Apple Vision Pro — each of which supports Mixed Reality and Augmented Reality — a pertinent question arises regarding the methods and implications of integrating the real world with the virtual realm to enhance the user experience in VR [23, 24, 1, 25]. Some MR/AR solutions have emerged recently, such as the use of a "Passthrough" mode in devices such as the Meta Quest 3, and the use of a dial called the "Crown" in the Apple Vision Pro [26, 27]. The Passthrough mode has emerged as a widely recognized technique that enables users to visualize their real-world surroundings when they step beyond the virtual boundaries defined during the HMD setup process. Passthrough functionality is enabled by the integration of video cameras into HMDs. This mode permits users to view their physical environment without the need to remove the HMD [28]. In a similar way, the Crown in the Apple Vision pro is a circular dial on the left side of the HMD, which users can control manually. This functionality assists users in delineating the field of view of the virtual world in relation to the physical environment, effectively framing it as a segment of the users' overall visual field, akin to curtains in a window. Such systems function the same regardless of the characteristics of the physical space or physical objects surrounding the user [29].

Near-range extended reality (NRXR) denotes immersive XR experiences that are intricately connected to the user's physical environment, thereby enhancing the interaction between real and virtual elements at close range [15, 30, 31]. This approach entails the use of depth-sensing front-facing cameras or similar technologies integrated into HMDs, thereby allowing users to perceive nearby objects within the virtual environment [32].

The term "near-range" (NR) is used to describe this technology because it restricts the visibility of real-world objects to those located at close proximity to the camera, while objects positioned at greater distances remain invisible within the XR environment as observed through the HMD. This functionality offers a unique experience in contrast to passthrough or crown technologies, as it effectively creates a defined mixed-reality experience. In the implementation of Near-Range Extended Reality (NRXR), a depth-sensing camera is utilized to facilitate a specific user experience. When the user is not holding any objects within close proximity to the camera, they engage in full virtual reality. In contrast, if physical objects are detected within a range of 1 to 2 meters from the camera, these objects are seamlessly integrated into the virtual environment, thereby creating a mixed-reality (MR) experience.

As the field of contemporary cybersecurity evolves, it is crucial to develop authentication methods that strike a balance between rigorous security protocols and user convenience [33]. This research aims to provide VR users with accessible methods to implement advanced security measures, such as two-step authentication, without requiring the removal of the HMD.

The primary research questions addressed in this study are as follows:

- RQ1: Can near-range extended reality (NRXR) facilitate the authentication of user credentials through two-step authentication?

- RQ2: Which types of authentication challenges are most suitable for implementing two-step authentication in the extended reality (XR) context?

- RQ3: When implementing two-step authentication through Near-Range Extended Reality (NRXR), which approach is more effective for users: presenting a challenge on the smartphone to be answered within the VR environment, or the reverse?

- RQ4: What are users' experiences, impressions, and preferences regarding two-step authentication when utilizing NRXR?

To address these research questions, the overall utility of NRXR was evaluated through a user study.

1.2 Former and recent research in Cybersecurity applications of VR and AR

The accelerating pace of technological advancement continuously presents both opportunities and challenges for the research and education communities. Recently, advancements in HMD technologies for both VR and AR have significantly enhanced the efficacy of these devices while also improving their affordability. Since the early 1990s, higher education has been experimenting with VR, which refers to a computer-generated environment that simulate a realistic experience [34]. Historically, however, these efforts have been focused on large room-scale systems driven by dozens of displays and computers (such as cave automatic virtual environments [35]). Because these efforts were extraordinarily expensive and required experts to operate them, their deployment was primarily limited to large research institutions. AR, which offers a live view of a physical, real-world environment that has computer-augmented elements, has been an area of interest since Harvard's Ivan Sutherland created a rudimentary AR headset in 1968 [36]. AR has been difficult to implement, however, and the required processing power, real-time 3D spatial mapping, and display technology have all been historically insufficient to create high-quality AR experiences. Contemporary HMDs are capable of delivering high-quality immersive experiences. As a result of this paradigm shift, VR and AR are positioned to become integral components of the higher education technology landscape, a trend that is already evident on some campuses [34]. Integrating VR and AR in higher education makes possible many applications. However, their use also raises security issues. Casey et al., for example, have demonstrated a vulnerability that let an attacker trick a VR user into crashing into a wall [37]. In another case, a University of California, Davis, researcher showed that VR tracking sensors can be compromised to allow attackers to peek into the user's physical space[38]. To effectively address both existing and emerging security risks associated with VR and AR, it is imperative for institutions to thoroughly understand these risks and implement fundamental security principles for their mitigation. A significant concern is that many AR and VR devices lack default data encryption and often integrate with third-party applications that may exhibit inadequate security measures. In addition to standard security measures, AR and VR present distinct challenges, particularly regarding physical security and safety. A significant concern with VR is its capacity to completely obscure a user's visual and auditory connection to the external environment. It is essential to prioritize the evaluation of the physical safety and security of the user's environment. This also applies to AR, in which it's important for users to maintain a high degree of situational awareness, particularly in more immersive environments. According to Guzman et al.[1]: "Authentication – Only the legitimate users of the device or service should be allowed to access the device or service. their authenticity should be verified through a feasible authentication method. then, identification or authorization can follow after a successful authentication".

1.3 Two-step authentication background

A significant threat to input protection is the unauthorized and/or unintended disclosure of information, whether it involves the actual data itself or the way the data is transmitted or transferred. Vulnerable inputs can be grouped into two types based on whether the user intends them: a) targeted physical objects, and b) unintended inputs, such as typing mistakes. Both types usually come from the surrounding environment and are mainly used for visual enhancement or context. We call these ’passive’ inputs. On the other hand, inputs that users intentionally provide, like gestures, are known as ’active’ inputs.

Apart from threats to confidentiality (i.e., information disclosure), the two other main threats related to inputs are detectability and user unawareness of the content. Detectability refers to the ability of a system or security mechanism to identify and respond to potential threats or unauthorized activities [39]. This concept encompasses various detection methods, including intrusion detection systems, monitoring tools, and anomaly detection algorithms. High detectability means that a security system can effectively recognize and alert administrators to malicious actions or breaches, thereby enabling timely intervention. User content unawareness in the context of cybersecurity refers to the lack of knowledge or consciousness that users have regarding the risks and threats associated with the digital content they encounter [40, 41]. This unawareness can manifest in several ways:

- **Inability to Identify Threats**: Users may not recognize phishing emails, malicious links, or fraudulent websites, making them susceptible to attacks.

- **Overconfidence in Security**: Some users may believe that common sense is sufficient for identifying safe content, leading to complacency and risky behavior.
- **Insufficient Training**: A lack of education or training on cybersecurity best practices can leave users ill-equipped to discern safe content from harmful content.
- **Information Overload**: The sheer volume of information available online can overwhelm users, causing them to skim content without fully understanding potential risks.
- **Social Engineering Vulnerabilities**: Attackers often exploit psychological factors, such as trust or urgency, leading users to engage with harmful content without critical evaluation.
- **Neglecting Security Features**: Users may overlook security features, like checking for HTTPS in web addresses, which can further expose them to risks.
- **Cognitive Biases**: Various cognitive biases can influence user behavior, leading to misjudgments about the safety of content.
- **Lack of Awareness of Privacy Settings**: Users might not fully understand or utilize privacy settings on social media or other platforms, exposing themselves to unwanted risks.

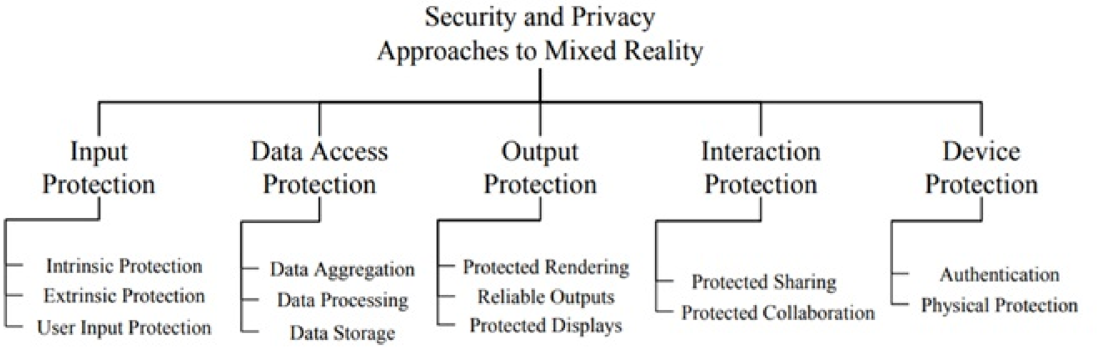


Figure 1.1: General approaches in VR/AR application to Security and Privacy by De Guzman et al. [1]

Addressing user content unawareness involves comprehensive education and training programs, regular updates on evolving threats, and promoting a culture of cybersecurity mindfulness.

1.4 Research questions

During the phases of research planning and system design, several essential questions arised that warranted consideration. In particular, this research aims at addressing the following research questions:

1. Q: Is it possible to provide a technique for authentication in AR/VR which can make a notable contribution in the cybersecurity with AR usage?

   It is posited that, given the limited research on authentication measures within AR and VR, the approach of splitting a password into two segments—one residing in the real world and the other in the virtual realm—may be a viable avenue for further development. This strategy has the potential to act as a catalyst for subsequent advancements at the intersection of these two significant fields.

2. Q: How to address the human factors involved, e.g. people tend to forget their passwords if they are too complex, or strive to choose the simplest route, setting overly primitive passwords? What if the degree of sophistication of a proposed solution will turn out too simple/too complex? How significantly growth of complexity may affect the overall performance of the system, if users are asked to do multiple iterations while creating or entering their passwords?

   It is acknowledged that the distinction between the two extremes is relatively tenuous; therefore, it is essential to ensure that the system maintains a fair balance between sophistication and simplicity. User feedback must be considered, and a dynamic improvement plan should be developed. There is an inherent trade-off: one may either compromise the security of the system to enhance usability and reduce complexity, or conversely, increase security at the expense of user comfort. Identifying this balance is a fundamental aspect of this research.

3. Q: How to navigate the system without a lot of effort or struggling with system interaction?

   Because the keyboard and mouse are absent in VR systems, and there are also gesture detection inaccuracies, handy and convenient user experience solutions must be provided. Turning a smartphone into a navigation device allows for both removing the need of an actual VR controller and addition of another measure to obtain and operate the information within VR.

In light of the research questions outlined above and following a comprehensive literature review of existing authentication methods, it was determined that an authentication system would be implemented to enable users to interact with the VR environment using their smartphones, without the necessity of removing the headset or diverting attention from the virtual scene. To enhance security, the password was divided into two segments: one segment was embedded within the VR environment, while the other was transmitted to the smartphone. Consequently, a robust system featuring a user-friendly interface was developed. Subsequently, a user study was conducted to compare various authentication methods and to analyze the capabilities of the designed system.

Chapter 2

Literature review and related work

Recent research has investigated the application of traditional password-based authentication methods within VR and AR environments [42, 43]. The process of entering passwords in these immersive settings has been found to be cumbersome and detrimental to the overall user experience [44, 16]. The challenges associated with password entry underscore the necessity for exploring more intuitive solutions that integrate seamlessly with the immersive environment. Potential alternatives include virtual or touch-sensitive physical keyboards, which offer a promising method for text entry in VR environments [45].

In immersive VR environments utilizing HMDs, physical keyboards have proven effective for text entry [46]. However, traditional physical keyboards necessitate external camera-based tracking systems to operate efficiently within VR. Menzner proposes the use of touch-sensitive physical keyboards, which incorporate sensing capabilities directly into the keyboard's surface [45]. This approach involves tracking users' fingertips directly on the keyboard, potentially enhancing the VR text entry experience by making it more intuitive and accessible.

Biometric authentication offers a viable alternative in VR environments, where traditional methods like PINs and passwords are less effective. A study by Heruatmadja highlights the challenges of VR security and reviews biometric techniques, emphasizing the use of machine learning methods such as k-Nearest Neighbors (k-NN) and Support Vector Machines (SVM) [47]. It finds that finger vein and hand movement biometrics are particularly accurate for identification in VR settings, aiming to improve future VR authentication systems.

Behavioral biometrics provide a non-intrusive method of user authentication based on unique behavioral patterns rather than physical characteristics. This approach focuses on how users interact with devices, capturing distinct behavior patterns for identification and verification. For example, utilization of hand tracking data from AR/VR interactions to identify users based on their unique finger movements and gestures. A study by Liebers et al. demonstrates the effectiveness of using hand tracking for implicit user identification in immersive environments [48].

2.1 Existing methods in VR/AR authentication and attempts at Near-range extended reality

With the growing adoption of VR and AR technologies across various domains such as gaming, healthcare, and education, ensuring secure user authentication has become increasingly critical. VR and AR environments present unique challenges, including the need for seamless interaction and minimal disruption to the immersive experience.

2.1.1 Recent authentication methods

2.1.1.1 Password-Based Authentication

Recent studies have explored the use of traditional password-based methods in VR/AR environments. However, entering passwords in these immersive settings can be cumbersome and counterproductive to the user experience. The difficulties users face when entering their passwords show the need of investigation on more intuitive solutions that blend seamlessly with the immersive environment, e.g. virtual keyboard or touch-sensitive physical keyboards. The latter are an alternative method for text entry in virtual reality environments. In immersive VR environments using HMDs, physical keyboards are effective for typing. However, traditional physical keyboards require external camera-based tracking systems to function effectively in VR. The paper by Menzner suggests leveraging touch-sensitive physical keyboards, which integrate sensing capabilities directly into the keyboard's surface [45]. Such approach consists of tracking users' fingertips directly through the keyboard, potentially improving the VR text entry experience by making it more intuitive and accessible.

2.1.1.2 Biometric Authentication

An alternative method for authentication in VR environments involves the use of biometrics. A study conducted by Heruatmadja et al. examines the unique challenges and security concerns associated with VR, indicating that traditional authentication methods, such as PINs and passwords, are often ineffective in this context [47]. The study evaluates various biometric modalities and technologies employed for authentication, with a particular emphasis on machine learning techniques like k-Nearest Neighbors (k-NN) and Support Vector Machines (SVM). The findings suggest that biometric methods utilizing finger vein patterns and hand movements are among the most accurate for individual identification in VR settings. This research aims to inform future studies and enhance VR authentication systems by offering insights into effective biometric techniques and their accuracy. In addition to finger and hand biometrics, facial recognition is also being investigated as a potential method for biometric authentication. Ortmann et al. [49] addresses a critical gap in VR technology: the accurate detection of emotions through facial expression recognition (FER), despite the obstructive nature of HMDs. By employing advanced architectures for FER and incorporating them into a novel affective game, the study presents a practical and innovative approach for assessing and demonstrating the effectiveness of these models.

EmojiRain, the affective game, is a creative way to assess FER models and engage users in a meaningful context [49]. This approach provides a tangible application of the technology and can offer valuable insights into real-world effectiveness. However, ensuring that FER models can accurately recognize facial expressions despite the occlusion caused by HMDs may be challenging and will require rigorous testing and refinement. Consequently, while facial expression recognition (FER) was considered a viable biometric authentication measure in this thesis, it necessitates specialized devices for effective implementation, which conflicts with the desired simplicity of the approach. Additionally, biometric authentication is highly specific and demands complex pre-configuration of individual users' biometric parameters, making it less compatible with the concept of splitting the password.

2.1.2 Behavioral Biometrics

Behavioral biometrics provide a non-intrusive method for user authentication. This approach involves identifying and verifying individuals based on their behavioral patterns rather than their physical traits. Such biometric systems concentrate on the manner in which users interact with devices or systems, capturing distinctive patterns in their behavior that can be utilized for authentication and identification purposes.

1. Interaction Based: unlike traditional biometrics that rely on physical attributes (like fingerprints or iris patterns), behavioral biometrics examines how individuals perform specific tasks or interactions. This includes typing patterns, mouse

movements, or gestures [50].

2. Dynamic and Adaptive: Behavioral biometrics can adapt over time as individuals' behavior changes, providing continuous authentication rather than a one-time verification. This makes it suitable for scenarios where users frequently interact with systems [51, 52].

3. Non-Intrusive: These systems are generally non-intrusive because they monitor and analyze behavior that users naturally exhibit during regular use, without requiring additional steps or hardware [53, 54].

4. Behavioral Patterns: The system identifies individuals based on distinctive behavioral traits, such as:

   Typing Dynamics: Speed and rhythm of typing [55].

   Mouse Movements: Patterns and trajectories of mouse use [56].

   Gestures: Specific hand movements or gestures made during interactions [57].

5. Security and Personalization: behavioral biometrics enhance security by continuously verifying users based on their unique behavior. It also enables personalized experiences by tailoring system responses based on individual interaction patterns [58].

For instance, in the study conducted by Liebers et al. [48], behavioral biometrics are employed through the analysis of hand tracking data from AR and VR interactions to identify users. This approach involves examining how individuals engage with virtual buttons, sliders, and other interface elements, allowing for differentiation based on their unique finger movements and gestures. The research underscores the feasibility and effectiveness of utilizing hand tracking data for implicit user identification in AR/VR environments. Another viable approach to enhancing authentication in VR environments involves leveraging decentralized technologies and self-sovereign identity (SSI) [59]. Research on SSI addresses the vulnerabilities inherent in current authentication methods, such as predictable passwords and the risk of biometric data theft, by proposing a decentralized solution that integrates user memories. This method employs SSI as a decentralized framework that empowers users to retain control over their own identity information. In contrast to traditional centralized systems, this approach mitigates the risks associated with data breaches and centralized data storage. An additional layer of security is introduced through the incorporation of users' memories into the authentication process. This entails the creation and storage of scenes that users can recall, which are then utilized to generate immutable and unpredictable secret information. These scenes are stored on the InterPlanetary File System (IPFS), a decentralized file storage solution, while the associated links to these scenes are recorded on the blockchain, ensuring both the immutability and traceability of the authentication data. By integrating SSI, memory-based authentication, IPFS, and blockchain technology, this system presents significant advantages in terms of security and user control. However, successful implementation will require addressing challenges related to memory recall, technical integration, scalability, and user acceptance.

2.1.3 Context-Aware Authentication

Context-aware authentication is a security approach that enhances user verification by taking into account the context in which authentication occurs. Unlike traditional methods that rely solely on static credentials, such as passwords or PINs, context-aware authentication incorporates a range of contextual factors to assess and validate user identity. This method seeks to improve security by dynamically adjusting authentication requirements based on the specific situational context. One innovative approach to context-aware authentication in VR involves the use of virtual agents (VAs) as interactive partners [44]. Rather than relying on traditional methods such as text input or two-factor authentication—which can disrupt the immersive nature of VR—the proposed system enables users to authenticate through a series of ten gestures, including high fives and fist bumps. Users can personalize their authentication sequences by combining these gestures, thereby enhancing security while preserving immersion. This method effectively addresses the limitations of conventional authentication techniques in VR, which are often cumbersome and can interrupt the immersive experience. By employing natural gestures with virtual agents, the system aligns seamlessly with the VR environment, offering a more intuitive authentication process. It maintains the immersive quality of VR by integrating authentication into virtual interactions, eliminating the need for users to remove their headsets or disengage from the VR experience. The inclusion of a diverse range of gestures, such as high fives and fist bumps, provides flexibility and can be tailored to individual preferences, potentially improving user satisfaction and ease of use. However, the effectiveness of gesture-based authentication in practice may be influenced by factors such as the accuracy of gesture recognition, user variability, and the complexity of the gesture combinations. By leveraging virtual agents and natural gestures, this approach aims to enhance both security and the overall user experience. Another study introduces a novel authentication method for virtual reality known as Direction-Based Authentication (DBA) [60]. This technique requires users to navigate through four distinct virtual environments, selecting a direction within each environment to construct a password. Users have the option to choose directions by either physically turning or utilizing a panel-controlled snap-turning mechanism. The DBA method seeks to strike a balance between memorability, efficiency, and security. Its security relies on the complexity and uniqueness of the directional sequences. While this approach may lower the risk of password guessing compared to conventional text-based passwords, its effectiveness against potential threats, such as observation or pattern recognition attacks, requires further validation.

Additionally, a context-aware authentication approach called SPHinX is specifically designed for immersive VR and extended reality (XR) environments. SPHinX employs a three-dimensional technique, allowing users to authenticate by painting or tracing patterns on a 3D object [61]. This method aims to enhance security by utilizing 3D interactions, thereby potentially reducing vulnerabilities such as shoulder surfing. By incorporating 3D objects into the authentication process, SPHinX seeks to address common security issues associated with two-dimensional schemes. The use of spatial patterns introduces an additional layer of complexity that complicates unauthorized access. By enabling users to paint or trace patterns on a 3D object, this method capitalizes on the spatial capabilities of VR, offering an innovative way to create and utilize authentication credentials. Lastly, a visual cryptograpy to decode messages sent from the machine for human observers to perceive [62]. The study provides valuable insights into the intersection of cryptography and augmented reality, highlighting both the potential for secure communication and the challenges related to user vigilance. All these approaches aim to integrate authentication seamlessly into the VR experience while addressing security concerns.

2.2 Near-Range eXtended Reality

Near-range eXtended Reality (NRXR) refers to immersive VR experiences that are closely integrated with the user's physical environment but extend beyond it through virtual elements. This concept focuses on creating a seamless blend of the real and virtual worlds, particularly in environments where the user is physically present and interacting with their immediate surroundings.

2.2.1 Key Characteristics:

1. Proximity to Physical Environment: Near-range extended reality operates within a short distance from the user's physical space. Unlike large-scale VR systems that might involve entire rooms or spaces, near-range systems are designed for arm-length interactions and are appropriate for use in smaller, more confined areas, within two to three meters, such as an office or a living room.

2. Integration of Real and Virtual Elements: The system integrates virtual objects and interactions with the real environment, enhancing the user's experience by allowing virtual elements to interact with or overlay on their physical surroundings. This integration is often achieved through technologies like AR, mixed reality (MR), or spatial computing.

3. User Interaction: Users interact with both physical and virtual objects. For example, they might use physical controllers or gesture-based inputs to manipulate virtual elements that appear to interact with real-world objects or environments.

4. Applications:

   Training and Simulation: Used for hands-on training simulations where users can practice skills in a virtual environment that closely mimics their real-world workspace.

   Design and Visualization: Helps designers and architects visualize and manipulate 3D models in the context of real-world objects, aiding in the design and planning process.

Entertainment and Gaming: Provides immersive gaming experiences where virtual objects interact with physical elements, enhancing realism and engagement.

Education and Learning: Facilitates interactive learning experiences by overlaying educational content onto real-world objects or environments.

2.2.2 Technologies Involved

1. AR: AR overlays digital information onto the user's view of the real world. Near-range extended reality often uses AR to display virtual objects or data in close proximity to the user's physical space.

2. Mixed Reality (MR):

   MR blends real and virtual worlds, allowing virtual objects to interact with physical objects in real-time. MR systems are used to create more immersive and interactive experiences by seamlessly integrating virtual elements into the user's near-range environment.

3. Spatial Computing:

   Spatial computing involves using sensors and advanced algorithms to understand and interact with the physical space around the user. This technology enables accurate placement and interaction of virtual objects within the user's near-range environment.

4. Head-Mounted Displays:

   HMDs are used to present virtual content while maintaining awareness of the physical environment. Some HMDs are equipped with cameras or sensors that allow users to see and interact with both real and virtual elements.

2.2.3 Advantages and Challenges

1. **Advantages**:

   Enhanced Interaction: By combining real and virtual elements, users can interact with virtual objects as if they were part of their physical environment, creating more engaging and realistic experiences.

   Improved Context Awareness: Near-range extended reality allows users to maintain awareness of their physical surroundings while interacting with virtual content, reducing the risk of disorientation or accidents.

   Flexible Use Cases: This approach can be adapted to various applications, from professional training and design to entertainment and education, providing versatile solutions for different needs.

2. **Challenges**:

Complexity of Integration: Combining virtual and real elements seamlessly requires sophisticated technology and precise calibration to ensure accurate interactions and prevent issues such as latency or misalignment.

Hardware Limitations: Near-range extended reality depends on the capabilities of hardware such as sensors, HMDs, and AR/MR devices. Limitations in these technologies can impact the quality and effectiveness of the virtual experience.

User Experience: Designing intuitive and comfortable interactions in near-range environments can be challenging, especially when balancing the immersion of virtual elements with the need for users to remain aware of their physical space.

2.2.4 Using Smartphones in VR

Numerous research initiatives have concentrated on the integration of smartphones and various input devices within virtual, augmented, and mixed reality environments. Specifically, studies have explored the roles of handheld controllers, smartwatches, and smartphones as vital tools for user interaction in these immersive contexts [63, 64, 65, 66, 67, 68, 69].

One notable contribution is presented by Pietroszek et al. [70], which proposes the utilization of smartphones as input devices for engaging with displays, thus circumventing the necessity for expensive tracking equipment. This approach is particularly advantageous in settings where cost-effectiveness is paramount. Furthermore, another research [71] introduces innovative methodologies that facilitate diverse interaction modalities using mobile devices within VR. In addition to smartphones, other handheld displays (HHDs), such as touchpads, have also been identified as effective means for interaction in VR environments [72].

In a complementary study [73], the authors advocate for the use of smartphones to conduct selection tasks and facilitate teleport-based navigation in virtual reality. The findings indicate that this smartphone-based approach offers a level of performance comparable to that achieved with conventional VR controllers. Additionally, the concept of Augmented Virtuality is being explored [68], which serves as a mechanism for smartphone access. The authors emphasize the significance of incorporating users' hands into the operational framework, providing evidence that the realistic rendering of skin tones representing users' hands enhances the overall user experience.

The NRXR framework inherently integrates these two advantageous aspects. In a related area of research, a study [74] examines the optimal strategies for spatially anchoring smartphones within virtual reality environments. The study posits that having users physically hold their smartphones and engage in direct touch interactions can significantly improve both the accuracy and speed of their actions. This principle resonates closely with the methodology employed in the current paper, which seeks to facilitate user access to their smartphones in a manner that aligns with these findings.

Overall, the integration of smartphones and other handheld devices into virtual and augmented reality contexts represents a promising avenue for enhancing user interaction. As these studies illustrate, the potential for improved accessibility, cost-effectiveness, and user engagement is substantial, warranting further exploration and development in this evolving field.

2.2.5 Summary

Near-range extended reality (XR) represents a dynamic and rapidly evolving field that seamlessly integrates virtual and real-world interactions within close physical proximity. This innovative domain leverages advanced technologies such as augmented reality (AR), mixed reality (MR), and spatial computing to create immersive experiences that significantly enhance user engagement and interaction. For instance, applications in education can allow students to visualize complex concepts in real-time, while in retail, customers can virtually try on products before making a purchase, fostering a more interactive shopping experience.

However, despite its promising benefits, the near-range XR approach encounters several challenges that must be navigated to unlock its full potential across various applications. One major hurdle is technology integration; developing systems that can effectively merge digital content with the physical environment requires sophisticated software and hardware solutions. Additionally, current hardware limitations, such as battery life, processing power, and the form factor of XR devices, can hinder widespread adoption and usability. Finally, user experience remains a critical concern, as intuitive design and accessibility are essential for encouraging widespread engagement. Addressing these challenges is vital for realizing the transformative possibilities of near-range XR in sectors such as education, healthcare, gaming, and beyond, ultimately shaping a future where digital and physical worlds coexist harmoniously.

Chapter 3

Methodology

To achieve a comprehensive understanding of the proposed system's limitations, advantages, and drawbacks, it is essential to explore various forms of two-step authentication in VR. Two-step authentication serves as a critical component in enhancing security, particularly within immersive environments where traditional authentication methods may prove less effective. Given the evolving nature of VR technology and its applications, understanding the impact of different authentication strategies on user experience and security is paramount.

While the potential methods for implementing two-step authentication are extensive, encompassing a wide range of user interactions and device integrations, this initial investigation has been intentionally limited to four specific types of challenges. This decision is grounded in practical considerations, including the need to maintain a manageable scope for the study and to ensure that the selected challenges represent

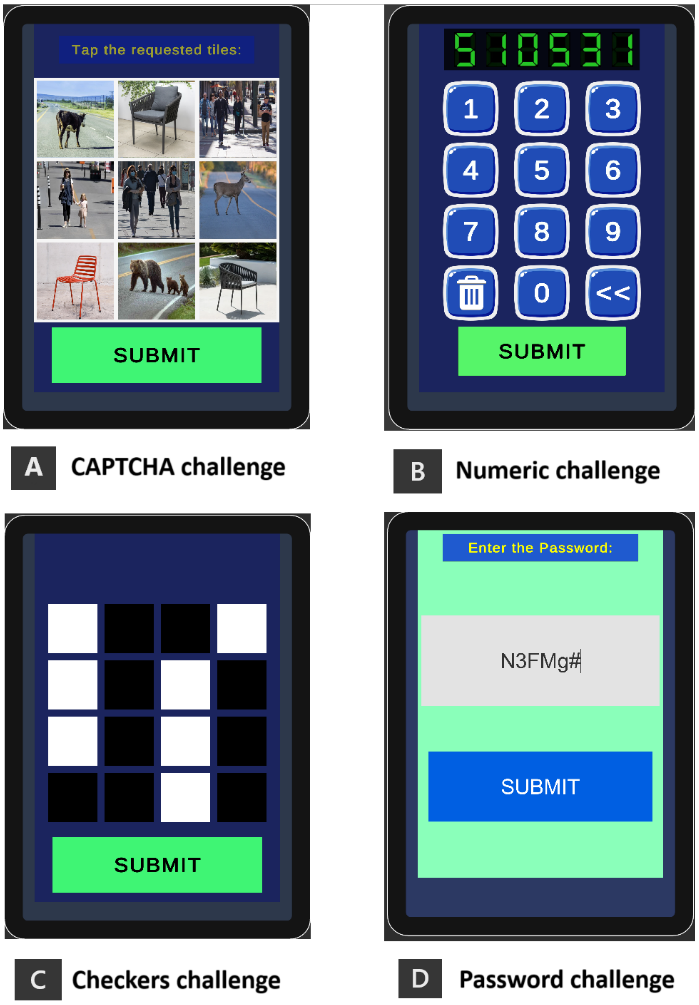


Figure 3.1: Overview of authentication challenges presented during experimental validation. A) CAPTCHA-style authentication, where participants select tiles corresponding to a request sent via a different device (HMD/PC). B) Numeric authentication, requiring users to enter a six-digit code. C) Checkers authentication, involving the visual matching of two checkered grids. D) Keyboard-based authentication, where participants input a six-character alphanumeric password.

a diverse array of authentication methods.

The four challenges chosen for this exploration are designed to encompass different modalities and levels of user engagement. By concentrating on these specific types, the study aims to draw meaningful comparisons that highlight the strengths and weaknesses of each approach.

A user study has been conducted to systematically compare these four two-step authentication strategies, assessing both their efficiency and user satisfaction. Efficiency metrics include the time taken to complete authentication and the error rates associated with each method, while user satisfaction is gauged through subjective feedback regarding ease of use, perceived security, and overall experience.

Given the wide array of potential approaches to addressing the authentication problem in VR, the study has opted to concentrate on four specific methods of authentication. This decision is driven by the need to balance variety and practicality while ensuring that the selected methods reflect both established and innovative techniques relevant to the context of VR.

The first method involves solving a CAPTCHA-style challenge. This approach is intuitive and widely recognized as an effective human verification technique. CAPTCHAs serve not only to distinguish between human users and automated systems but also to engage users in a straightforward manner, making them suitable for a range of applications.

The second method consists of entering a numeric code, which is the most prevalent form of two-step authentication. This approach is familiar to users and provides a straightforward means of enhancing security by requiring an additional piece of information beyond a password. Its ubiquity in various online services underscores its effectiveness and user acceptance.

The third method features a checkers-style matching challenge, which involves visually matching patterns. This type of task is particularly well-suited for graphical interfaces and leverages users' visual recognition skills, offering an engaging way to verify identity. The use of visual tasks can also reduce cognitive load compared to purely text-based inputs.

Finally, the fourth method incorporates the provision of an alphanumeric password via a virtual keyboard. This choice reflects the natural usage patterns of different types of keyboards that users encounter in their daily lives. With the widespread adoption of smartphones, tablets, and laptops, users are increasingly familiar with various keyboard layouts, including QWERTY and virtual keyboards. This familiarity facilitates a smoother and more intuitive input process within a VR environment.

Moreover, the integration of a virtual keyboard allows for greater flexibility in input methods. Users can interact with the keyboard using hand gestures, controllers, or even gaze-based selections, which enhances accessibility and usability. This adaptability is crucial in immersive environments, where traditional input methods may not be practical or effective.

Figure 3.1 illustrates these four distinct forms of authentication, each selected for its unique strengths and relevance to the study's objectives. The subsequent section will provide a detailed description of each method, exploring their mechanisms, user interactions, and implications for overall security and user experience in virtual reality environments. This focused examination will enable a deeper understanding of how different authentication strategies perform under the specific conditions of VR, ultimately contributing to the development of more effective security solutions.

3.1 Overview of the Authentication Challenges

3.1.1 CAPTCHA-style challenge

In the CAPTCHA-like challenge, users are presented with a 3x3 grid of images and are required to select three objects that correspond to a request provided at the outset of the challenge. The key aspect of this authentication method is that only the challenge creator possesses knowledge of which specific elements on the grid meet the criteria outlined in the initial request. Consequently, the challenge creator can communicate a general description of the icons that fulfill the requirements to one device, while simultaneously sending the challenge grid to a second device used for the authentication process.

For instance, a typical scenario may involve the user being instructed to identify all images that contain animals. In this case, the user receives the description on one device and views a grid containing both animal images and other unrelated content on the second device. This dual-device approach enhances security by ensuring that the user must engage with both devices to complete the challenge successfully.

The structure of this challenge necessitates that users navigate through two rounds of CAPTCHA tasks, culminating in a minimum of six clicks to resolve the challenge. This interaction not only serves as a method for verifying user identity but also adds a layer of complexity to the authentication process, effectively mitigating the risk of automated attacks.

Moreover, the design of this CAPTCHA-like challenge is intentional, as it leverages users' cognitive and visual processing abilities. By requiring users to discern specific categories of images based on descriptive criteria, the challenge capitalizes on natural human skills in pattern recognition and categorization. This engagement can also lead to higher user satisfaction when compared to more traditional authentication methods, as the visual nature of the task aligns with familiar interactions that users often encounter in everyday scenarios.

Overall, this authentication method not only emphasizes security through a two-device approach but also incorporates an engaging and intuitive user experience. By understanding and utilizing the cognitive strengths of users, the CAPTCHA-like challenge presents a promising avenue for enhancing security in virtual environments while maintaining user engagement.

3.1.2 Numeric code challenge

One of the most prevalent methods of two-step authentication involves the transmission of a six-digit numerical code to the user's smartphone. Typically, this code is delivered via text message, allowing users to receive it directly on their mobile devices. Upon receipt, users enter the code into a second device to complete the authentication process. This technique has gained widespread adoption across various sectors, including banking, email services, and numerous online platforms, due to its effectiveness in enhancing security by providing an additional layer of verification.

In this implementation, the researchers adopt this widely recognized approach within the context of a custom application. Specifically, the system simulates the reception of the numerical code on one device while requiring users to input the code on a second device, mirroring the conventional process familiar to users.

The rationale for employing a numerical code as an authentication mechanism is grounded in its balance between security and user convenience. The six-digit code is straightforward enough for users to remember and enter quickly while being sufficiently complex to deter unauthorized access. Additionally, the dual-device interaction enhances security by ensuring that the code must be accessed on a personal device, thereby reducing the risk of interception.

3.1.3 Checkers matching challenge

The checkers-style visual matching challenge was designed as a visual authentication method tailored for graphical interfaces. In this challenge, users are presented with a 4x4 grid of checkered tiles on one device and a corresponding 4x4 grid on a second device. The task requires users to flip each tile between black and white states through tapping or selection until the tile arrangement on the second device matches that of the first device. Notably, there are only six differences between the two grids, allowing users to solve the challenge with a minimum of six flips.

A key advantage of this challenge lies in the clear distinction of the tiles, which can be easily identified as being in either an "on" or "off" state. This contrasts with the more complex images used in the CAPTCHA-style challenge, where users must interpret the contents of each image within the grid. The straightforward nature of the checkered tiles facilitates quicker comprehension and interaction, ultimately enhancing the user experience during the authentication process.

Additionally, the tiles can be efficiently encoded as a binary string, enabling seamless conversion between visual representations and data. This encoding allows for the rapid validation of user actions upon submission of their response, contributing to the system's overall efficiency and user-friendliness. In summary, the checkers-style visual matching challenge presents a compelling alternative to traditional authentication methods, utilizing visual simplicity and binary encoding to improve both security and user engagement in the authentication process.

3.1.4 Alphanumeric Password challenge

Alphanumeric passwords serve as a fundamental method of authentication for users accessing online systems, as highlighted by Schneegass [75]. In this challenge, several established guidelines for creating robust passwords have been maintained, including the use of both uppercase and lowercase letters, as well as a combination of numbers, letters, and special characters.

To ensure that this challenge remains comparable to the other authentication strategies employed in the study, a restriction was implemented that limits the password length to a maximum of 6 characters. This decision, while deviating from the common practice of requiring a minimum password length of 8 characters, was made to align the number of required user interactions with the other three challenges, each of which necessitates a similar level of engagement. The choice of a 6-character limit strikes a balance between ensuring some degree of security and maintaining user convenience, allowing for quicker input while still requiring thoughtful selection of characters.

However, it is important to note that this limitation introduces an additional layer of complexity, as users must switch between different character sets on the virtual keyboards during the input process. This switching can increase cognitive load, as users must remember which characters are available in each set (e.g., uppercase letters, lowercase letters, numbers, and special characters). Consequently, this added complexity may impact user efficiency and satisfaction, as users may face challenges in quickly finding and entering the desired characters.

Furthermore, the restriction to 6 characters serves to illustrate the trade-offs often faced in authentication design: while shorter passwords may be easier to enter, they may also be less secure. The implementation of this challenge thus encourages users to think strategically about their password choices within the constraints provided, fostering an awareness of the balance between security and usability. By incorporating these considerations, the alphanumeric password challenge aims to provide a comprehensive evaluation of various authentication strategies, contributing to a deeper understanding of user interactions and preferences in digital environments.

3.2 Interaction modalities of two-step authentication in VR

In the NRXR framework, the HMD can function as either the first or second device in a two-step authentication process, while the smartphone remains visible to users, serving as the complementary authentication device. This versatility allows for a seamless integration of both devices in the authentication workflow.

In this context, the study has explored three distinct interaction modalities, henceforth referred to as experimental conditions. Each condition is designed to investigate the effectiveness and usability of different configurations of device interactions during the authentication process. By examining these modalities, the research aims to iden-

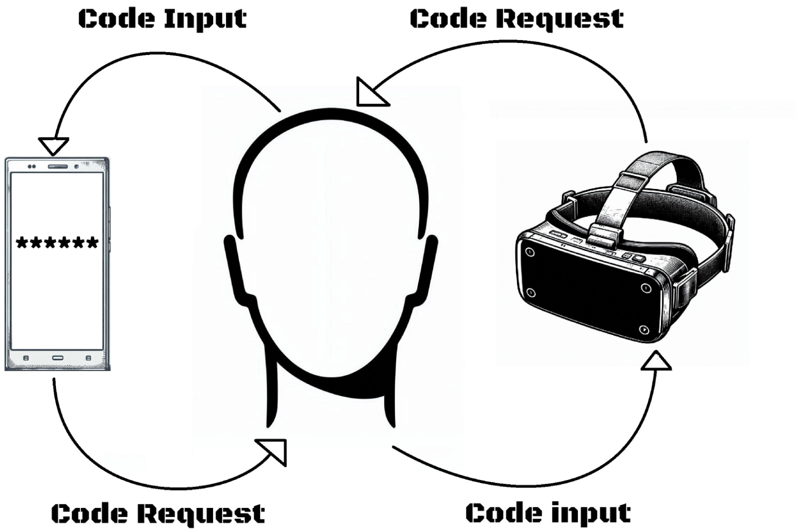


Figure 3.2: Representation of an experimental setup with a phone-HMD code request and input, two-ways: HMD-to-Phone; Phone-to-HMD. *Image partially produced by DeepAI Image generator[2]*

tify optimal ways to facilitate user interactions, improve security, and enhance overall satisfaction with the authentication experience. Figure 3.2 illustrates the two-way interaction involving the HMD), the smartphone, and a human operator. In different scenarios, the request for the code may be initiated by either the HMD or the smartphone, while the second device is used for the code input.

The exploration of these experimental conditions is crucial, as it allows for a comprehensive assessment of how varying configurations can impact user performance and perceptions. By leveraging the strengths of both the HMD and the smartphone, the study seeks to contribute valuable insights into the design of more effective two-step authentication systems that are both secure and user-friendly. Ultimately, this investigation aims to inform future developments in authentication technology, ensuring that user needs and preferences are central to the design process.

3.2.1 Condition 1: HMD1_Phone2

In this condition, shortly called as HMD1_Phone2, the HMD functions as the primary device for the authentication challenge, wherein it presents users with the task to be completed (step 1). Meanwhile, the smartphone acts as the secondary device, enabling users to enter and submit their solutions to the challenge (step 2). This configuration underscores the dual-device interaction that characterizes the authentication process, allowing for a seamless transition between visual engagement in the VR environment and input on a separate device.

Figure 3.4 provides a visual representation of how challenges are communicated to participants within the VR setting. It illustrates not only the presentation of the authentication tasks but also how users perceive their smartphones while immersed in the HMD. This dual focus is critical, as it highlights the necessity of maintaining user awareness of both devices during the authentication process, ensuring that participants can effectively navigate the challenges presented to them.

Figure 3.1 further elaborates on this interaction by displaying the smartphone app screens associated with each type of challenge. This visual documentation offers insight into the design and functionality of the app, which is integral to the user's ability to complete the authentication process efficiently. Moreover, the inclusion of

Figure 3.10B, which depicts the smartphone's virtual keyboard used for responding to the password challenge, illustrates the mechanics of input within the authentication framework.

By integrating these visual elements, the study aims to provide a comprehensive understanding of how the HMD and smartphone collaboratively function in the authentication process. This exploration is essential not only for evaluating the efficacy of the authentication methods employed but also for identifying potential areas for improvement in user experience. Ultimately, the dual-device approach presents an innovative strategy for enhancing security measures while accommodating user interaction preferences in digital environments.

3.2.2 Condition 2: Phone1_SVRP2

In this scenario, called Phone1_SVRP2, the smartphone serves as the primary device for authentication, presenting the user with the challenge to be solved (Phone1, step 1 or Phone1, as illustrated in Figure 3.3, left panel). The HMD functions as the secondary device, where users enter and submit their solutions to the challenge (step 2, depicted in Figure 3.5), where SVRP2 stands for SmartVR Pointer (SVRP) being the secondary device and is used to provide the answer in the VR (SVRP2). The SmartVR Pointer technique uses raycasting mechanism for the pointer withing the VR to follow the user's head movement, making it easier to interact with the environment [73]. This configuration highlights the versatility of using multiple devices in the authentication process, enhancing user engagement and interaction.

Given that the challenges can be resolved within the VR environment using various input devices, users require an effective selection mechanism to interact with the challenges. This includes selecting tiles from grids and choosing digits or characters from virtual keyboards displayed within the HMD. To facilitate this interaction, a virtual keyboard is provided to users within the VR environment (as shown in Figure 3.7).

To enable users to submit their responses while wearing the HMD, the SmartVR Pointer Gaze-based selection (SVRP2) method is employed. This approach allows for selection within the VR environment by utilizing the smartphone, as documented in prior research [73]. The decision to implement this method is particularly advantageous, as users are already holding their smartphones, which can be utilized not only to receive the authentication challenge but also to provide responses.

By leveraging the smartphone's capabilities in conjunction with the immersive experience of the HMD, the study aims to create a more cohesive and efficient authentication framework that aligns with users' natural interactions in digital environments.

3.2.2.1 Condition 3: Phone1_VRC2

In this context, the smartphone serves as the primary device for authentication, functioning as the interface that presents the user with the challenge to be solved, as depicted in step 1 of Figure 3.3, right panel. In contrast, the HMD operates as the

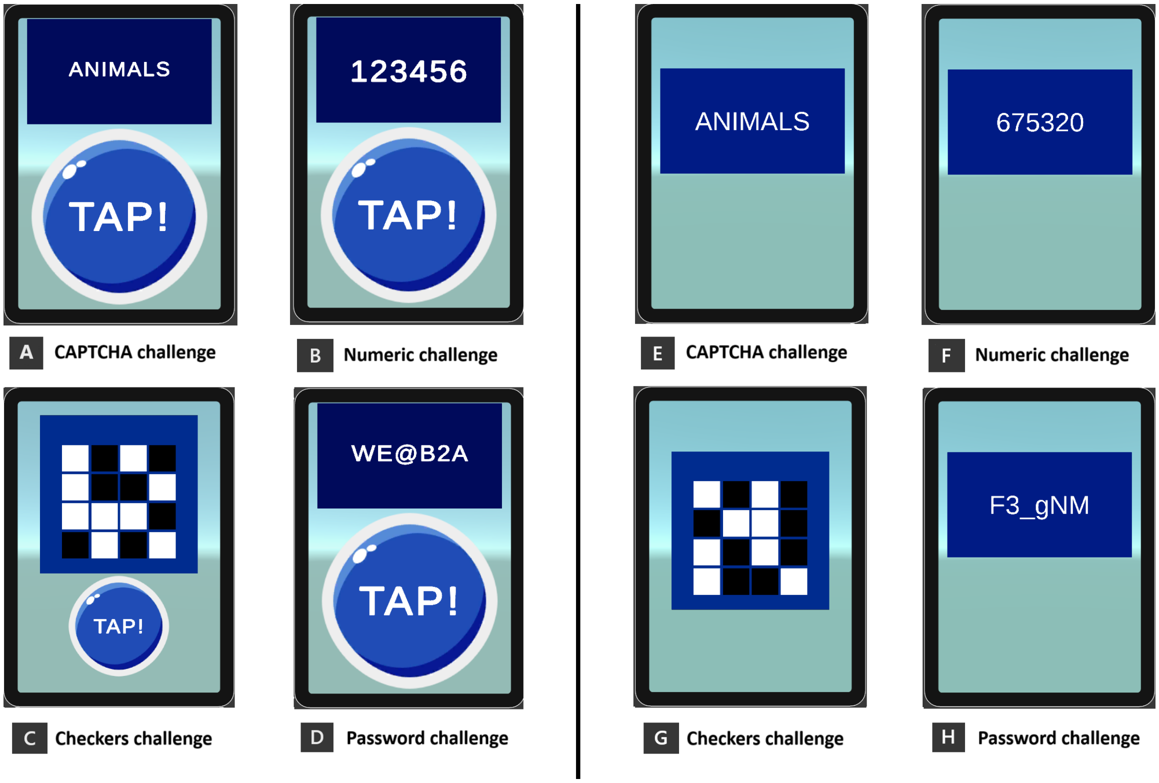
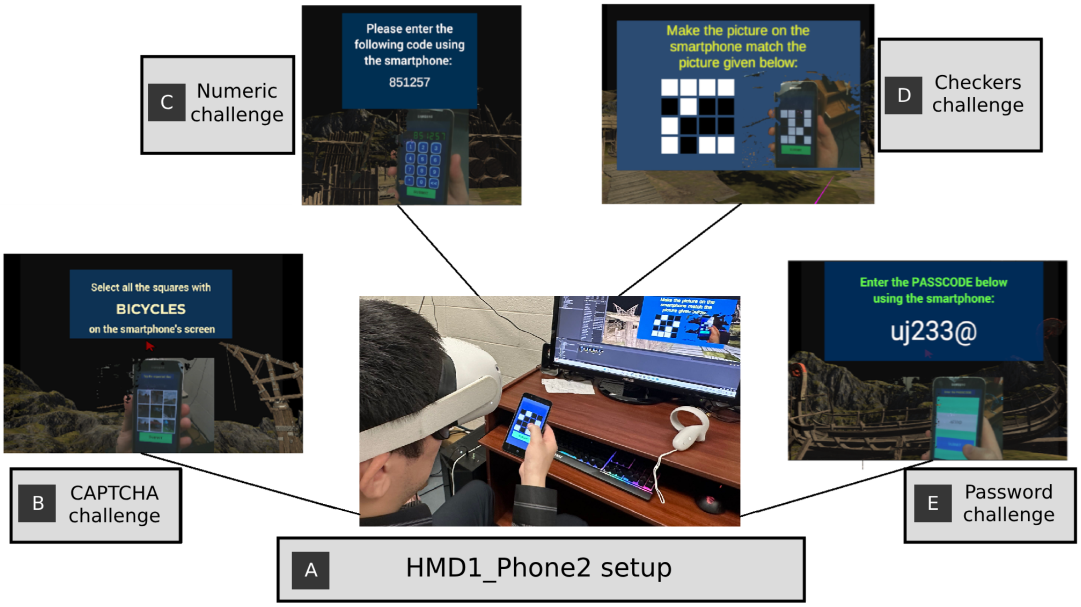


Figure 3.3: An overview of the authentication methods employed for step 1 in conditions 2 and 3. Panels A-D illustrate the challenges presented on the smartphone while using Phone1_SVRP2. In this scenario, users are able to indicate their selections within the VR environment through a gaze-based pointer that is activated by a tap button. Panels E-H depict the challenges presented on the smartphone when utilizing Phone1_VRC2. In this condition, participants use the trigger button on the VR controller to make their selections within the VR environment. This dual-device interaction highlights the varying modalities of user engagement in the authentication process, emphasizing the adaptability of the methods employed.



Please enter the following code using the smartphone: 851257

Make the picture on the smartphone match the picture given below:

Select all the squares with BICYCLES on the smartphone's screen

Enter the PASSCODE below using the smartphone: uj233@

Figure 3.4: Overview of the authentication methods in condition 1 (HMD1_Phone2). A) Displays the experimental setup with a user holding the smartphone while completing the challenges. B-E) Sequence of tasks for participants to solve using the smartphone app, including the CAPTCHA challenge, Numeric challenge, Checkers challenge, and Password challenge.

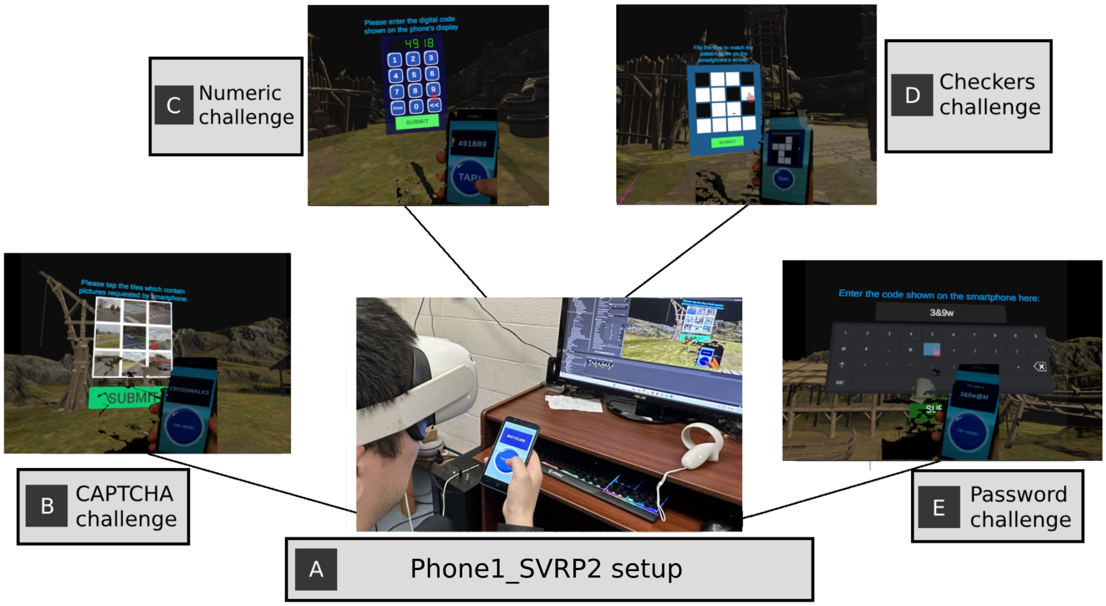


Figure 3.5: Overview of the authentication methods of condition 2 (Phone1_SVRP2): A) Illustrates the experimental setup with a user holding the smartphone for reading and answering the challenge within the VR environment; B,C,D,E) Sequence of tasks provided for the user to solve, correspondingly: CAPTCHA challenge, numeric challenge, checkers challenge, password challenge.

secondary device in the authentication process, where the user is required to input and submit their solution to the challenge, as illustrated in step 2 of Figures 3.6 and 3.7. This dual-device approach not only delineates the roles of each device in the authentication sequence but also emphasizes the integrated use of multiple technological platforms to enhance user interaction and engagement in the virtual environment. This condition resembles Condition 2 previously discussed, with a significant distinction: it incorporates the standard VR controller supplied by the manufacturer of the HMD, referred to as VRC2, as the primary input mechanism within the virtual environment. This decision was chosen because most HMDs are equipped with bespoke controllers designed specifically for facilitating user interactions, such as selection and navigation within VR contexts.

In this methodology, users may be required to engage in a dual-hand operation: one hand is tasked with holding a smartphone to access or review the challenges presented, while the other hand operates the VR controller, as illustrated in Figure 3.6A. Alternatively, users might need to alternate between viewing the smartphone screen and manipulating the VR controller, which could introduce a level of cognitive and physical demand on the user.

It is noteworthy that the challenges presented—CAPTCHA, Numeric, and Password—could theoretically be submitted via text messages without necessitating the installation of any specific application on the smartphone. However, for the sake of maintaining methodological consistency across all experimental conditions, we opted

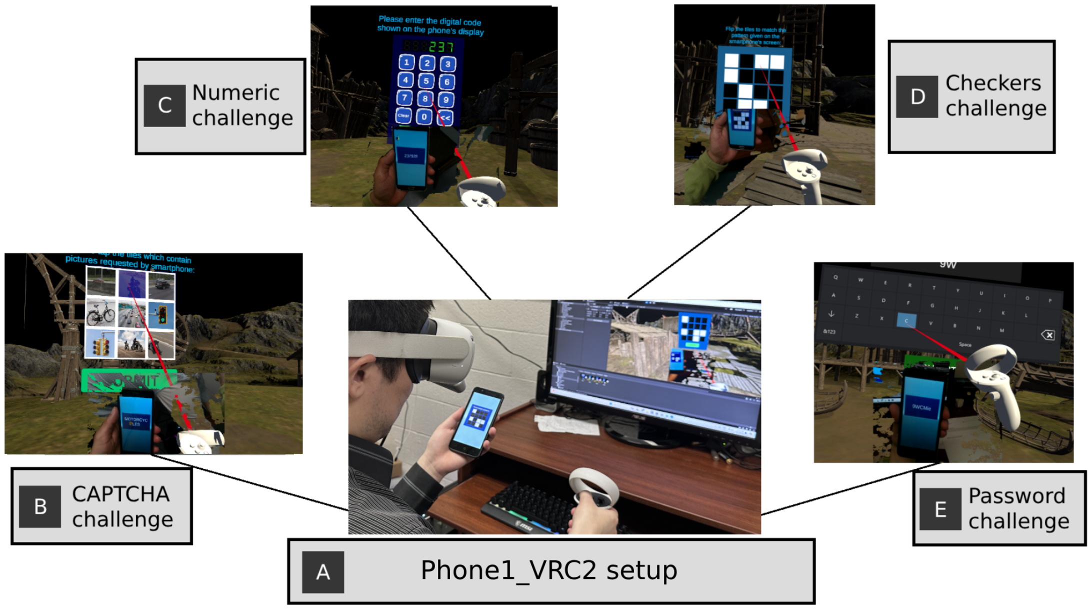
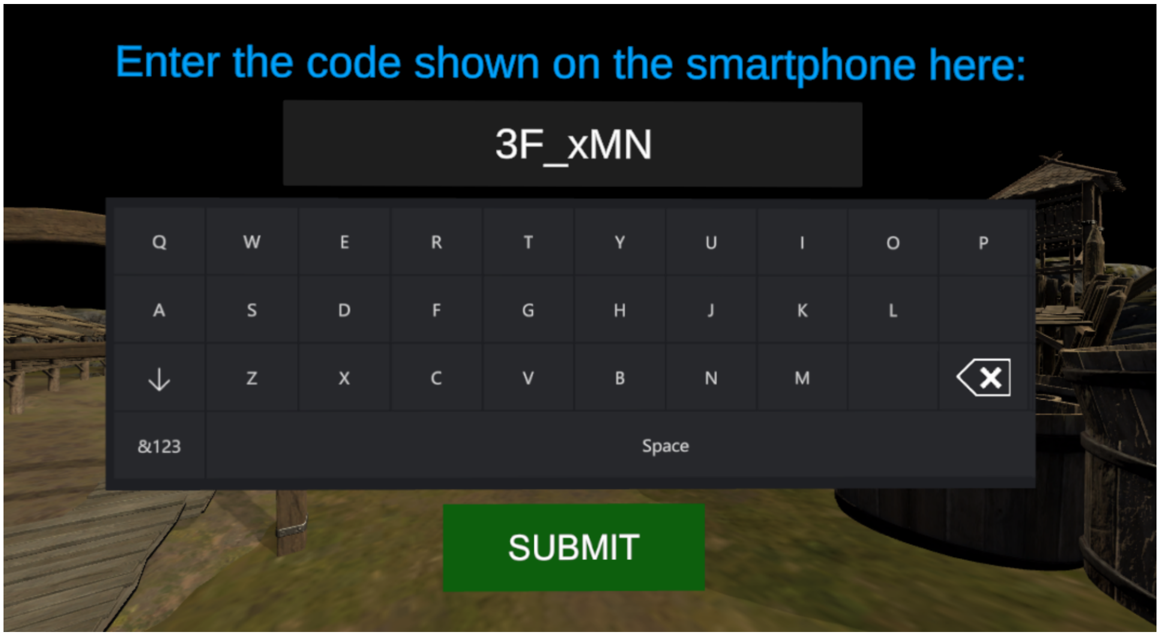


Figure 3.6: Overview of the authentication methods of condition 3 (Phone1_VRC2): A) Illustrates the experimental setup with a user holding the smartphone and a VR controller; B,C,D,E) Sequence of tasks provided for the user to solve, correspondingly: CAPTCHA challenge, numeric challenge, checkers challenge, password challenge.

to employ a dedicated smartphone application. This choice ensures that participants engage with the challenges under equivalent technological parameters.

3.2.3 Overview

Building upon the challenge types and conditions previously outlined, we decided to develop a 4x3 factorial experiment that encompasses four distinct tasks or chal-



Enter the code shown on the smartphone here:

3F_xMN

Figure 3.7: Virtual Keyboard in the VR environment. Utilized during Password challenge in Conditions 2 (Phone1_SVRP2) and 3 (Phone1_VRC2)

lenges: CAPTCHA, Checkers, Numeric, and Password challenges. This experimental framework integrates three conditions for NRXR authentication delivery, resulting in a total of twelve unique authentication options.

The rationale for employing this factorial design lies in its ability to systematically explore the interaction effects between different types of challenges and authentication conditions. By examining a range of tasks, the researchers aimed to capture a comprehensive picture of user experiences and preferences in various contexts, thereby enhancing the validity of the findings.

Following the design phase, a user study was conducted to evaluate the feasibility and usability of each authentication option. This study aimed not only to assess the ease with which participants could engage with the various challenges but also to measure their performance metrics across different conditions. Performance indicators such as completion time, error rates, and user satisfaction were analyzed to determine the effectiveness of each authentication strategy.

3.2.4 System Hardware and Software

The system was implemented using the Unity 3D Game Engine, a widely recognized platform in the development of interactive applications and virtual environments. Furthermore, Unity's compatibility with smartphone development frameworks, such as Android SDK, allows for the seamless incorporation of smartphone capabilities, including touch inputs and mobile-specific functionalities, such as tapping, drawing or virtual keyboard.

The hardware and software utilized in this implementation included:

- **Meta Quest 2** Featuring a resolution of 1832 x 1920 pixels per eye and a refresh rate of 90 Hz, this headset provides a high-quality visual experience essential for immersion in virtual environments.
  - Software Package Requirements: The integration of the Oculus PC app for Meta Quest Link establishes a seamless connection between the headset and the Unity engine. This software enables efficient data transfer and real-time rendering, minimizing latency and maximizing responsiveness in interactions.

- **Intel RealSense and Technology Developer Kit (SR300)**. This depth-sensing camera was incorporated to enhance close-range depth perception, a critical feature for user interactions within a VR context. The camera's specifications—color resolution of 1920x1080 at 30 frames per second, along with an operating range of 0.3m to 2m—enable precise spatial awareness and tracking of user movements. Such capabilities are particularly important in tasks requiring accurate depth recognition, as they allow the system to interpret user actions in real time and respond appropriately, thereby facilitating a more intuitive interaction model. Depth Field of View: H: 73, V: 59, D: 90. Auto-exposure: Off. Brightness level: 350 (setup inside Unity).

- **ZTE Z557BL Smartphone**: this device has a touchscreen resolution of 480 x 854 pixels, along with basic processing capabilities suitable for the application's requirements. The Smartphone has 1.0 GB RAM and 8 GB storage. Android version: 8.1.0. Dimensions: 14.53 x 7.19 x 0.91 cm.

- **Software requirements:**:We use SteamVR Runtime for Windows, along with Unity-compatible Intel RealSense SDK 2.0, to ensure cohesive operation among all hardware components within the Unity environment. We selected version of Unity (2020.3.25f1).

In this implementation, the Intel RealSense SR300 RGB-D camera ismounted on the Meta Quest 2 headset. This configuration enables users to maintain visual contact with the smartphone while immersed in the VR environment. By requiring users to

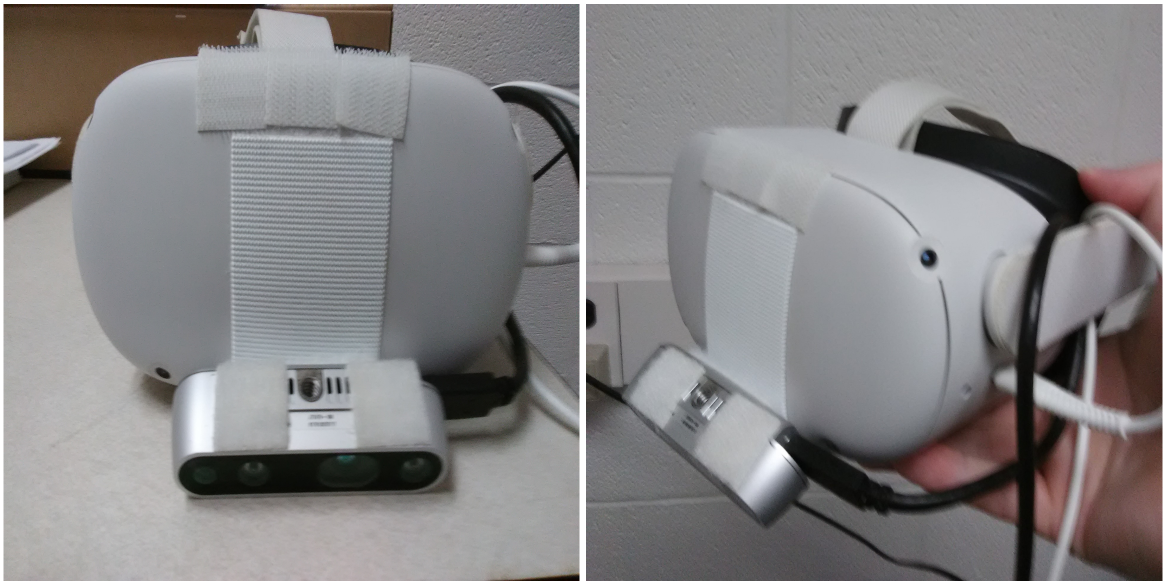


Figure 3.8: Experimental Setup, Left: the front view displays the camera mounted on the headset, with the camera's position relative to the headset being adjustable.; Right: Side view demonstrating the dynamic adjustment of the camera angle, oriented to facilitate a comfortable position for the user to hold the phone in front of the camera.

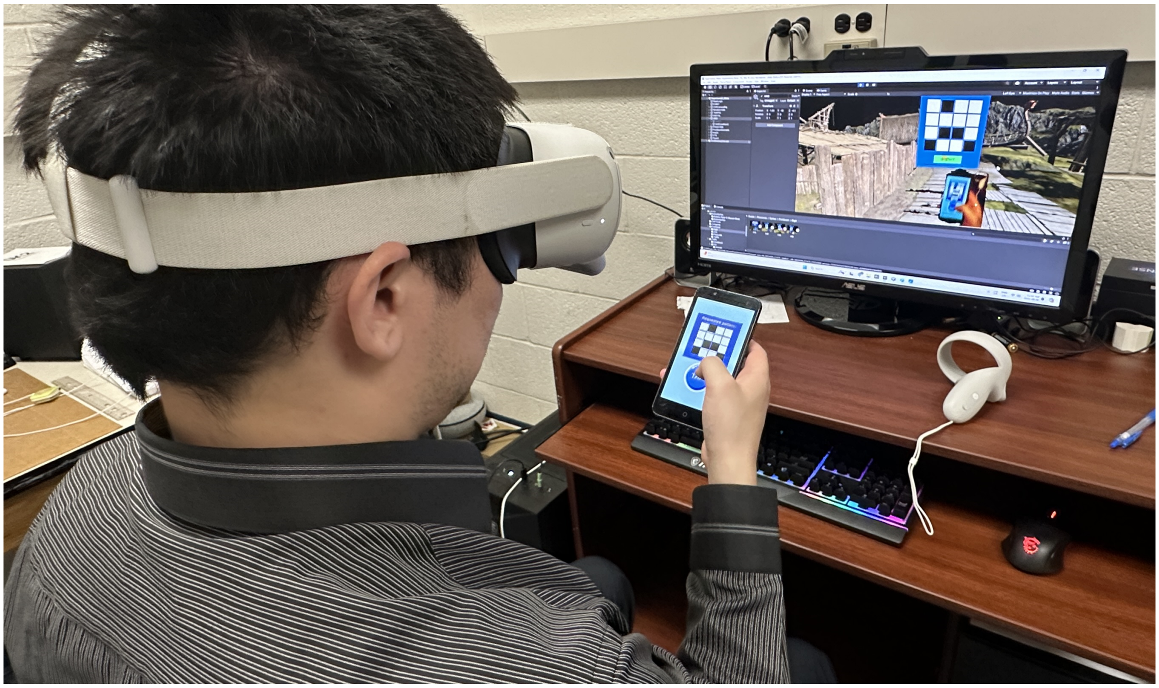


Figure 3.9: Experimental Setup: In Condition 2, the participant holds the mobile device in front of the camera attached to the HMD. The participant is required to input the code (requested by the mobile device) within the VR environment.

position the smartphone within the field of view (FOV) of the camera, the design facilitates real-time interaction with the device.

Our approach supports a hybrid interaction model, where users can draw on the strengths of both platforms—leveraging the immersive capabilities of VR while utilizing familiar smartphone functionalities. Lastly, this design choice enhances user engagement and satisfaction by minimizing the cognitive load associated with switching between devices, ultimately fostering a more cohesive and enjoyable user experience in the virtual environment. Such a framework not only enriches the user experience

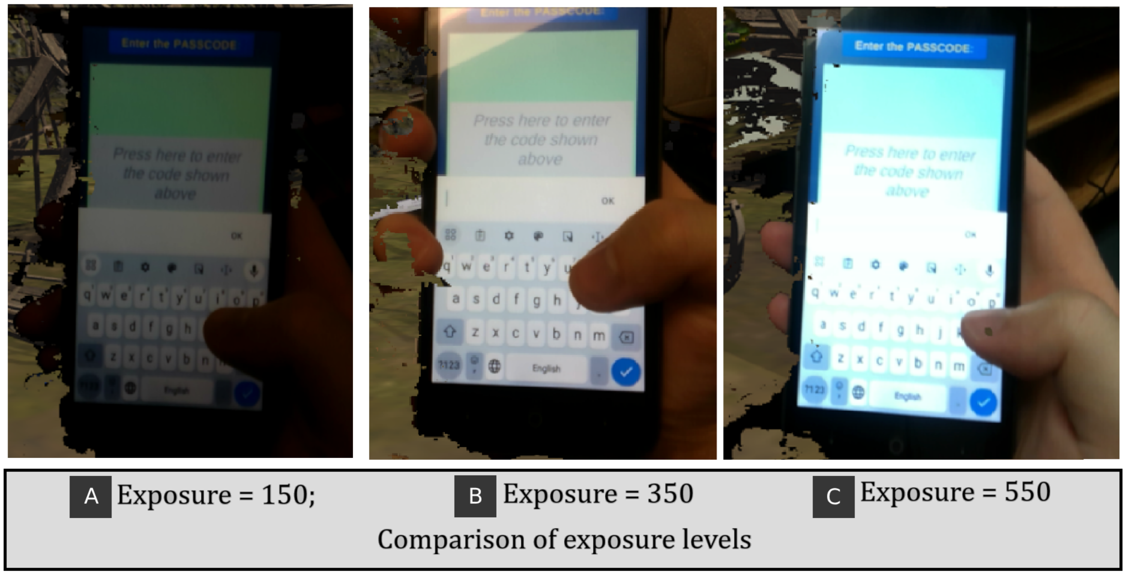

Enter the PASSCODE
Press here to enter the code shown above
A Exposure = 150;
B Exposure = 350
C Exposure = 550
Comparison of exposure levels

Figure 3.10: Manual adjustment of exposure: A) and C) illustrate that too low or too high exposure levels cause picture to darken or brighten so much that it becomes nearly impossible to read the contents of the phone; B) appropriate manual adjustment of the exposure level provides a clear and readable image.

but also sets the stage for further exploration of cross-device interactions in future research.

3.2.4.1 Dealing with overexposure during smartphone video capture

The Intel RealSense camera combines a depth-sensing component with a conventional video camera, enabling a range of applications that require both spatial awareness and visual capture. Typically, standard video cameras are equipped with a dynamic auto-exposure function that automatically adjusts the exposure levels based on the brightness of the scene being recorded. This feature is designed to maintain optimal visibility, ensuring that video frames do not appear too dark or too bright under varying lighting conditions.

To address challenges with auto-exposure when capturing scenes with light-emitting devices like smartphone screens, the feature is disabled, allowing for manual exposure adjustment. By setting a fixed, lower brightness level, the smartphone screen becomes more readable, improving user interaction despite darker surrounding areas. This adjustment, optimized through Unity profiler monitoring, ensures better visibility and enhances the overall VR experience, particularly in scenarios where engaging with the smartphone is crucial.

3.3 Experimental Design

Following the receipt of ethics approval from an Academic Committee on Ethics in Human Research, a within-subject user study was conducted, employing a 4x3 factorial design with 30 participants. The study was situated within a VR scenario that simulated a walkthrough of an old town, featuring teleporting markers to facilitate navigation.

Prior to the experiment, a demographic questionnaire was administered to ascertain the characteristics of the participants.

Once participants completed the demographic questionnaire and signed the informed consent form for data collection, they were provided with a set of instructions outlining the experimental procedures. Figures 3.4 to 3.6 visually represent the various VR scenarios and conditions implemented during the study. The questionnaires are available in Appendix C, located in the Appendices section.

Participants were recruited through email distribution lists and social media postings. After obtaining consent, participants engaged in a total of 15 rounds of sequential challenge completion in the VR environment, initially using a VR controller to navigate via teleporting markers. Following this, they completed another 15 rounds utilizing a smartphone in conjunction with the SmartVR pointer technique [73], replicating the navigation method of the initial session.

Participants were randomly assigned to one of several groups, each exposed to all three conditions in varying orders (for example, sequence of conditions 1, then 3, then 2, or 3, 1, 2). This randomization is critical for mitigating order effects and enhancing the validity of the results. With six possible orders for condition exposure, each group consisted of five participants. For each condition, participants commenced with one trial round, which was not measured. This trial round served to acclimate participants to the VR environment and the navigation methods. Subsequently, each participant completed five measured rounds, along with one additional round dedicated to collecting feedback, culminating in a total of seven rounds per condition (1 training round, 5 measured rounds, and 1 feedback round).

Throughout each round, participants encountered challenges in the following sequence: CAPTCHA, Numeric, Checkers, and Password (presumably, from easiest one to the hardest one). Users transitioned from one challenge to the next using designated teleporting locations that directed them to the subsequent task. Data collection focused on two primary metrics: the time taken by participants to complete each challenge—recorded from the moment they arrived at the challenge until it was solved—and the number of unsuccessful attempts for each task.

On the seventh round, participants provided feedback through a user experience questionnaire utilizing a 7-point Likert scale. This questionnaire was designed to capture participants' perceptions and satisfaction regarding each challenge, enabling a comprehensive analysis of user experience and performance. The questionnaire consisted of the following quiestions:

- How much did you like this way of authenticating?

  1 (I did not like it at all) — 2 — 3 — 4 (Neutral) — 5 — 6 — 7 (I liked it very much)

- On a scale from 1 to 7, How effective did you find this way of authenticating?

  1 (Not effective at all) — 2 — 3 — 4 (Neutral) — 5 — 6 — 7 (Very effective)

- On a scale from 1 to 7, How easy to use did you find this way of authenticating?

  1 (Not easy at all) — 2 — 3 — 4 (Neutral) — 5 — 6 — 7 (Very easy)

At the conclusion of the experiment, unstructured feedback regarding the participants' experiences was gathered using a paper-based questionnaire featuring open-ended questions.

Specifically, participants were asked to share their preferences regarding the various methods, challenges, and input conditions encountered throughout the experiment. Understanding these preferences is crucial for evaluating the effectiveness and user-friendliness of the implemented approaches. Additionally, the questionnaire sought to identify any symptoms or discomfort that participants may have experienced during the VR session.

Moreover, participants were invited to discuss which tasks or interactions they found to be the easiest and hardest. This feedback is instrumental in identifying potential areas for improvement in the design of VR challenges and navigation methods. Analyzing these open-ended responses allows for deeper insights into user experiences, facilitating the refinement of future VR applications and enhancing the overall user experience. Such qualitative data complements the quantitative findings, offering a holistic view of participant engagement and satisfaction, ultimately contributing to a more comprehensive understanding of the system's performance and usability.

Please refer to the Appendix for the questionnaires utilized in this study. The Appendix includes both the demographic questionnaire administered prior to the experiment and the open-ended feedback questionnaire collected at the end. These instruments were designed to capture essential participant information and gather detailed insights into their experiences, preferences, and any challenges encountered during the VR sessions.

3.3.1 Data Analysis

To investigate whether the composition of the six order groups with respect to participants' gender, age, occupation, and prior experience with HMDs adhered to the expectations derived from a random allocation of participants, Pearson's Chi-square tests were conducted. The p-values for these tests were calculated using Monte Carlo simulations, employing 100,000 replicates to ensure robust statistical inference.

Furthermore, to assess the differences in task completion times and the number of clicks among the various conditions, Analysis of Variance (ANOVA) analyses were performed for each of the four tasks. In these analyses, the effects of both the order of challenges presented to the participant and the round number were taken into account, allowing for an understanding of how these variables might influence performance.

To facilitate pairwise comparisons of the means across different conditions, orders, and rounds, Tukey's Honestly Significant Difference (HSD) test was employed as a post-hoc analysis. This approach enabled the identification of specific differences between groups that might not have been apparent in the overall ANOVA results.

Additionally, to evaluate variations in participants' responses to the Likert-scale questions in the user experience questionnaire across conditions, pairwise Wilcoxon tests were conducted. These tests were adjusted for multiple comparisons using the false discovery rate (FDR) correction, thereby mitigating the risk of Type I errors associated with multiple hypothesis testing.

All statistical analyses were executed using R software (version 4.3.1), and data visualizations were generated utilizing the ggplot2 package (version 3.4.3).

Chapter 4

Results

Out of the 30 participants in the study, the age distribution was as follows: 40% (12 individuals) were aged 18 to 24, 56.67% (17 individuals) were aged 24 to 48, and a small minority, 3.33% (1 individual), fell within the 48 to 65 age range. This demographic breakdown indicates a predominance of younger adults, particularly those in their mid-20s to late 40s, which may reflect trends in technology adoption among these age groups.

Regarding academic background, 36.67% (11 participants) were enrolled in computer science programs, whether graduate or undergraduate. In contrast, 40% (12 participants) were non-computer science students, while the remaining 23.33% (7 individuals) comprised staff, faculty, or alumni.

For gender representation among participants, one-third (10 participants) identified as female and two-thirds (20 participants) identified as male. This disparity could influence our findings.

In terms of experience with HMDs, nearly half of the participants (46.67%, or 14 individuals) reported having never used an HMD. A third (33.33%, or 10 individuals) had limited experience, using HMDs for less than one month in total. A smaller percentage, 10% (3 individuals), had between one and six months of experience, while 6.67% (2 individuals) reported having used HMDs for six months to two years. One participant chose not to disclose their HMD usage experience. This distribution indicates that a significant portion of the participants are novices regarding HMD technology, which may impact their engagement with and feedback on related systems or applications.

In this study, participants demonstrated a marked increase in completion times for the Password challenge compared to the other three challenges, with the Numeric challenge yielding the fastest completion times (see Table 4.1). Analysis of variance (ANOVA) results indicated that, with the exception of the Checkers challenge, the primary factor influencing completion times was the condition under which the challenges were presented (refer to Table 4.2).

Furthermore, the effects of the order of condition presentation and the round number on challenge completion time exhibited significant variability across the different challenges. Specifically, these factors were found to be statistically significant for the CAPTCHA and Checkers challenges, while their influence was notably diminished in the Numeric and Password challenges.

These findings underscore the importance of considering the nature of the authentication challenge when selecting an interaction modality.

Condition	**CAPTCHA**	**Numeric**	**Checkers**	**Password**
HMD1_Phone2	17.76 ± 10.46	**10.68 ± 3.27**	13.63 ± 5.18	33.45 ± 19.22
Phone1_SVRP2	12.92 ± 4.16	12.47 ± 4.79	14.47 ± 6.50	**28.35 ± 9.33**
Phone1_VRC2	**12.41 ± 5.02**	13.90 ± 5.92	**13.44 ± 9.33**	36.32 ± 18.05
Average ± sd	14.36 ± 7.5	**12.35 ± 4.95**	13.85 ± 5.29	32.71 ± 16.44

Table 4.1: Mean completion times (in seconds) and standard deviation per condition for each of the four challenges. The lowest mean completion time per challenge and the lowest overall average completion time are highlighted.

The results of the ANOVA analysis revealed statistically significant differences in mean completion times across conditions for the CAPTCHA, Numeric, and Password challenges (see Figure 4.1 and Table 4.1).

Notably, the Password challenge exhibited the largest performance differences, with participants completing the task an average of 8 seconds faster in the Phone1_SVRP2 condition compared to the Phone1_VRC2 condition. Similarly, in the Numeric challenge, participants showed an average improvement of 3.2 seconds when using the HMD1_Phone2 condition as opposed to the Phone1_VRC2 condition. In contrast, the CAPTCHA challenge demonstrated a decline in performance, with participants

Factor	**CAPTCHA**		**Numeric**		**Checkers**		**Password**	
	F-value	p-value	F-value	p-value	F-value	p-value	F-value	p-value
Condition	30.02	$\mathbf{5.99 \times 10^{-13}}$	17.45	$\mathbf{5.09 \times 10^{-8}}$	1.69	0.185	9.69	$\mathbf{7.62 \times 10^{-5}}$
Round	12.13	$\mathbf{2.31 \times 10^{-09}}$	3.17	0.014	3.49	**0.008**	1.90	0.11
Order	15.28	$\mathbf{3.83 \times 10^{-07}}$	1.75	0.175	7.14	**0.0009**	6.88	**0.001**

Table 4.2: ANOVA results of completion times per challenge. P-values less than 0.01 are highlighted.

Condition	**CAPTCHA**	**Numeric**	**Checkers**	**Password**	**Average**
HMD1_Phone2	85%	97%	**92%**	88%	90%
Phone1_SVRP2	94%	**99%**	89%	**91%**	**93%**
Phone1_VRC2	**96%**	93%	91%	87%	91%
Average ± sd	91.67% ± 5.86%	**96.33% ± 3.06%**	90.67% ± 1.53%	88.67% ± 2.08%	91.83%

Table 4.3: Success rate per condition for each of the four challenges. The highest success rate per challenge and the highest overall average success rate are highlighted.

taking an average of 5.3 seconds longer in the HMD1_Phone2 condition compared to the Phone1_VRC2 condition, and 4.8 seconds longer than in the Phone1_SVRP2 condition.

These findings highlight the significant impact of interaction modalities on task performance across different challenges. The variation in completion times suggests that specific conditions can either enhance or hinder user efficiency, emphasizing the necessity for careful consideration of interaction designs in future system development.

As the minimum number of clicks required to complete any of the challenges was set to six, on average, participants required 7.96 ± 2.97, 8.3 ± 2.04, 8.8 ± 1.56, and 13.97 ± 7.99 clicks to complete the Numeric, Checkers, CAPTCHA, and Password challenges, respectively. The number of clicks was not significantly influenced by condition, order, or round in the CAPTCHA and Numeric challenges. However, condition emerged as a significant factor in both the Checkers (F value = 18.72, p-value = 1.57×10^{-8}) and Password (F value = 24.93, p-value = 5.55×10^{-11}) challenges.

In the Checkers challenge, participants required an average of 1.4 and 0.85 additional clicks in the Phone1_SVRP2 and Phone1_VRC2 conditions, respectively, compared to the HMD1_Phone2 condition (see Figure 4.2). Similarly, in the Password challenge, participants needed an average of 3.74 and 6.15 more clicks in the Phone1_SVRP2 and Phone1_VRC2 conditions, respectively, than in the HMD1_Phone2 condition (see Figure 4.2).

The study also tracked the number of unsuccessful attempts made by participants, calculating the success rate for each challenge and condition combination as the percentage of successful attempts over total attempts (refer to Table 4.3). Overall success rates averaged from 90

Moreover, there was a significant positive correlation between completion time and the number of clicks. This correlation was the strongest for the Password challenge (Spearman's ρ = 0.53, p-value ¡ 2.2×10^{-16}) and the weakest for the CAPTCHA challenge (Spearman's $\rho = 0.15$, p-value = 0.002).

These findings underscore the intricate relationship between user interaction metrics, completion times, and the efficacy of different conditions across various challenges. Understanding these dynamics is crucial for designing more effective interaction modalities and optimizing user experiences in future applications.

Participants' feedback, as illustrated in Figure 4.3, indicates a preference for the Phone1_SVRP2 and Phone1_VRC2 conditions over the HMD1_Phone2 condition. This preference was statistically supported by FDR-adjusted Wilcoxon rank's p-values of 0.007 and 1.9×10^{-5}, respectively, suggesting that participants significantly favored these conditions.

Moreover, the perceived effectiveness of the Phone1_SVRP2 and Phone1_VRC2 conditions was also rated higher than that of the HMD1_Phone2 condition, with FDR-adjusted Wilcoxon rank's p-values of 0.003 for both comparisons. This finding underscores the effectiveness of the Phone1 conditions in meeting participants' expectations for task completion.

In terms of ease of use, participants similarly rated the Phone1_SVRP2 and Phone1_VRC2 conditions as easier to use compared to the HMD1_Phone2 condition, with FDR-adjusted Wilcoxon rank's p-values of 0.003 and 0.0001, respectively. The consistency of these ratings suggests that both Phone1 conditions provided a more user-friendly experience.

Overall, the scores for the Phone1_SVRP2 and Phone1_VRC2 conditions were comparable, indicating apreference for these interaction modalities over the HMD1_Phone2 condition. The remaining plots for separate challenges' results (e.g. Captcha clicks/time plot) can be found in Appendix E (Figures E.14 - E.21), located in the Appendices section.

4.1 Unstructured Feedback

Participants shared their preferences regarding the best and worst challenges encountered during the experiment by providing feedback in the unstructured section of the post-questionnaire. The results of this feedback are summarized in Table 4.4. Comments were categorized into four distinct groups for each challenge, and the percentages of comments in each category were calculated based on the total of 42 comments, which included 23 positive and 19 negative remarks.

The Checkers challenge received the most favorable feedback, with 26% of all comments identifying it as either a good challenge or the best challenge, and notably, there were no negative comments recorded for this challenge. The Numeric challenge followed as the runner-up, garnering 16.67% positive comments alongside 7.14% negative comments.

In contrast, the CAPTCHA challenge elicited mixed reactions, with positive and negative comments evenly distributed at 9.52% each. The Password challenge was particularly challenging for users, as evidenced by 28.57% of comments expressing negative sentiments and only 2.38% indicating positive feedback. One participant's comment exemplifies this struggle: "With respect to entering the code from the keypad of the phone, I almost got the feeling that my grandpa gets while he enters a text message." This feedback underscores the difficulties faced by participants in this challenge.

Overall, the analysis of participants' feedback reveals distinct preferences between challenges, with Checkers emerging as the most favored and Password as the least well-received.

A similar analysis was conducted for the three conditions, yielding a total of 42 comments. The feedback reflected a clear preference, with twice as many positive comments as negative ones (28 positive vs. 14 negative). Participants overwhelmingly favored the Phone1_SVRP2 condition, with 35.71% of comments expressing appreciation for most or some of its features, while only 2.38% reported any dislike for it.

The Phone1_VRC2 condition was the second most preferred, with 23.81% of comments indicating positive sentiments about some or most of its aspects; however, 11.9% of participants noted some dislikes. Conversely, the HMD1_Phone2 condition was the least favored, receiving only 7.14% of positive comments. A significant 19.05% of participants expressed dissatisfaction with this condition, resulting in an overall negative balance between positive and negative feedback. This negative sentiment may be attributed to the challenges participants faced when completing the CAPTCHA and Password tasks, which were linked to the HMD1_Phone2 condition.

For a detailed breakdown of the preferences for each condition, refer to Table 4.5. This analysis highlights the significant variations in user experiences across the different conditions, providing valuable insights for enhancing future designs and addressing usability issues.

Category	**CAPTCHA**	**Numeric**	**Checkers**	**Password**	**Total**
Best challenge	2.38%	4.76%	14.29%	0.00%	**21.43%**
Good challenge	7.14%	11.90%	11.90%	2.38%	**33.33%**
Bad challenge	7.14%	7.14%	0.00%	19.05%	**33.33%**
Worst challenge	2.38%	0.00%	0.00%	9.52%	**11.90%**
Balance	**0.00%**	**9.52%**	**26.19%**	**-26.19%**	**9.52%**

Table 4.4: Summary of participants' comments regarding the challenges encountered during the experiment, gathered as unstructured feedback within the post-test questionnaire . The last row shows the balance of the percentages of positive comments minus the negative ones.

While not all participants expressed a specific preference for a particular combination of challenge and condition, the most frequently cited optimal pairing was the Checkers challenge in conjunction with the Phone1_SVRP2 condition. One participant notably emphasized this preference, stating: "Reading the codes from the smartphone's screen seemed the most efficient to me due to the possibility to simul-

Category	**HMD1_Phone2**	**Phone1_SVRP2**	**Phone1_VRC2**	**Total**
Mostly Positive	0.00%	21.43%	9.52%	**30.95%**
Positive	7.14%	14.29%	14.29%	**35.71%**
Negative	9.52%	2.38%	7.14%	**19.05%**
Mostly Negative	9.52%	0.00%	4.76%	**14.29%**
Balance	**-11.90%**	**33.34%**	**11.91%**	**33.32%**

Table 4.5: Summary of participants' comments regarding the conditions encountered during the experiment, with mostly positive results being an average within [6;7] on a Likert scale, positive within [4;5], negative within [2;3], and mostly negative within [0;1] range. The last row shows the balance of the percentages of positive comments minus the negative ones.

taneously look and read the codes and enter the answer with head movement. I liked the idea of authentication via the 'checkers' system; it was the most entertaining one."

This feedback highlights the perceived efficiency and engagement offered by this combination, suggesting that the integration of visual cues with interactive movements enhanced the overall user experience.

4.1.1 Summary

The impact of the condition on participants' completion times varied significantly across the different challenges. Notably, while the Password challenge appeared to be the least suited for a virtual reality (VR) environment, participants nonetheless completed this challenge the fastest when using the Phone1_SVRP2 condition. This suggests that, despite inherent challenges associated with password entry in VR, the specific features of the Phone1_SVRP2 condition may have facilitated a more efficient experience for users.

In contrast, the Checkers challenge demonstrated that the condition used did not significantly influence participants' performance, indicating that the nature of this challenge may inherently promote consistent completion times, regardless of the interaction modality.

For the Numeric challenge, participants achieved the fastest completion times in the HMD1_Phone2 condition. This finding highlights that some challenges may benefit from the immersive capabilities offered by VR more than the others, potentially enhancing user engagement and focus.

The CAPTCHA challenge revealed a different trend, where the Phone1_SVRP2 and Phone1_VRC2 conditions allowed participants to complete the task relatively quickly, and significantly faster than the HMD1_Phone2 condition. This suggests that the latter may introduce unnecessary complexities or inefficiencies that hinder performance in CAPTCHA tasks.

Overall, users expressed more favorable perceptions of the Phone1_SVRP2 and Phone1_VRC2 conditions compared to the HMD1_Phone2 condition.

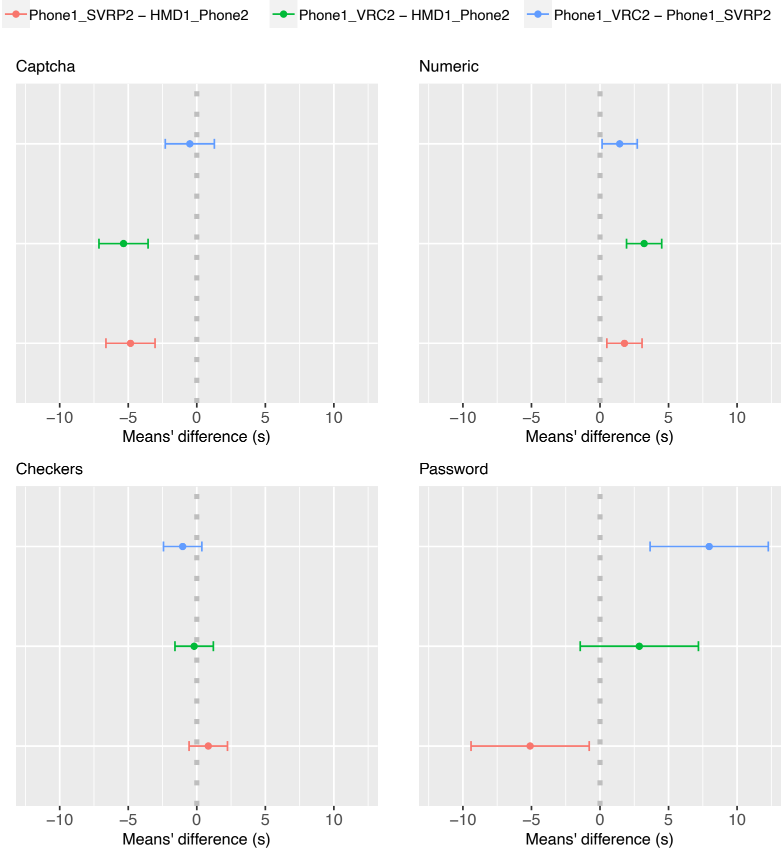


Figure 4.1: The figure displays the 95% confidence intervals for the pairwise differences in mean completion times between conditions for all four challenges. Each circle represents the mean difference in completion time, with the dashed vertical gray line indicating the point of no difference between the means. The further the confidence interval is from this dashed line, the more statistically significant the difference in completion times. All differences are measured in seconds. This visualization allows for a clear assessment of the varying effects of different conditions on participants' performance across challenges, highlighting which pairwise comparisons yielded the most substantial and significant differences.

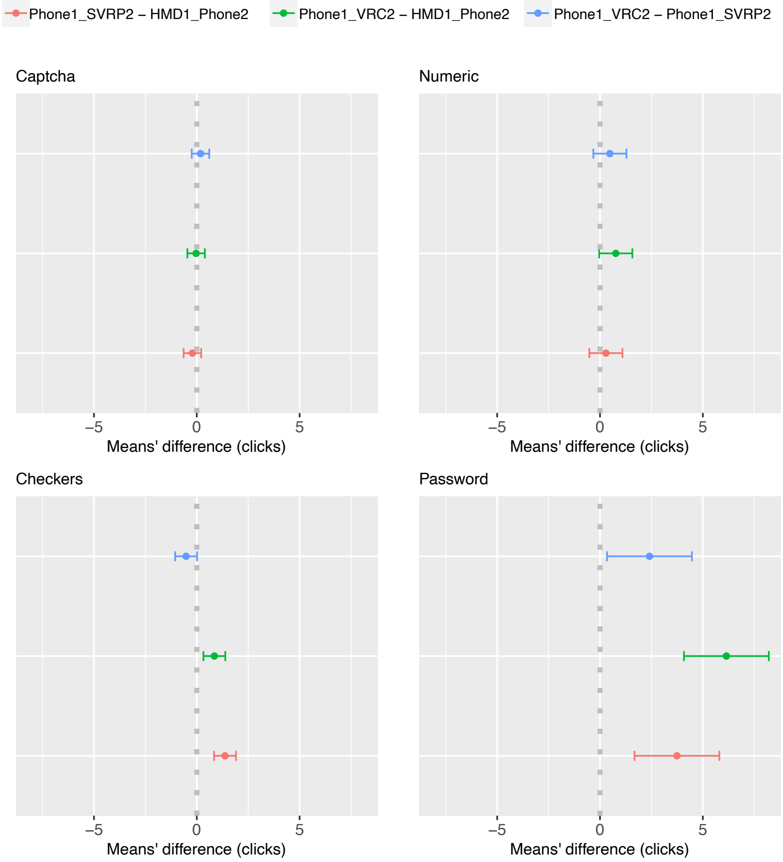


Figure 4.2: The figure presents the 95% confidence intervals for the pairwise differences in mean number of clicks between conditions for all four challenges. Each circle indicates the mean difference in clicks, while the dashed vertical gray line marks the point of no difference between the means. The farther the confidence interval extends from this dashed line, the more statistically significant the difference in the number of clicks. All differences are represented as counts of clicks. This visualization provides an effective overview of how different conditions impact user interaction across challenges, emphasizing which comparisons reveal the most meaningful differences in clicking behavior.

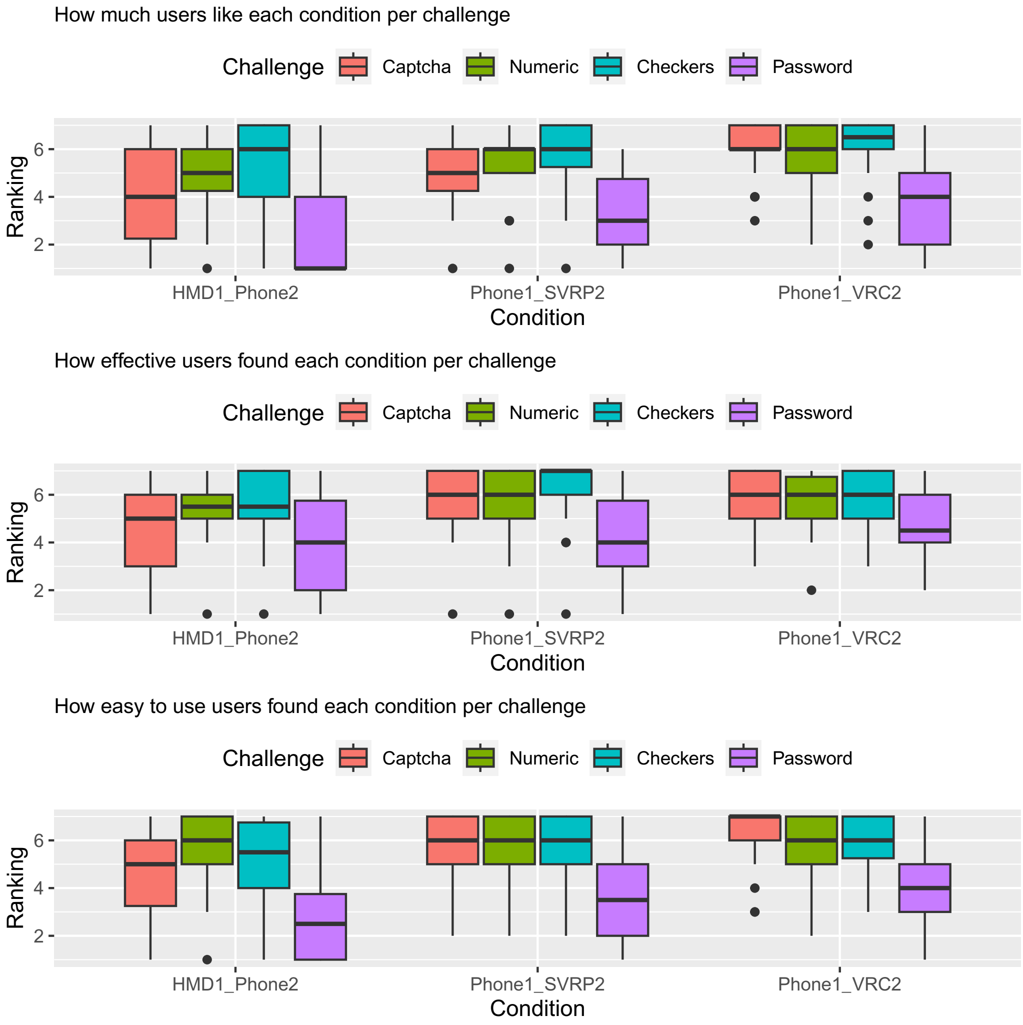


Figure 4.3: The distribution of Likert-scale scores provided by participants for each condition across challenges reflects their evaluations of how much they liked the condition, its perceived effectiveness, and ease of use. In this ranking system, a score of 7 represents the highest level of satisfaction, 4 denotes a neutral perception, and 1 indicates the lowest level of satisfaction. The horizontal line within each box represents the median score, while the height of the box illustrates the interquartile range (IQR), indicating the spread of scores around the median.

Chapter 5

Discussion

This section reflects on the results obtained in relation to the research questions, discusses limitations, and suggests avenues for future work.

5.1 Reflection on Results

Regarding Research Question 1 (RQ1), all participants successfully completed every challenge across the three conditions. This outcome is encouraging given the diversity of the authentication tasks involved. The observed success rates strongly support the feasibility of utilizing NRXR for two-step authentication, demonstrating that users can effectively identify text, digits, images, and patterns without removing their HMDs. However, significant differences emerged between the various challenges and conditions, which will be elaborated upon.

Addressing Research Question 2 (RQ2), which explores the most suitable types of authentication challenges for implementing two-step authentication in a VR context, the results indicate that the Checkers challenge was the most favorable for deployment. It received the highest ratings in terms of user preference, effectiveness, and ease of use across all conditions. While some participants excelled under specific interaction modalities, Checkers consistently yielded positive results overall and was clearly preferred in the unstructured feedback. The Numeric challenge emerged as a close second, likely due to its familiarity among users and recording the highest average success rate, particularly in conjunction with the Phone1_SVRP2 condition.

However, the Checkers challenge is more vulnerable to brute-force attacks compared to the Numeric code, which offers a significantly larger configuration space (65,536 versus 1 million). To mitigate this vulnerability, adding an additional row or column to the Checkers grid could increase its complexity, making its number of configurations more comparable to that of the Numeric challenge.

The CAPTCHA challenge ranked third in terms of performance, receiving neutral to positive feedback. Nonetheless, it was rated least favorable in the HMD1_Phone2 condition, where participants found it less effective and user-friendly. The difficulty in recognizing shapes in tiles using the NRXR technique, compared to a direct view through the HMD, likely contributed to this outcome.

Among the challenges analyzed, the Password challenge was found to be the least suitable for the VR environment, despite its robustness against external attacks, which allows for approximately 100 billion configurations. The complexity of the task increased likely due to the need for users to switch between different keyboard layouts for special, upper, and lower case characters. This was particularly challenging in the HMD1_Phone2 condition, where the smaller display area made character recognition more difficult. Furthermore, the penalty for correcting mistakes was greater for users relying on a keyboard, as they had to delete previously entered characters to return to the point of error. These factors likely explain why the Password challenge received the lowest rankings among all tasks.

In addressing Research Question 3 (RQ3), the effectiveness of presenting challenges using a smartphone (conditions Phone1_SVRP2 and Phone1_VRC2) versus within the VR environment (condition HMD1_Phone2) showed that participants generally found it less effective to first present challenges using the HMD and then respond with the smartphone. This was particularly true for the CAPTCHA and Password challenges, which received the lowest effectiveness ratings in the HMD1_Phone2 condition. For the Checkers and Numeric challenges, users perceived both variations as equally effective. These findings reinforce the recommendation that the Checkers matching challenge is the most suitable authentication method, followed closely by the Numeric challenge. The CAPTCHA challenge was rated higher in the Phone1 conditions compared to the HMD1_Phone2 condition, with Phone1_SVRP2 achieving the highest overall success rate, followed by Phone1_VRC2.

Lastly, in relation to Research Question 4 (RQ4), the combination of structured and unstructured feedback provided valuable insights into participants' experiences, impressions, and preferences. A clear trend emerged, with a significant percentage of participants preferring the Checkers challenge, contrasting with the proportion that expressed dissatisfaction with the Password challenge. The Numeric challenge garnered positive feedback, ranking as the second most favored after Checkers, while the feedback on the CAPTCHA challenge remained balanced across conditions. Excluding the Password challenge, participants found the other three challenges relatively easy to use, regardless of the interaction modality. Notably, a substantially higher proportion of participants reported positive impressions of the Phone1_SVRP2 condition compared to the other two conditions.

These reflections underscore the importance of usability and user experience in the design of authentication challenges, suggesting that tailored approaches to VR environments can significantly enhance user satisfaction and task effectiveness. Future research should continue to explore ways to optimize these challenges and conditions to improve overall user experience and security in authentication processes.

5.1.1 Limitations

Several limitations were identified in the current setup. The foremost limitation is the presence of cables. While the latest generation of head-mounted displays (HMDs) has made significant strides in reducing the need for users to remain tethered to a computer or laptop, achieving complete wireless operation remains a challenge. Although some models, such as the Apple Vision Pro, still require a connection to a portable battery, the ideal scenario involves users operating without any physical cables linking them to a workstation.

The option of using wireless cameras was considered; however, the delay between user actions and their reflection in the VR environment posed a substantial limitation due to transmission times. This latency issue may improve with the adoption of faster network protocols in the future. Additionally, the depth-sensing camera employed in this setup is not designed for wireless operation. Transitioning to a fully wireless configuration would necessitate additional hardware, further complicating the burden of wearing both the HMD and the camera.

Another limitation pertains to the types of challenges suitable for two-step authentication in VR. The range of potential implementations for two-step authentication challenges in a virtual environment is extensive. For instance, challenges could include gaming-style 3D puzzles where users must manipulate objects in 3D space to uncover a code for use on a second device, or Mixed-Reality challenges that juxtapose real and virtual objects. Given the vast array of possibilities, the current study focused on well-established challenges, leaving the exploration of more complex and innovative options for future research.

5.1.2 Future Work

For future work, several avenues for improvement have been identified. One key area is the implementation of NRXR without relying on a depth-sensing camera.

In this context, machine learning techniques could simulate real depth sensing, potentially proving effective for many everyday scenarios. This approach would offer the significant advantage of eliminating the need for a physical cable connecting the depth-sensing camera to the workstation.

Another potential enhancement is the integration of hand tracking, allowing users to complete the final step of two-step authentication without the use of a controller. This change could facilitate a more intuitive interaction by removing the need for a VR controller or smartphone during the authentication process in Phone1 conditions. However, it is important to consider that this shift would forfeit haptic feedback and the tangible aspects of the current setup, which provide their own benefits.

Additionally, utilizing the built-in cameras of the latest generation of HMDs could represent a substantial improvement. At the time of this submission, manufacturers restrict developers from accessing the video streams from these cameras due to privacy concerns. Gaining access to this hardware would enable the recreation of depth-sensing capabilities similar to those of the Intel Real Sense camera, thus providing a pathway for implementation without the need for cables.

Another area for improvement involves incorporating high dynamic range (HDR) video capture. This enhancement would improve the capture of smartphone and smartwatch screens while avoiding the darkening of other elements in the scene, such as users' hands, leading to a more realistic representation of skin tones. An alternative design might involve a 2D-3D hybrid setup to track the smartphone and display users' hands. However, this approach would still depend on a wired camera mounted on the HMD.

Exploring alternative methods for two-step authentication presents another line of inquiry. One possibility is to use voice as the second authentication step. Users could be prompted to read aloud a message received on their smartphone, with the system verifying both the content of the message and the user's voice as a biometric signature. Nonetheless, this method is vulnerable to attacks utilizing text-to-speech generative AI. An alternative could involve users receiving audio codes to act upon and complete the authentication challenge.

Lastly, enhancing hardware capabilities is crucial for advancing the overall experience. The latest generation of HMDs boasts significantly higher screen resolutions than the setup used in this study. For example, the Meta Quest 3 features approximately 4.5 megapixels per eye, while the Apple Vision Pro offers around 11.7 megapixels per eye. In contrast, the Meta Quest 2 utilized in this experiment has roughly 3.5 megapixels per eye. Combining this increased resolution with high-quality stereoscopic video capture could lead to substantial improvements, particularly in the readability of text displayed on smartphones. Ideally, users would perceive their smartphone screens and hands as clearly through their HMDs as they would without them.

Chapter 6

Conclusion

Methods for implementing two-step authentication in VR using smartphones were explored, demonstrating the feasibility of successful user authentication through various approaches. The findings indicate that NRXR can effectively facilitate tasks such as scanning and selecting images, matching visual patterns, operating virtual numeric keypads, and reading and typing short passwords for authentication purposes.

Among the methods evaluated, the checkers-style matching challenge emerged as the most suitable option, while the numeric sequence challenge ranked as a close second. This is particularly noteworthy, as the numeric sequence is a familiar method for most users today. Additionally, CAPTCHA-style challenges were found to be viable under specific conditions. Conversely, the study revealed that short but robust passwords posed significant challenges for users and were generally disliked.

The research highlights the potential for various approaches to enhance two-step authentication in VR and encourages further exploration of these methods to improve user experience and security.

One of the more challenging aspects of two-step authentication in VR, however, was the use of short but robust passwords. Despite the fact that strong, complex passwords are a critical element of security, users consistently struggled with remembering and inputting these passwords in VR environments. The tactile feedback of typing on a physical keyboard, which many users are accustomed to, is absent in VR, which leads to higher rates of input errors and frustration. Additionally, the use of passwords in VR requires users to navigate virtual keyboards, which can be clunky or unintuitive in some setups, further reducing their effectiveness.

Despite these challenges, the study emphasizes the potential for various approaches to be combined in ways that could improve both security and user experience in VR. For instance, the integration of biometric methods, such as facial recognition or voice authentication, could further bolster the security of these systems, complementing the smartphone-based methods discussed in the research. Additionally, allowing users to choose their preferred method of authentication could improve accessibility and adoption rates, making VR platforms more user-friendly and secure.

The findings from this research suggest that while two-step authentication in VR presents unique challenges, the methods explored have substantial potential to enhance security without compromising user experience. Further exploration is encouraged, particularly in refining these methods to increase usability, develop more advanced authentication systems, and ensure they are adaptable to the varying needs of users across different VR environments. As VR technology continues to evolve, the development of secure and intuitive authentication systems will be essential in creating safe and engaging virtual worlds for users.

Bibliography

[1] Jaybie A. De Guzman, Kanchana Thilakarathna, and Aruna Seneviratne. Security and privacy approaches in mixed reality: A literature survey. *ACM Comput. Surv.*, 52(6), oct 2019. https://doi.org/10.1145/3359626.

[2] DeepAI.org. Ai image generator. Machine Learning model, Text to Image. `https://deepai.org/machine-learning-model/text2img`. (Accessed on 04/10/2024).

[3] Nicholas J Wade. Wheatstone and the origins of moving stereoscopic images. *Perception*, 41(8):901–924, 2012. PMID: 23362669, https://doi.org/10.1068/p7270.

[4] Dimitris Chatzopoulos, Carlos Bermejo, Zhanpeng Huang, and Pan Hui. Mobile augmented reality survey: From where we are to where we go. *IEEE Access*, 5:6917–6950, 2017. 10.1109/ACCESS.2017.2698164.

[5] Fabio Arena, Mario Collotta, Giovanni Pau, and Francesco Termine. An overview of augmented reality. *Computers*, 11(2), 2022. https://www.mdpi.com/2073-431X/11/2/28.

[6] Jeffrey H. Shuhaiber. Augmented Reality in Surgery. *Archives of Surgery*, 139(2):170–174, 02 2004. https://doi.org/10.1001/archsurg.139.2.170.

[7] Hsin-Kai Wu, Silvia Wen-Yu Lee, Hsin-Yi Chang, and Jyh-Chong Liang. Current status, opportunities and challenges of augmented reality in education. *Computers & Education*, 62:41–49, 2013.

[8] Klen Čopič Pucihar and Paul Coulton. Exploring the evolution of mobile augmented reality for future entertainment systems. *Comput. Entertain.*, 11(2), jan 2015. https://doi.org/10.1145/2582179.2633427.

[9] Pooya Soltani and Antoine H.P. Morice. Augmented reality tools for sports education and training. *Computers & Education*, 155:103923, 2020. https://doi.org/10.1016/j.compedu.2020.103923.

[10] Mayumi Takaya, Yusuke Tsuruta, and Akihiro Yamamura. Reverse turing test using touchscreens and captcha. *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, 4(3):41–57, 2013.

[11] C. E. Landwehr. Cybersecurity and artificial intelligence: From fixing the plumbing to smart water. *IEEE Security & Privacy*, 6(05):3–4, sep 2008. 10.1109/MSP.2008.113.

[12] Md. Al-Hasan, Kaushik Deb, and Mohammad Obaidur Rahman. User-authentication approach for data security between smartphone and cloud. In *Ifost*, volume 2, pages 2–6. IEEE, 2013.

[13] Pedro Flores. Digital simulation in the virtual world: Its effect in the knowledge and attitude of students towards cybersecurity. In *2019 Sixth HCT Information Technology Trends (ITT)*, pages 1–5, 2019.

[14] Mubarak Al-Hadadi and Ali Al Shidhani. Smartphone security awareness: Time to act. In *2013 International Conference on Current Trends in Information Technology (CTIT)*, pages 166–171. IEEE, 2013.

[15] A. Henrysson and M. Ollila. Augmented reality on smartphones. In *2003 IEEE International Augmented Reality Toolkit Workshop*, pages 27–28, 2003. 10.1109/ART.2003.1320421.

[16] Ioanna Anastasaki, George Drosatos, George Pavlidis, and Konstantinos Rantos. User authentication mechanisms based on immersive technologies: A systematic review. *Information*, 14(10), 2023. https://www.mdpi.com/2078-2489/14/10/538.

[17] Alexios Mylonas, Stelios Dritsas, Bill Tsoumas, and Dimitris Gritzalis. Smartphone security evaluation the malware attack case. In *Proceedings of the International Conference on Security and Cryptography*, pages 25–36, 2011.

[18] Tim Dörflinger, Anna Voth, Juliane Krämer, and Ronald Fromm. “my smartphone is a safe!” the user’s point of view regarding novel authentication methods and gradual security levels on smartphones. In *2010 International Conference on Security and Cryptography (SECRYPT)*, pages 1–10, 2010.

[19] Tae Oh, Bill Stackpole, Emily Cummins, Carlos Gonzalez, Rahul Ramachandran, and Shinyoung Lim. Best security practices for android, blackberry, and ios. In *2012 The First IEEE Workshop on Enabling Technologies for Smartphone and Internet of Things (ETSIoT)*, pages 42–47, 2012.

[20] Irina V. Mashkina, Murat B. Guzairov, Vladimir I. Vasilyev, Liliya R. Tuliganova, and Andrei S. Konovalov. Issues of information security control in virtualization segment of company information system. In *2016 XIX IEEE International Conference on Soft Computing and Measurements (SCM)*, pages 161–163, 2016.

[21] Sarina Dastgerdy. Virtual reality and augmented reality security: A reconnaissance and vulnerability assessment approach, 2024. https://arxiv.org/abs/2407.15984.

[22] Ken Reese. Evaluating the usability of two-factor authentication. In *Evaluating the Usability of Two-Factor Authentication*, 2018. `https://www.proquest.com/openview/14d13b58170d9cd0687bceaf0fef3727/1?cbl=18750&diss=y&pq-origsite=gscholar`.

[23] Kiron Lebeck, Kimberly Ruth, Tadayoshi Kohno, and Franziska Roesner. Securing augmented reality output. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 320–337, 2017.

[24] Klaus-Tycho Foerster, Alex Gross, Nino Hail, Jara Uitto, and Roger Wattenhofer. Spareeye: enhancing the safety of inattentionally blind smartphone users. In *Proceedings of the 13th International Conference on Mobile and Ubiquitous Multimedia*, MUM '14, page 68–72, New York, NY, USA, 2014. Association for Computing Machinery.

[25] Jonas Blattgerste, Patrick Renner, and Thies Pfeiffer. Advantages of eye-gaze over head-gaze-based selection in virtual and augmented reality under varying field of views. In *Proceedings of the Workshop on Communication by Gaze Interaction*, COGAIN '18, New York, NY, USA, 2018. Association for Computing Machinery. 0.1145/3206343.3206349.

[26] Monique Santoso and Jeremy N. Bailenson. How video passthrough headsets influence perception of self and others. `https://synthical.com/article/80bb7b74-6dd3-4af3-92cc-e24edcd95ec6`, 6 2024.

[27] Jan Egger, Christina Gsaxner, Gijs Luijten, Jianxu Chen, Xiaojun Chen, Jiang Bian, Jens Kleesiek, and Behrus Puladi. Is the apple vision pro the ultimate display? a first perspective and survey on entering the wonderland of precision medicine. *JMIR Serious Games*, 12:e52785, Sep 2024.

[28] David Nahon, Geoffrey Subileau, and Benjamin Capel. "never blind vr" enhancing the virtual reality headset experience with augmented virtuality. In *2015 IEEE Virtual Reality (VR)*, pages 347–348, 2015.

[29] Taejin Ha, Steven Feiner, and Woontack Woo. Wearhand: Head-worn, rgb-d camera-based, bare-hand user interface with visually enhanced depth perception. In *2014 IEEE International Symposium on Mixed and Augmented Reality (ISMAR)*, pages 219–228, 2014.

[30] Taejin Ha and Woontack Woo. Arwand: Phone-based 3d object manipulation in augmented reality environment. In *2011 International Symposium on Ubiquitous Virtual Reality*, pages 44–47, 2011.

[31] Shaishav Siddhpuria, Sylvain Malacria, Mathieu Nancel, and Edward Lank. Pointing at a distance with everyday smart devices. In *Proc. CHI*, pages 1–11, NY, USA, 2018. Association for Computing Machinery, Inc.

[32] W. Lorensen, H. Cline, C. Nafis, R. Kikinis, D. Altobelli, and L. Gleason. Enhancing reality in the operating room. In *Proceedings Visualization '93*, pages 410–415, 1993. 10.1109/VISUAL.1993.398902.

[33] Robert Biddle, Sonia Chiasson, and P.C. Van Oorschot. Graphical passwords: Learning from the first twelve years. *ACM Comput. Surv.*, 44(4), sep 2012. https://doi.org/10.1145/2333112.2333114.

[34] Mariana-Daniela González-Zamar and Emilio Abad-Segura. Implications of virtual reality in arts education: Research analysis in the context of higher education. *Education Sciences*, 10(9), 2020.

[35] H. Creagh. Cave automatic virtual environment. In *Proceedings: Electrical Insulation Conference and Electrical Manufacturing and Coil Winding Technology Conference (Cat. No.03CH37480)*, pages 499–504, 2003.

[36] Rick Van Krevelen. Augmented reality: Technologies, applications, and limitations. 04 2007.

[37] Peter Casey, Ibrahim Baggili, and Ananya Yarramreddy. Immersive virtual reality attacks and the human joystick. *IEEE Transactions on Dependable and Secure Computing*, PP:1–1, 03 2019.

[38] Joe Durbin. Oculus sensors are technically hackable webcams. *The Guardian*, 2017. https://www.uploadvr.com/hackable-webcam-oculus-sensor-be-aware/.

[39] E Biermann, E Cloete, and L.M Venter. A comparison of intrusion detection systems. *Computers & Security*, 20(8):676–683, 2001. https://www.sciencedirect.com/science/article/pii/S0167404801008069.

[40] S S Tirumala, Maheswara Rao Valluri, and GA Babu. A survey on cybersecurity awareness concerns, practices and conceptual measures. In *2019 International Conference on Computer Communication and Informatics (ICCCI)*, pages 1–6, 2019.

[41] Charlie Chen, Ruey-Shiang Shaw, and s Yang. Mitigating information security risks by increasing user security awareness: A case study of an information security awareness system. *IT, Learning, and Performance Journal*, 24, 01 2006.

[42] George Hadjidemetriou, Marios Belk, Christos Fidas, and Andreas Pitsillides. Picture passwords in mixed reality: Implementation and evaluation. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI EA '19, page 1–6, New York, NY, USA, 2019. Association for Computing Machinery.

[43] ChatGPT. ChatGPT by openAI. Overview of modern authentication techniques and mechanisms. Retrieved from `https://chatgpt.com/`. (Accessed on 03/08/2024).

[44] Daniel Rupp, Philipp Grießer, Andrea Bonsch, and Torsten W. Kuhlen. Authentication in immersive virtual environments through gesture-based interaction with a virtual agent. In *2024 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*, pages 54–60, 2024.

[45] Tim Menzner, Alexander Otte, Travis Gesslein, Jens Grubert, Philipp Gagel, and Daniel Schneider. A capacitive-sensing physical keyboard for vr text entry. In *2019 IEEE Conference on Virtual Reality and 3D User Interfaces (VR)*, pages 1080–1081, 2019.

[46] Ahmed Arif and Wolfgang Stuerzlinger. Analysis of text entry performance metrics. pages 100 – 105, 10 2009.

[47] Chandra Hermawan Heruatmadja, Meyliana, Achmad Nizar Hidayanto, and Harjanto Prabowo. Biometric as secure authentication for virtual reality environ-

ment: A systematic literature review. In *2023 International Conference for Advancement in Technology (ICONAT)*, pages 1–7, 2023.

[48] Uwe Gruenefeld Jonathan Liebers, Sascha Brockel and Stefan Schneegass. Identifying users by their hand tracking data in augmented and virtual reality. *International Journal of Human–Computer Interaction*, 40(2):409–424, 2024.

[49] Thorben Ortmann. Towards facial expression recognition in immersive virtual reality with emojirain. In *2023 11th International Conference on Affective Computing and Intelligent Interaction Workshops and Demos (ACIIW)*, pages 1–5, 2023.

[50] Chi Lin and Mohammad S. Obaidat. *Behavioral Biometrics Based on Human-Computer Interaction Devices*, pages 189–209. Springer International Publishing, Cham, 2019. https://doi.org/10.1007/978-3-319-98734-7_7.

[51] Yunji Liang, Sagar Samtani, Bin Guo, and Zhiwen Yu. Behavioral biometrics for continuous authentication in the internet-of-things era: An artificial intelligence perspective. *IEEE Internet of Things Journal*, 7(9):9128–9143, 2020.

[52] Simon Eberz, Kasper B. Rasmussen, Vincent Lenders, and Ivan Martinovic. Evaluating behavioral biometrics for continuous authentication: Challenges and metrics. In *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, ASIA CCS '17, page 386–399, New York, NY, USA, 2017. Association for Computing Machinery.

[53] P.M. Rodwell, S.M. Furnell, and P.L. Reynolds. A non-intrusive biometric authentication mechanism utilising physiological characteristics of the human head. *Computers & Security*, 26(7):468–478, 2007.

[54] Sevasti Karatzouni. Non-intrusive continuous user authentication for mobile devices, 2014. `https://doi.org/10.24382/3299`.

[55] Poonam Rangnath Dholi and K. P. Chaudhari. Typing pattern recognition using keystroke dynamics. In Vinu V. Das and Yogesh Chaba, editors, *Mobile Communication and Power Engineering*, pages 275–280, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

[56] Nazirah Abd Hamid, Suhailan Safei, Siti Dhalila Mohd Satar, Suriayati Chuprat, and Rabiah Ahmad. Mouse movement behavioral biometric systems. In *2011 International Conference on User Science and Engineering (i-USEr)*, pages 206–211, 2011.

[57] Napa Sae-Bae, Nasir Memon, and Katherine Isbister. Investigating multi-touch gestures as a novel biometric modality. In *2012 IEEE Fifth International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, pages 156–161, 2012.

[58] Mohammed Abuhamad, Ahmed Abusnaina, Daehun Nyang, and David Mohaisen. Sensor-based continuous authentication of smartphones' users using be-

havioral biometrics: A contemporary survey. *IEEE Internet of Things Journal*, 8(1):65–84, 2021.

[59] Pınar Kürtünlüoğlu, Beste Akdik, Reyhan Duygu, and Enis Karaarslan. Towards more secure virtual reality authentication for the metaverse: A decentralized method proposal. In *2023 16th International Conference on Information Security and Cryptology (ISCTürkiye)*, pages 1–6, 2023.

[60] Yuxuan Huang, Danhua Zhang, and Evan Suma Rosenberg. Dba: Direction-based authentication in virtual reality. In *2023 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*, pages 953–954, 2023.

[61] Daniel Bologna, Vincenzo Micciché, Giovanni Violo, Alessandro Visconti, Alberto Cannavò, and Fabrizio Lamberti. Sphinx authentication technique: Secure painting authentication in extended reality. In *2023 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*, pages 941–942, 2023.

[62] Sarah J. Andrabi, Michael K. Reiter, and Cynthia Sturton. Usability of augmented reality for revealing secret messages to users but not their devices. In *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security*, SOUPS '15, page 89–102, USA, 2015. USENIX Association.

[63] Amit P. Desai, Lourdes Pena-Castillo, and Oscar Meruvia-Pastor. A window to your smartphone: Exploring interaction and communication in immersive vr with augmented virtuality. In *2017 Computer And Robot Vision (CRV) Conf. Proc.*, Edmonton, AB, March 2015.

[64] Ghassem Alaee, Amit P. Deasi, Lourdes Pena-Castillo, Edward Brown, and Oscar Meruvia-Pastor. A user study on augmented virtuality using depth sensing cameras for near-range awareness in immersive vr. In *IEEE VR's 4th Workshop on Everyday Virtual Reality (WEVR 2018), IEEE, 2018*. Institute of Electrical and Electronics Engineers Inc., 3 2018.

[65] Peter Mohr, Markus Tatzgern, Tobias Langlotz, Andreas Lang, Dieter Schmalstieg, and Denis Kalkofen. Trackcap: Enabling smartphones for 3D interaction on mobile head-mounted displays. In *Proc. CHI*, NY, USA, 2019. Association for Computing Machinery, Inc.

[66] Keisuke Hattori and Tatsunori Hirai. Inside-out tracking controller for vr/ar hmd using image recognition with smartphones. In *ACM SIGGRAPH 2020 Posters, SIGGRAPH 2020*. Association for Computing Machinery, 8 2020. `https://doi.org/10.1145/3388770.3407430`.

[67] Li Zhang, Weiping He, Huidong Bai, Jun He, Yiyue Qiao, and Mark Billinghurst. A hybrid 2D-3D tangible interface for virtual reality. In *Proc. SIGGRAPH*, NY, USA, 2021. ACM.

[68] Huidong Bai, Li Zhang, Jing Yang, and Mark Billinghurst. Bringing full-featured mobile phone interaction into virtual reality. *Computers and Graphics (Pergamon)*, 97:42–53, jun 2021. 10.1016/j.cag.2021.04.004.

[69] Arda Ege Unlu and Robert Xiao. PAIR: Phone as an augmented immersive reality controller. In *Proc. VRST*, pages 1–6, NY, USA, 2021. Association for Computing Machinery, Inc. 10.1145/3489849.3489878.

[70] Krzysztof Pietroszek, Anastasia Kuzminykh, James R. Wallace, and Edward Lank. Smartcasting: A discount 3D interaction technique for public displays. In *Proc. OzCHI*, pages 119–128, NY, USA, 2014. Association for Computing Machinery, Inc.

[71] Sahar A. Aseeri, Daniel Acevedo-Feliz, and Jurgen Schulze. Poster: Virtual reality interaction using mobile devices. In *IEEE Symposium on 3D User Interface 2013, 3DUI 2013 - Proceedings*, pages 127–128, 2013. `https://doi.org/10.1109/3DUI.2013.6550211`.

[72] Rahul Budhiraja, Gun A. Lee, and Mark Billinghurst. Interaction techniques for hmd-hhd hybrid ar systems. In *2013 IEEE International Symposium on Mixed and Augmented Reality, ISMAR 2013*, pages 243–244, 2013. `https://doi.org/10.1109/ISMAR.2013.6671786`.

[73] Brianna McDonald, Qingyu Zhang, Aiur Nanzatov, Lourdes Peña-Castillo, and Oscar Meruvia-Pastor. Smartvr pointer: Using smartphones and gaze orien-

tation for selection and navigation in virtual reality. *Sensors*, 24(16), 2024. https://www.mdpi.com/1424-8220/24/16/5168.

[74] Fengyuan Zhu, Mauricio Sousa, Ludwig Sidenmark, and Tovi Grossman. Phoneinvr: An evaluation of spatial anchoring and interaction techniques for smartphone usage in virtual reality. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, CHI '24, New York, NY, USA, 2024. Association for Computing Machinery.

[75] Stefan Schneegass, Youssef Oualil, and Andreas Bulling. Skullconduct: Biometric user identification on eyewear computers using bone conduction through the skull. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI '16, page 1379–1384, New York, NY, USA, 2016. Association for Computing Machinery.

Appendices

Appendix A

Research Ethics Board Approval letter

MEMORIAL
UNIVERSITY

Interdisciplinary Committee on
Ethics in Human Research (ICEHR)

St. John's, NL Canada A1C 5S7
Tel: 709 864-2561 icehr@mun.ca
www.mun.ca/research/ethics/humans/icehr

ICEHR Number:	**20231802-SC**
Approval Period:	May 12, 2023 – May 31, 2024
Funding Source:	
Responsible Faculty:	Dr. Oscar Meruvia-Pastor Department of Computer Science
Title of Project:	*Two-step authentication in VR using Near-Range Extended Reality*

May 12, 2023

Aiur Nanzatov
Department of Computer Science, Faculty of Science
Memorial University

Dear Aiur Nanzatov:

Thank you for your correspondence addressing the issues raised by the Interdisciplinary Committee on Ethics in Human Research (ICEHR) for the above-named research project. ICEHR has re-examined the proposal with the clarifications and revisions submitted, and is satisfied that the concerns raised by the Committee have been adequately addressed. In accordance with the *Tri-Council Policy Statement on Ethical Conduct for Research Involving Humans (TCPS2)*, the project has been granted *full ethics clearance* for **one year**. ICEHR approval applies to the ethical acceptability of the research, as per Article 6.3 of the *TCPS2*. Researchers are responsible for adherence to any other relevant University policies and/or funded or non-funded agreements that may be associated with the project. If funding is obtained subsequent to ethics approval, you must submit a Funding and/or Partner Change Request to ICEHR so that this ethics clearance can be linked to your award.

The *TCPS2* **requires** that you **strictly adhere to the protocol and documents as last reviewed** by ICEHR. If you need to make additions and/or modifications, you must submit an Amendment Request with a description of these changes, for the Committee's review of potential ethical concerns, before they may be implemented. Submit a Personnel Change Form to add or remove project team members and/or research staff. Also, to inform ICEHR of any unanticipated occurrences, an Adverse Event Report must be submitted with an indication of how the unexpected event may affect the continuation of the project.

The *TCPS2* **requires** that you submit an Annual Update to ICEHR before **May 31, 2024**. If you plan to continue the project, you need to request renewal of your ethics clearance and include a brief summary on the progress of your research. When the project no longer involves contact with human participants, is completed and/or terminated, you are required to provide an annual update with a brief final summary and your file will be closed. All post-approval ICEHR event forms noted above must be submitted by selecting the ***Applications: Post-Review*** link on your Researcher Portal homepage. We wish you success with your research.

Yours sincerely,

James R Drover

James Drover, Ph.D.
Vice-Chair, Interdisciplinary Committee on
Ethics in Human Research

JD/bc
cc: Supervisor – Dr. Oscar Meruvia-Pastor, Department of Computer Science

Appendix B

Recruitment Letter

Call for Participants

Subject: Recruitment for Scientific Research Project on
Two-step authentication in VR using Near-Range Extended Reality

Hello,

My name is Aiur Nanzatov, I am a graduate student in the Master of Computer Science program at MUN. As part of my Master's Thesis, I am researching the topic of "Two-step authentication in VR using Near-Range Extended Reality" under the supervision of Dr. Oscar Meruvia-Pastor.

The research will be a user study, where participants will take part in two separate experiments:
First is navigation in VR environment using waypoints to teleport from one place to another and solving a Tetris-style key & lock challenge in VR.
The second one is to complete the virtual series of authentication challenges scenario using the selected Virtual Reality (VR) technology through a Head Mounted Device (HMD).
The participants will also be asked to complete a pre-simulation demographic questionnaire and two post-simulation questionnaires. The expected time for the study is about 60-90 minutes. Participants will spend about 20-30 minutes completing experiment 1, 30-45 minutes completing experiment 2, plus 10-15 minutes for instructions and feedback. Participants will be compensated $20 in the form of a gift card, for their time. The study will be conducted in the room EN-1045, Engineering Building, Department of Computer Science. Memorial University.

The study may cause motion sickness because of the Virtual Reality Head-Mounted Device use, which may result in fatigue, headache, discomfort, dizziness or nausea. Motion sickness will be monitored during the simulation. Participants who suffer symptoms after 30 minutes of having finished the experiment will be instructed to visit the Emergency Department, Student Wellness and Counselling Centre (https://www.mun.ca/studentwellness/) or NL's "Bridge the Gapp" resource (https://nl.bridgethegapp.ca/) for medical assessment. Therefore, please be advised of the potential symptoms. Do not volunteer for this study if you think this will be problematic for you.

If you are interested, please contact me to schedule an appointment for the study or schedule an appointment here:
https://calendly.com/aznanzatov/nrxr?month=2024-06

Experience with using VR is not required. Participation in the study will not be reported to professors, program administrators or employers. Also, all the equipment required for the experiment will be provided to you by the research team.

If you have any questions or would like further details, please visit the site https://www.cs.mun.ca/~aznanzatov/nrxr/ or contact me at aznanzatov@mun.ca or 1-709-687-0022.

The proposal for this research has been reviewed by the Interdisciplinary Committee on Ethics in Human Research and found to be in compliance with Memorial University's ethics policy. If you have ethical concerns about the research, such as the way you have been treated or your rights as a participant, you may contact the Chairperson of the ICEHR at icehr.chair@mun.ca or by telephone at 709-864-2861

Appendix C

Questionnaires

Code #:

Two-step authentication in VR using Near-Range Extended Reality

Pre-test

Please note that you may skip any questions that you do not wish to answer.

1. Occupation:

	Computer Science Undergraduate student
	Computer Science Graduate student
	Non-Computer Science Undergraduate student
	Non-Computer Science Graduate student
	Faculty
	Staff
	Alumni
	Prefer not to answer
	Other – please specify:

____

2. Age:

	Under 18
	18-24
	24-48
	48-65
	Over 65
	Prefer not to answer

3. Dominant hand:

	Left
	Right
	Ambidextrous
	Prefer not to answer

Code #:

4. Experience using Head-Mounted Devices (HMDs)?

	Never
	Less than one month
	1-6 months
	6 months – 2 years
	Over 2 years
	Prefer not to answer

5. Frequency of using Head-Mounted Devices (HMDs)?

	Daily
	Weekly
	Monthly
	Never
	Prefer not to answer
	Other:__________________________

6. Gender

	Male
	Female
	Prefer not to answer
	Another Gender Identity (optional to specify): _________________________

7. Please rate your degree of confidence in performing each of the following criteria related to navigation, interaction within 3D virtual scenes and smartphones. Rate your degree of confidence using the scale 0-100 (**0=cannot at all; 50=moderately can do; 100=highly certain can do**).

0	10	20	30	40	50	60	70	80	90	100
Cannot at all					Moderately can do					Highly certain can do

Abilities	**Confidence (0 – 100)**
1. Operate smartphone applications, video games, other smartphone software.	
2. Create, manipulate, adjust and manage smartphone passwords and passcodes	
3. Operate HMD interaction (controller, gamepad, mouse/keyboard).	
4. Interact with a virtual reality scene environment/objects.	
5. Navigate / move around a virtual reality scene.	
6. Identify and recognize user interface mechanisms and tooltips.	

Code #: ____________________

Two-step authentication in VR using Near-Range Extended Reality

Post-test

Please note that you may skip any questions that you do not wish to answer.

1. Please rate following symptoms after the Virtual Reality experience.

	Symptoms	None	Slight	Moderate	Severe
1)	General discomfort				
2)	Fatigue				
3)	Headache				
4)	Eye strain				
5)	Difficulty focusing				
6)	Increased salivation				
7)	Sweating				
8)	Nausea				
9)	Difficulty concentrating				
10)	Fullness of head				
11)	Blurred vision				
12)	Dizzy (eyes open)				
13)	Dizzy (eyes closed)				
14)	Vertigo				
15)	Stomach awareness				
16)	Burping				

Adapted from: Kennedy, R. S., Lane, N. E., Berbaum, K. S., & Lilienthal, M. G. (1993). Simulator sickness questionnaire: An enhanced method for quantifying simulator sickness. *The international journal of aviation psychology*, *3*(3), 203-220.

Code #: ____________________

2. Please rank the methods below by preference of use:

1)	Solving the challenges using the VR Controller to enter the code.	Least Preferred			Neutral			Most Preferred
		1	2	3	4	5	6	7
2)	Solving the challenges using the Smartphone to read the code only.	Least Preferred			Neutral			Most Preferred
		1	2	3	4	5	6	7
3)	Solving the challenges using the Smartphone to enter the code.	Least Preferred			Neutral			Most Preferred
		1	2	3	4	5	6	7

If you would like to comment on why you preferred a certain method(s), please write it here:

____

____

____

____

____

____

____

Code #: ____________________

3. Please enter any additional comments on what you liked about the different tasks and conditions of the experiment here:

____

____

____

____

____

4. Please enter any additional comments on what you disliked about the different tasks and conditions of the experiment here:

____

____

____

____

____

Appendix D

Informed Consent form

Informed Consent Form

Title: *Two-step authentication in VR using Near-Range Extended Reality*

Researcher(s): *Aiur Zhambalovich Nanzatov*

Department of Computer Science
Memorial University of Newfoundland
aznanzatov@mun.ca

Supervisor(s): *Dr. Oscar Meruvia-Pastor*
Department of Computer Science
Memorial University of Newfoundland
oscar@mun.ca

Co-Supervisor(s):

Collaborator(s): *Dr. Lourdes Pena-Castillo*
Department of Computer Science
Memorial University of Newfoundland
lourdes.pena@mun.ca

You are invited to take part in a research project entitled "Two-step authentication in VR using Near-Range Extended Reality".

This form is part of the process of informed consent. It should give you a basic idea of what the research is about and what your participation will involve. It also describes your right to withdraw from the study. To decide whether you wish to participate in this research study, you should understand enough about its risks and benefits to make an informed decision. This is the informed consent process. Take time to read this carefully and to understand the information given to you. Please contact the researcher, Aiur Nanzatov, if you have any questions about the study or would like more information before you consent.

It is entirely up to you to decide whether to take part in this research. If you choose not to participate in this research or decide to withdraw from the study once it has started, there will be no negative consequences for you, now or in the future.

Introduction:
I, Aiur Zhambalovich Nanzatov, am conducting this research as the Principal Investigator under the supervision of Dr. Oscar Meruvia-Pastor. This research is part of my Master's Program.

Virtual Reality (VR) is defined as ‘‘a computer-generated, interactive, three-dimensional environment in which a person is immersed”. Since the development of Virtual Reality about 15 years ago, technology has grown significantly. Besides Virtual Reality, other subsets of virtual technologies include Augmented Reality, Mixed Reality, and Augmented Virtuality. Virtual Reality is used in many different fields, such as gaming, architectural design, education, learning, medicine and more. Virtual, Mixed and Augmented Reality Systems (VMARs) are an emerging set of technologies being evaluated and adopted across various education disciplines. They typically involve the use of Virtual Reality and Head-Mounted Displays (HMD). VMARs have been shown to create an enhanced sense of presence and ‘immersion’. Near-range awareness is a technique which is incorporating the users’ personal mobile device within the field of view (FOV) inside the VR, i.e. while wearing an HMD. The recent proliferation of these technologies could create new learning opportunities to improve knowledge and skill retention and increase access to more secure, safe and simple solutions for information security professionals in authentication procedures.

Purpose of the study:

The proposed study will involve evaluating a SmartVR pointer mechanism that implements the utilization of a QR code which is displayed on the smartphone’s screen as a virtual reality environment navigation tool and further expanding it to an extended reality (XR) application for smartphone authentication using a separation of the password/authentication measure to two independent parts – first half of the password is visible/presented to user at the smartphone’s screen, while the second half is provided via head-mounted device (HMD). Thus, the task of combining the two halves into the complete password is only attainable to the person who possesses both parts of the password.

The objectives of this study are:

1. Investigate the most efficient and convenient ways of a two-step authentication password implementation.

2. Conduct an experiment to measure the designed application’s capabilities and features and compare such against current alternatives.

3. Examine the viability of the SmartVR Pointer solution as a navigation mechanism within the VR environment.

4. Examine the effectiveness of VR head-mounted devices usage in a two-step smartphone authentication system.

What you will do in this study:

As a participant you will take part in two separate experiments:

Experiment 1.

Task 1: Navigation in a VR environment which requires you to select teleporting waypoints to move from one place to another.

Task 2: Solving a Tetris-style key & lock challenge in VR. You will be asked to manipulate the 3D objects of different shapes in a way that the Tetris pieces are matching the requested pattern, using either controller or a smartphone as a pointer.

Experiment 2.

The goal of experiment 2 is to demonstrate the viability of Near-Range Extended Reality (NR XR) to implement two-step authentication and determine which method is the best preferred by users and which method is found easiest to use.

Here you will walk through the Viking Village, and we will give you some challenges you will need to solve using the smartphone.

You will be able to use gaze-based selection of teleporting points, which does not require QR code tracking.

The challenges are following:

Task 1: Authentication using captcha (also known as the CAPTCHA challenge).

Task 2: Authentication using a numeric keypad (also known as the keypad challenge).

Task 3: Authentication using a juxtaposition of grid elements (also known as the match-the-grids challenge).

Task 4: Visual Authentication using an passcode sequence (also known as the passcode challenge).

All equipment that will be required for the experiment will be provided to you by a research team. This includes a smartphone with application, head-mounted devices (HTC Vive and Meta Quest 2), VR controllers.

Data types gathered:

Data will be recorded in the text file format which will contain information about the measurements during experiment completion (such as attempt count, challenge completion time, number of clicks registered during the walkthrough and total completion time). This data will be measured automatically by the software.

Also, as a participant, you will complete three questionnaires: one “pre-test” and 2 “post-test” questionnaires (for both experiments). The “pre-test” questionnaire is a demographic questionnaire indicating characteristics such as gender, occupation, experience and confidence with virtual scene navigation and interaction, experience with smartphone and controller usage. This information will enable comparison and analysis of potential influences these characteristics may have on study outcomes. The “pre-test” questionnaire will be administered at the beginning of the session.

The “post-test” questionnaires will be administered after each experiment and will refer to your experience within the VR environment during the task completion.

Location of the study:
The study will be conducted in EN-1045 computer vision lab in Engineering Building, MUN

Length of time:
For both groups, the expected time for the study is around 60-90 minutes. Participants will spend about 20-30 minutes completing experiment 1, about 30-45 mins completing the experiment 2, and about 10-15 minutes for instructions and evaluation.

Withdrawal from the study:
A participant may withdraw at any point in the study for any reason, and without having to specify a reason. If the data gathered upon that point is not complete at the time of withdrawal, it will be removed. However, the data will not be automatically removed from the study if a participant withdraws after the numerical data gathering has been completed. Upon withdrawal the participants will be asked if they would request to remove their data if requested within 1 week of completing the experimental sessions.

During the training session, if a participant reports motion sickness, the participant will be asked to answer a Simulation Sickness Questionnaire (SSQ). The questionnaire allows participants to rate the severity of their symptoms as no symptoms, minimal, moderate, and severe. Participants will complete the survey at any point they report experiencing motion sickness.

Possible benefits:

a) For participants: The benefits for participants in the study is that they will have first-hand exposure to the Near-Range awareness for augmented virtuality usage, while also increasing their overall experience in the Virtual/Augmented Reality and authentication techniques and approaches. They will also learn the type of experimentation needs to be performed for validating scientific research.
b) For the scientific community: The research and software development outcomes will be beneficial to the AR/VR and information security industries. Proposed methods may provide information security professionals with an authentication model to enhance the safety and security of existing approaches, as well as creation of new ones, involving Near-Range awareness and splitting the password into two separate parts as an additional security measure for HMD and smartphone utilization. Moreover, this project provides a possibility of better VR immersion effect with cameras projecting the real world’s objects into the virtual scene directly.

Possible risks:

Head-Mounted Display's (HMD's) use for an extended period may cause some participants to experience motion sickness or simulation sickness. Participants suffering from motion sickness can feel fatigued, headache, discomfort, difficulty focusing, dizziness or nausea. To ensure that participants do not experience severe motion sickness symptoms, participants will be asked to answer Simulator Sickness Questionnaire (SSQ) at various time points, as described above in Section "Withdrawal from the study". Also, as a precautionary step, the participant's exposure time to the virtual environment for each task will be limited to 30 minutes and break time will be allocated between tasks to allow participants to rest. If the symptoms persist, participants will be instructed rest in the lab or remain on campus until the symptoms subdue. If the symptoms still persist after 30 minutes of having finished the experiment, participants will be instructed to visit the Emergency Department at the Health Sciences Centre (General Hospital) (https://emergency.easternhealth.ca/emergency-departments/#STJ), Student Wellness and Counselling Centre (https://www.mun.ca/studentwellness/, (available to Memorial University students only), or NL's "Bridge the Gapp" resource (https://nl.bridgethegapp.ca/) for medical assessment. Participants are advised of the potential symptoms. Participants are asked not to volunteer for this study if this will be problematic for them.

Health Sciences Centre contact information:

Health Sciences Centre (General Hospital)
Emergency Department: 709-777-6300
300 Prince Philip Drive, St. John's, NL

Another potential risk that we can think about is that some participants might feel upset or frustrated if they cannot complete the tasks. To reduce the anxiety, participants will be assured that they do not need to feel an obligation to complete the experiment.

Confidentiality:

During this study, no information about participants' identity will be used either during the analysis of the data or the release of the findings. The participants' names or identifying information will be recorded in the informed consent form, which will be kept confidential. The participants will be assigned a random identification numbers in the internal computer systems, statistical analysis and in the release of the findings. These identification numbers will be recorded on the questionnaires instead of the participants name to keep confidentiality. These identification numbers with corresponding participant names will be stored in a document. The principal investigator, Aiur Nanzatov, will have access to this document. This is only to allow for data to be removed, if a participant requests within the given time limit, after the completion of the experiment. Other than this situation, the information gathered in the document will not be used to identify the data set with the participant. All the team members listed above will have access to the coded data without participant identifications, for analysis and interpretation.

Upon completion of the study the informed consent forms and completed surveys will be archived in the office of the Principal Supervisor. These forms will be kept for a minimum of five years and will be destroyed after that. All data will be retained for a minimum of five years, after which the data will be purged from the drive.

Anonymity:

Participant's identity will be kept coded, and results will only be reported in aggregate. Also, the feedback form which the participants will complete after the experiment will not be anonymous and will include their names but the quotes from such forms will be anonymized.

During the experiment photographs of participants will be made, for the purposes of illustration of the experimental apparatus and functionality for potential use in publications. Thus, although participant's face will mostly be covered by the HMD, it may still be possible to identify some participants on the photographs, which affects the degree of anonymity.

Storage of Data:

Upon completion of the study the informed consent forms and completed surveys will be archived in the office of the Principal Supervisor. These forms will be kept for a minimum of five years and will be destroyed after that.

Reporting of Results:

The study results, observations and conclusions will be included in the thesis and associated publications. The thesis will be publicly available and can be accessed through the QEII thesis collection URL: https://www.library.mun.ca/qeii/aboutus/qeiicollections/. None of the personal identification details of the participants will be mentioned anywhere in the thesis. Results will also only be reported in aggregate.

Sharing of Results with Participants:

The study results, observations and conclusions will be included in the thesis and associated publications. After the results are published an email with a link to the published results, will be sent out to only those participants who wish to receive the published results and provided explicit consent to receive emails in the consent form.

Questions:

You are welcome to ask questions at any time before, during, or after your participation in this research. If you would like more information about this study, please contact:

Aiur Nanzatov, Email: aznanzatov@mun.ca,

Dr. Oscar Meruvia-Pastor, Email: oscar@mun.ca

Note:

The proposal for this research has been reviewed by the Interdisciplinary Committee on Ethics in Human Research and found to be in compliance with Memorial University's ethics policy. If you have ethical concerns about the research, such as the way you have been treated or your rights as a participant, you may contact the Chairperson of the ICEHR at icehr@mun.ca or by telephone at 709-864-2861.

Consent:

Your signature on this form means that:

- You have read the information about the research.
- You have been able to ask questions about this study.
- You are satisfied with the answers to all your questions.
- You understand what the study is about and what you will be doing.
- You understand that you are free to withdraw participation in the study without having to give a reason, and that doing so will not affect you now or in the future.
- You understand that if you choose to end participation **during** data collection, any data collected from you up to that point will be destroyed.
- You understand that your data is not being collected anonymously but it will be anonymized after collection, and you have 1 week to request to remove your data from the study.
- Your information will be kept confidential and all identifying factors will be removed in the analysis and distribution of the results.

Noting that most of my face will be covered by the HMD, I agree to be photographed for the purpose of illustrating the experimental setup and potential use in publications. □ Yes □ No

I agree to the use of direct quotations □ Yes □ No

By signing this form, you do not give up your legal rights and do not release the researchers from their professional responsibilities.

Your signature confirms:

□ I have read what this study is about and understood the risks and benefits. I have had adequate time to think about this and had the opportunity to ask questions and my questions have been answered.

□ I agree to participate in the research project understanding the risks and contributions of my participation, that my participation is voluntary, and that I may end my participation.

□ A copy of this Informed Consent Form has been given to me for my records.

Email Consent

Would you like to receive a copy of the published result of this research? □ Yes □ No

If yes, please provide your email address ____

Signature of participant Date

Researcher's Signature:
I have explained this study to the best of my ability. I invited questions and gave answers. I believe that the participant fully understands what is involved in being in the study, any potential risks of the study and that he or she has freely chosen to be in the study.

Signature of Principal Investigator Date

Appendix E

Figures

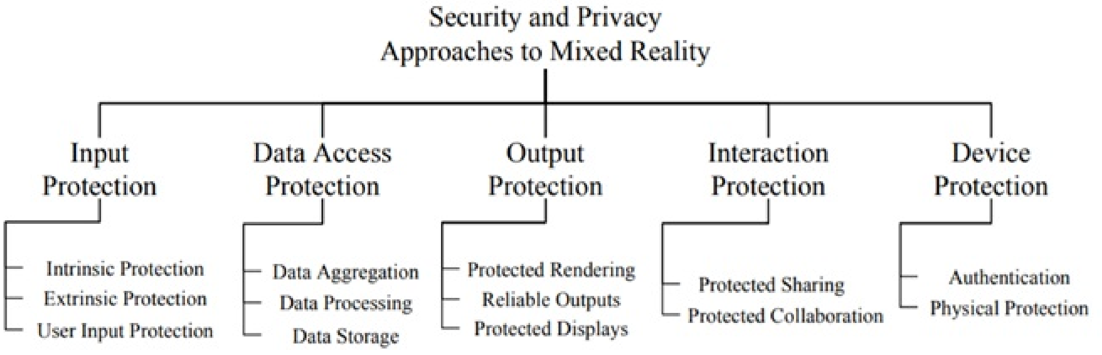
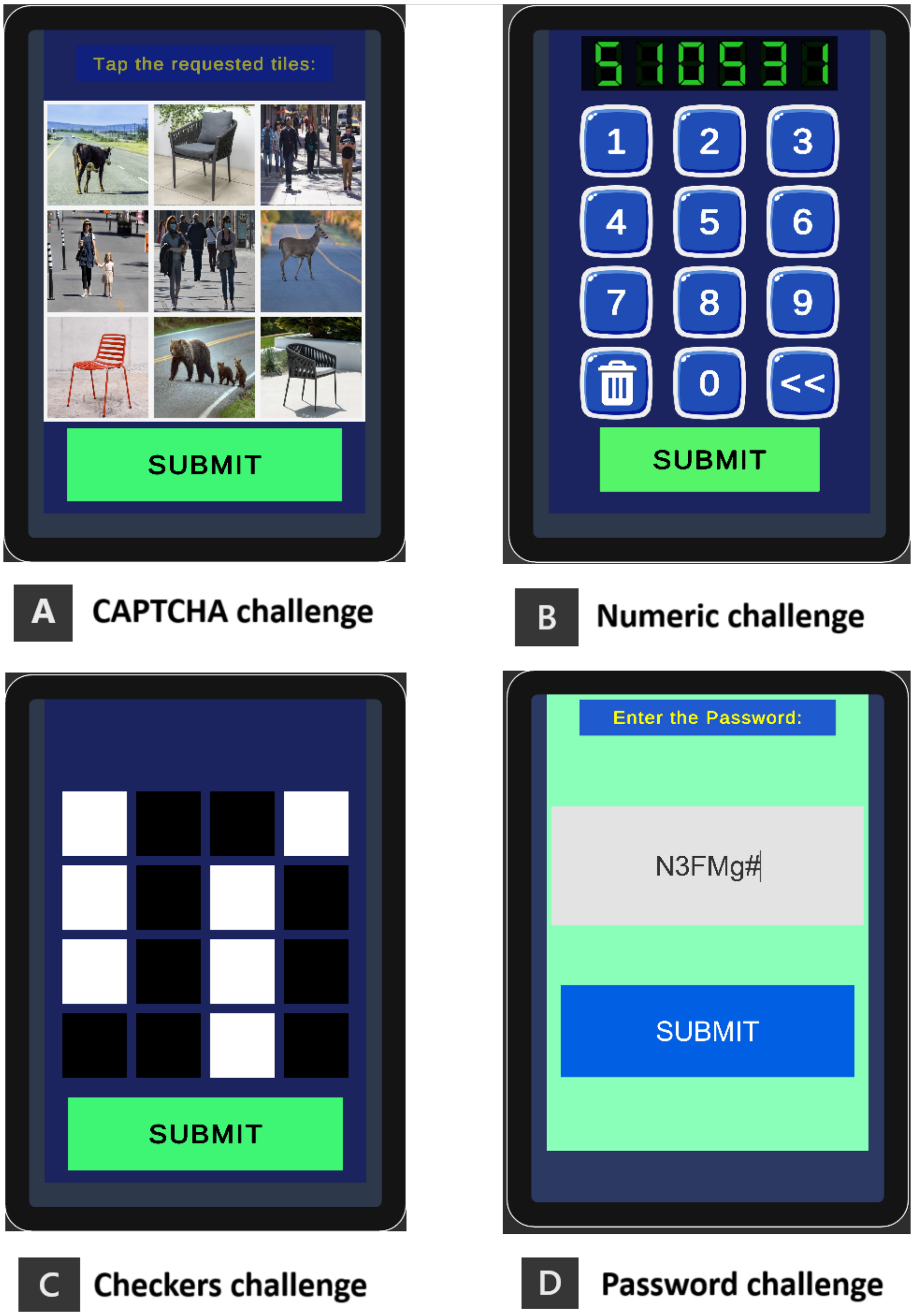


Figure E.1: General approaches in VR/AR application to Security and Privacy by De Guzman et al.



A CAPTCHA challenge

B Numeric challenge

C Checkers challenge

D Password challenge

Figure E.2: An overview of the authentication methods

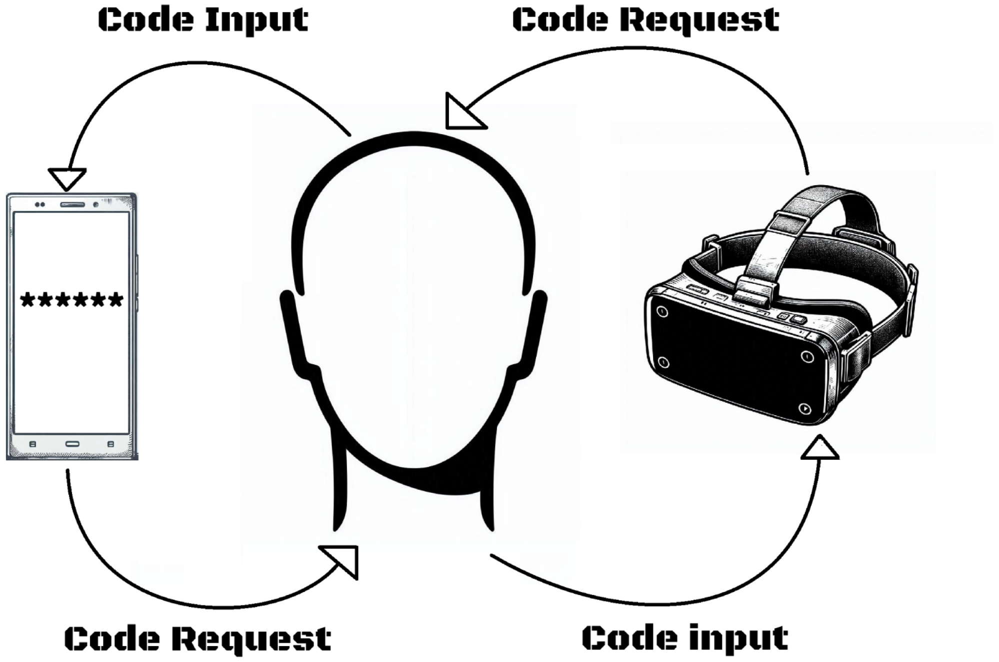


Figure E.3: Variations of code request and code input from the smartphone/headset

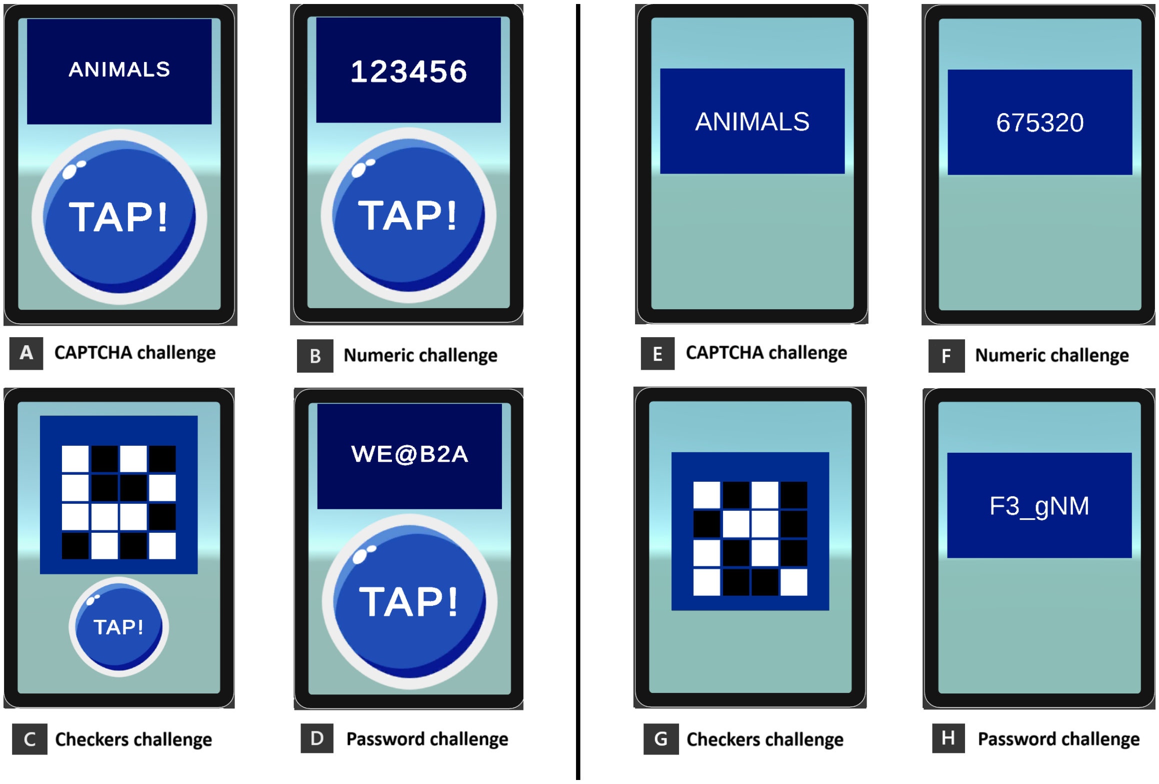


Figure E.4: Conditions 2 and 3 requests from the smartphone's screen.

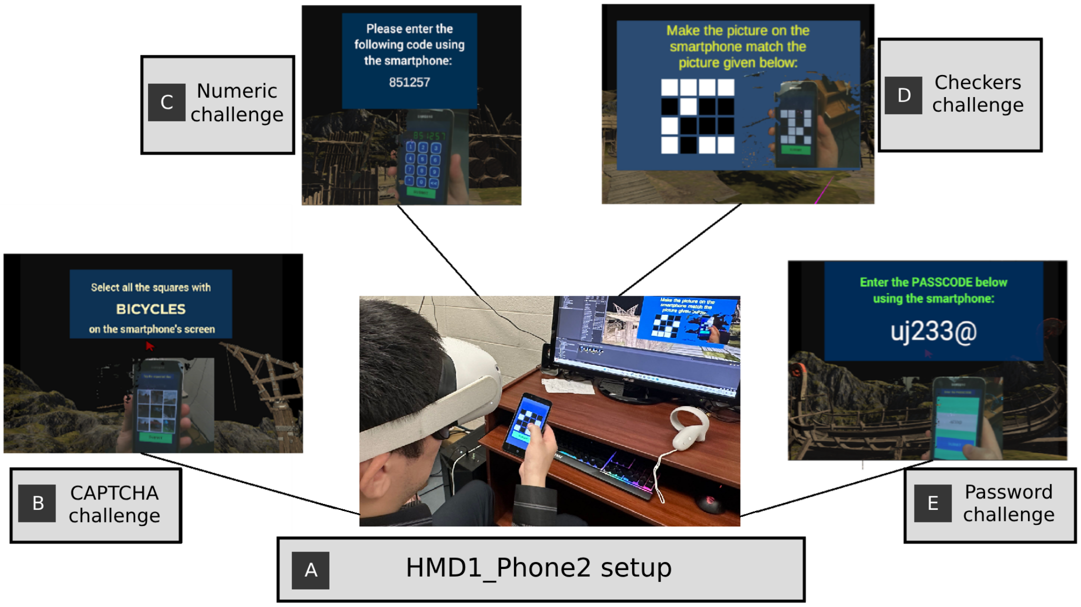

C Numeric challenge
Please enter the following code using the smartphone:
851257
Make the picture on the smartphone match the picture given below:
D Checkers challenge
Select all the squares with
BICYCLES
on the smartphone's screen
Enter the PASSCODE below using the smartphone:
uj233@
B CAPTCHA challenge
E Password challenge
A HMD1_Phone2 setup

Figure E.5: Condition 1 Overview with all possible interactions.

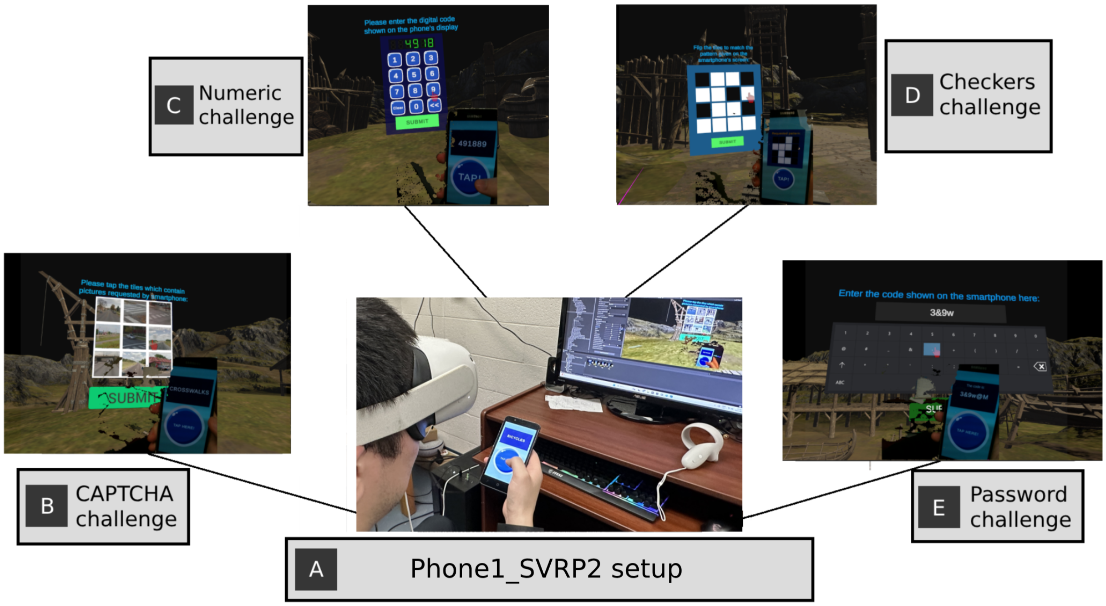

C Numeric challenge
Please enter the digital code shown on the phone's display
491889
TAP!
D Checkers challenge
B CAPTCHA challenge
Please tap the tiles which contain pictures requested by smartphone:
SUBMIT
CROSSWALKS
Enter the code shown on the smartphone here:
3&9w
E Password challenge
A Phone1_SVRP2 setup

Figure E.6: Condition 2 Overview with all possible interactions.

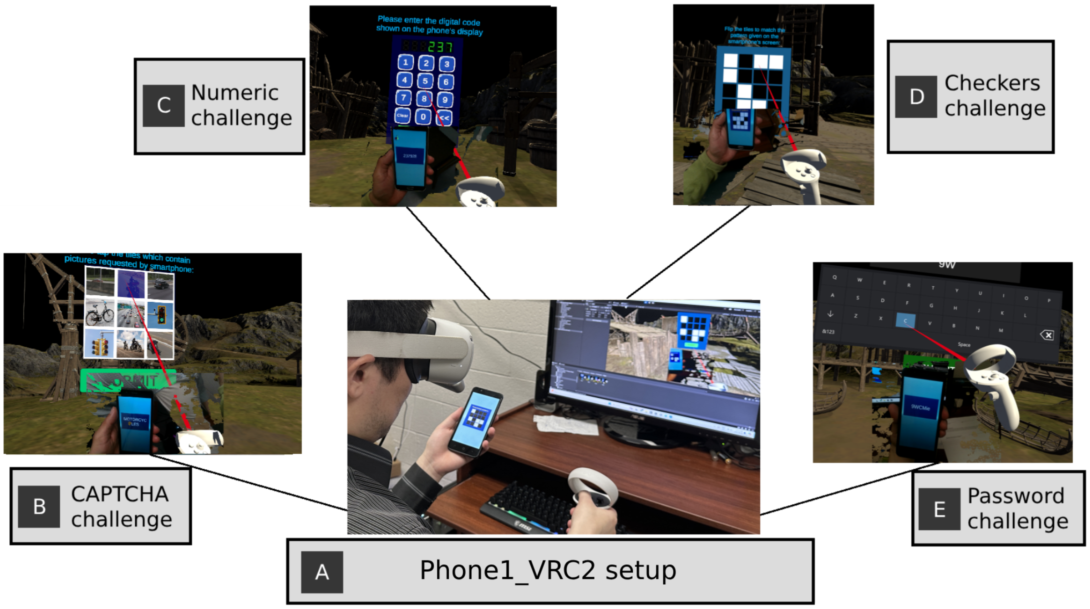
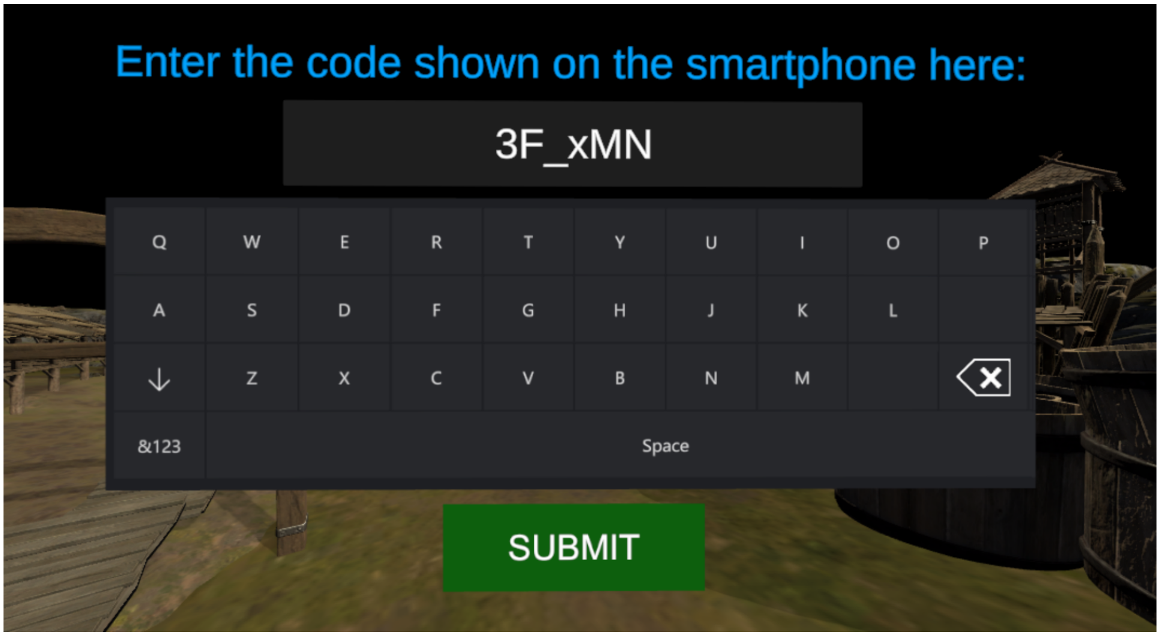


Figure E.7: Condition 3 Overview with all possible interactions.



Enter the code shown on the smartphone here:

3F_xMN

Figure E.8: Virtual Keyboard in the VR environment, utilized during the Password challenge in conditions 2 and 3.

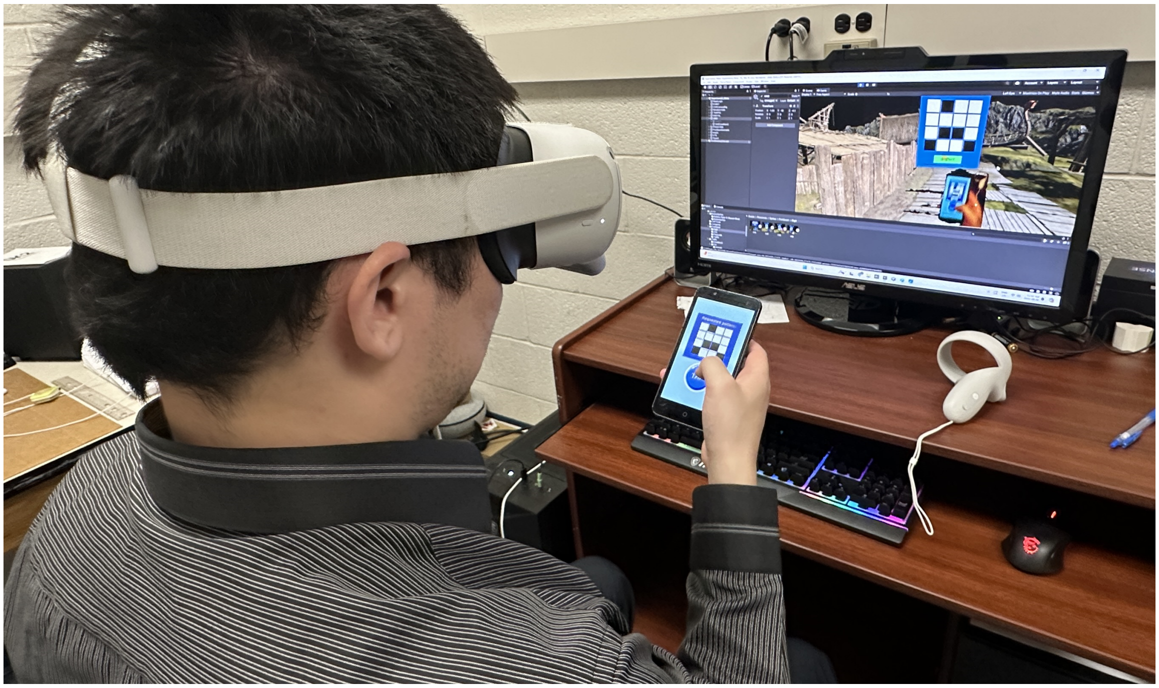


Figure E.9: Experimental Setup: In Condition 2, the participant holds the mobile device in front of the camera attached to the HMD. The participant is required to input the code requested by the mobile device within the VR environment.

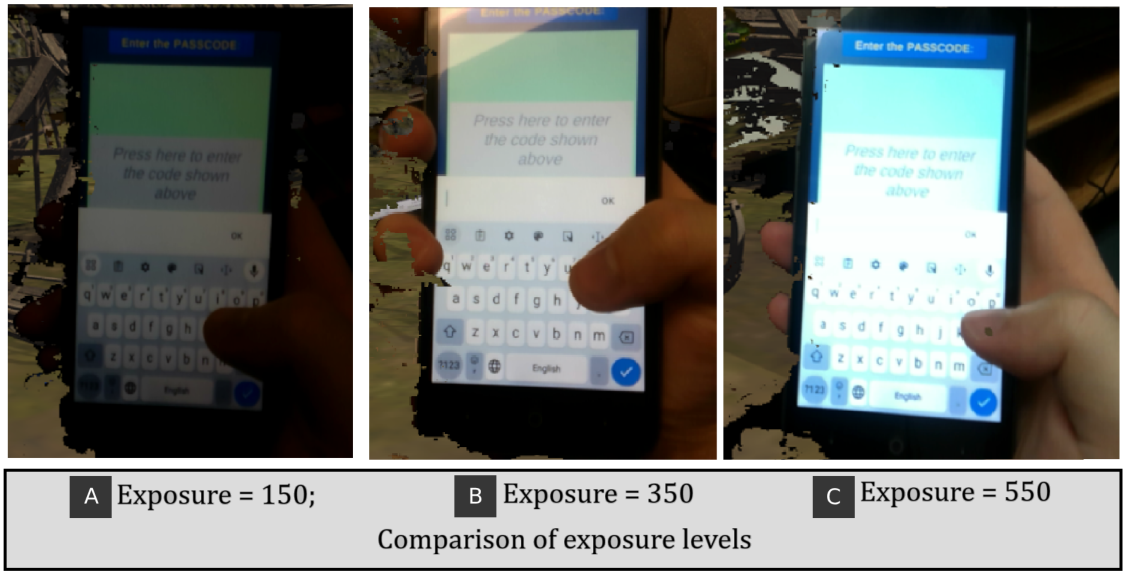


Figure E.10: Different customizable levels of exposure for the keyboard and input field to be visible.

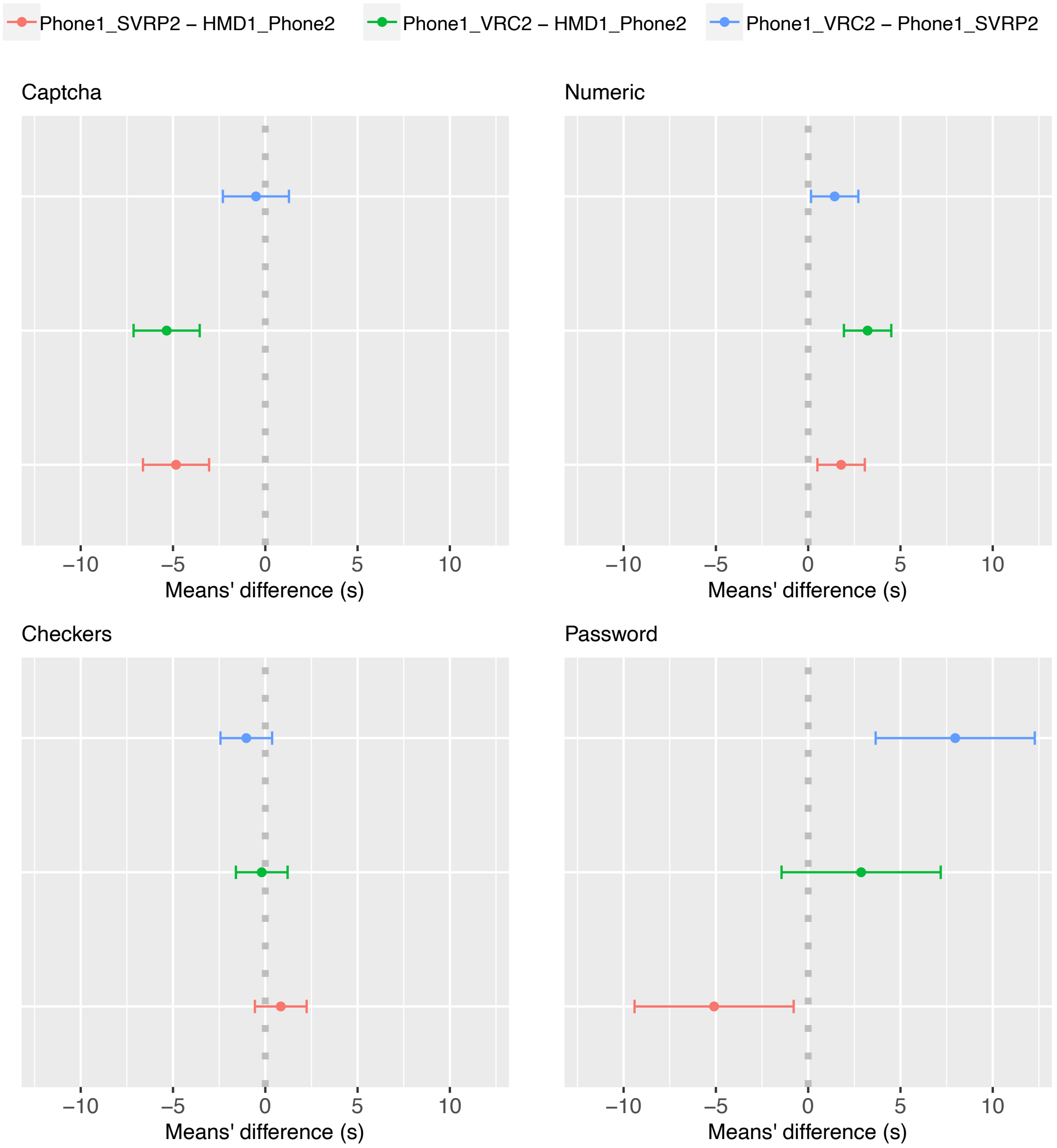


Figure E.11: The figure displays the 95% confidence intervals for the pairwise differences in mean completion times between conditions for all four challenges. Each circle represents the mean difference in completion time, with the dashed vertical gray line indicating the point of no difference between the means. The further the confidence interval is from this dashed line, the more statistically significant the difference in completion times. All differences are measured in seconds. This visualization allows for a clear assessment of the varying effects of different conditions on participants'

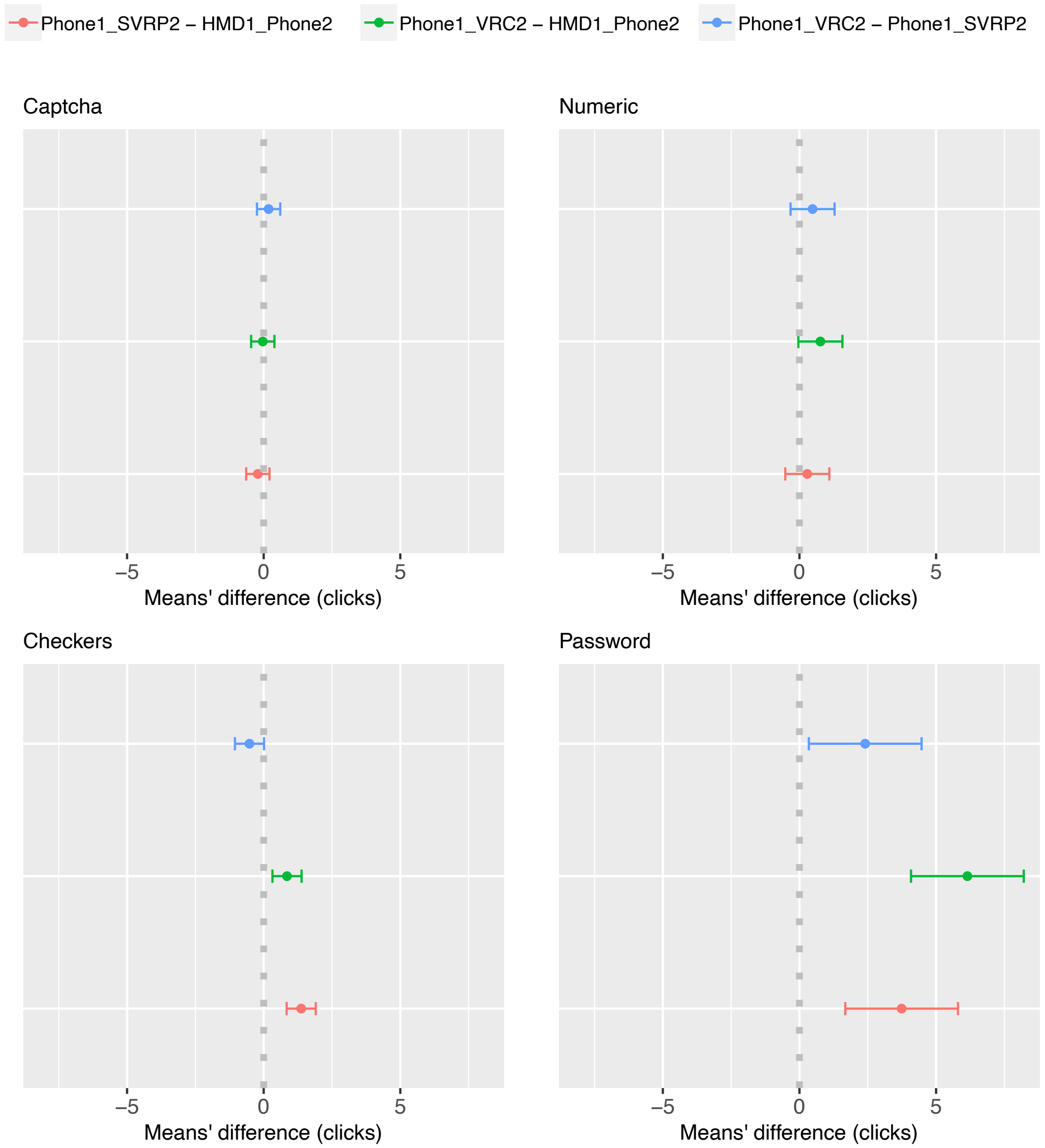
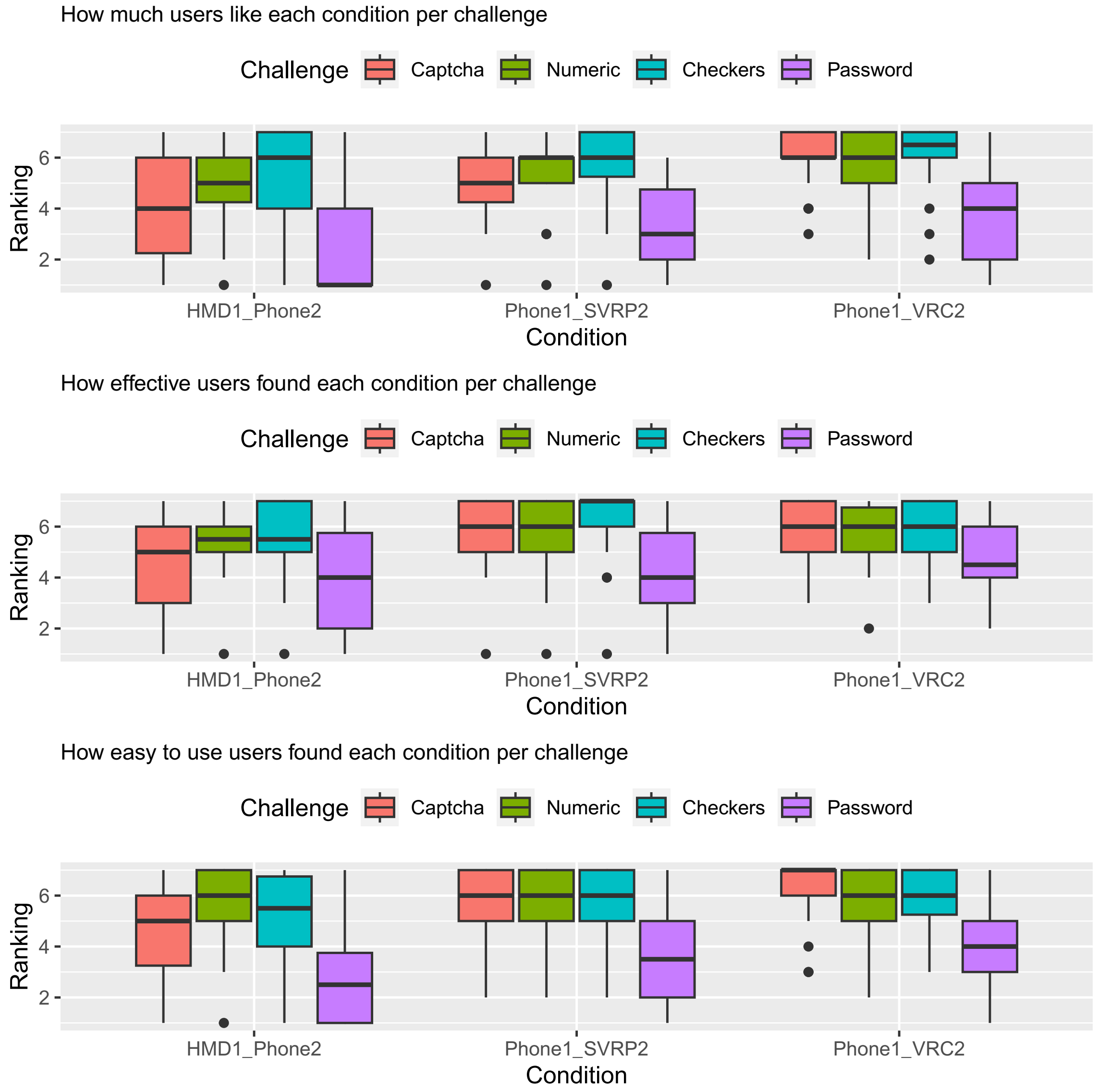


Figure E.12: The figure presents the 95% confidence intervals for the pairwise differences in mean number of clicks between conditions for all four challenges. Each circle indicates the mean difference in clicks, while the dashed vertical gray line marks the point of no difference between the means. The farther the confidence interval extends from this dashed line, the more statistically significant the difference in the number of clicks. All differences are represented as counts of clicks. This visualization provides an effective overview of how different conditions impact user interaction across



How much users like each condition per challenge

How effective users found each condition per challenge

How easy to use users found each condition per challenge

Figure E.13: The distribution of Likert-scale scores provided by participants for each condition across challenges reflects their evaluations of how much they liked the condition, its perceived effectiveness, and ease of use. In this ranking system, a score of 7 represents the highest level of satisfaction, 4 denotes a neutral perception, and 1 indicates the lowest level of satisfaction. The horizontal line within each box represents the median score, while the height of the box illustrates the interquartile range (IQR), indicating the spread of scores around the median.

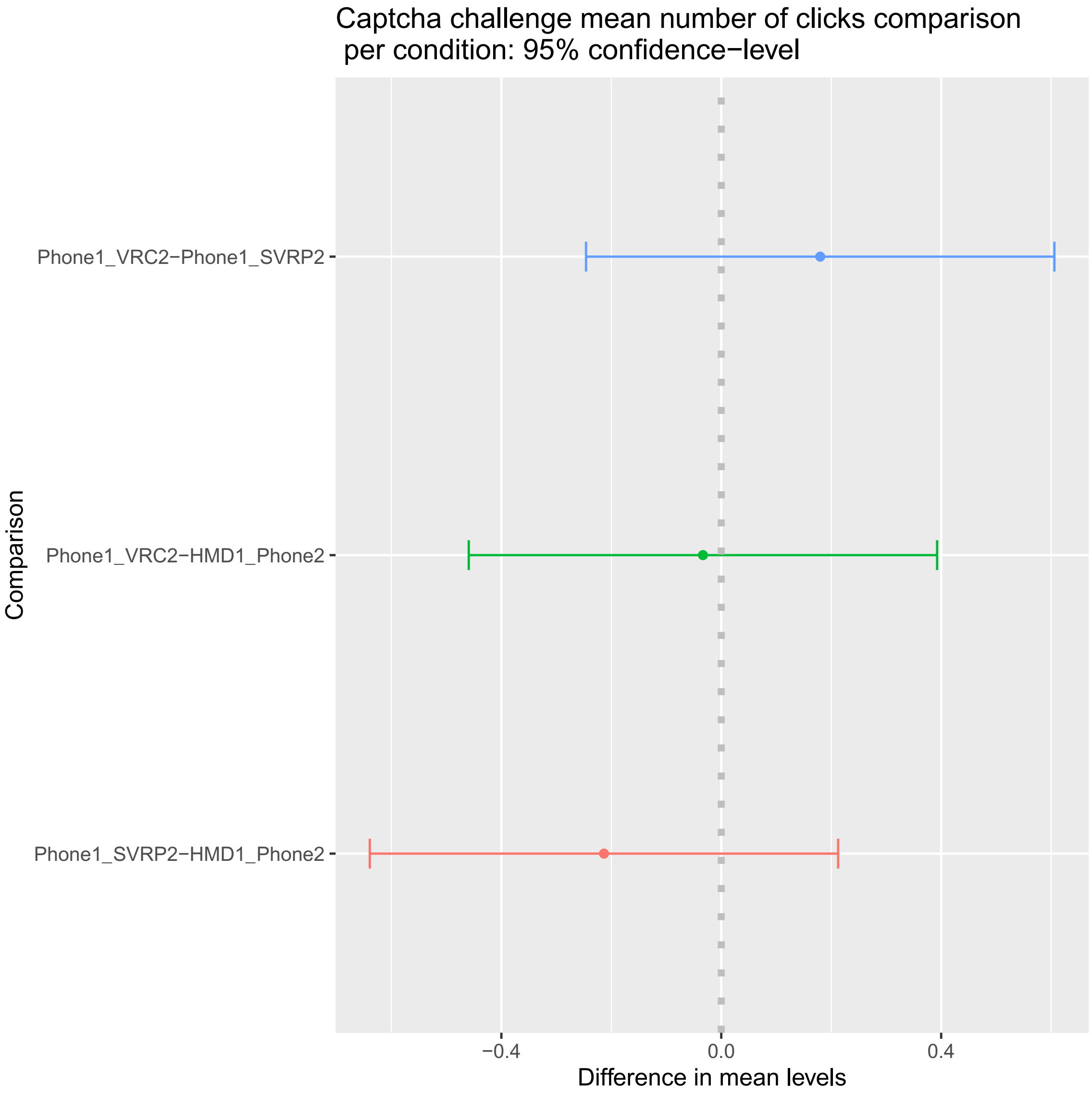


Figure E.14: The figure presents CAPTCHA challenge mean number of clicks comparison per condition: 95% confidence level.

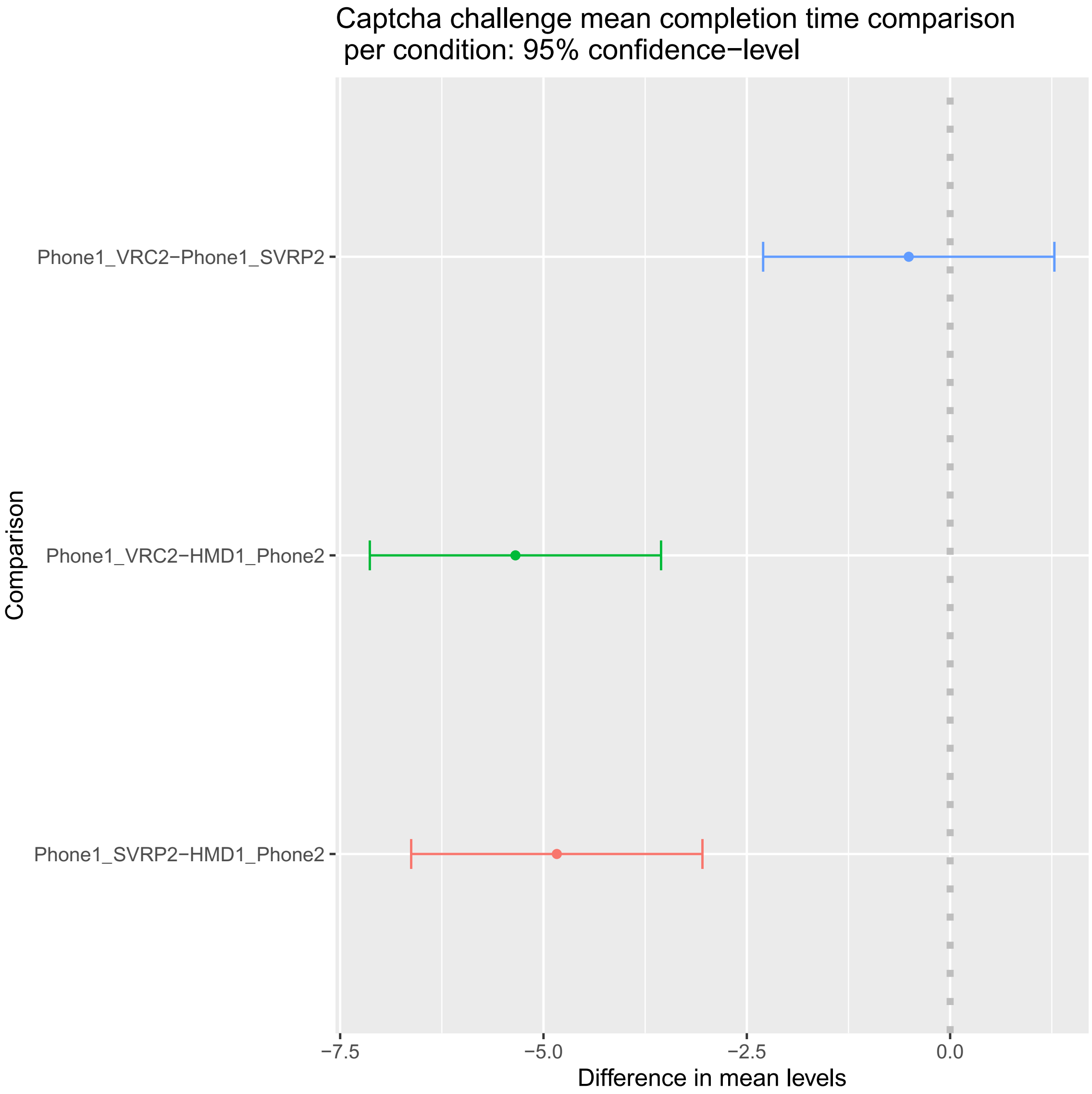


Figure E.15: The figure presents CAPTCHA challenge mean completion time comparison per condition: 95% confidence level.

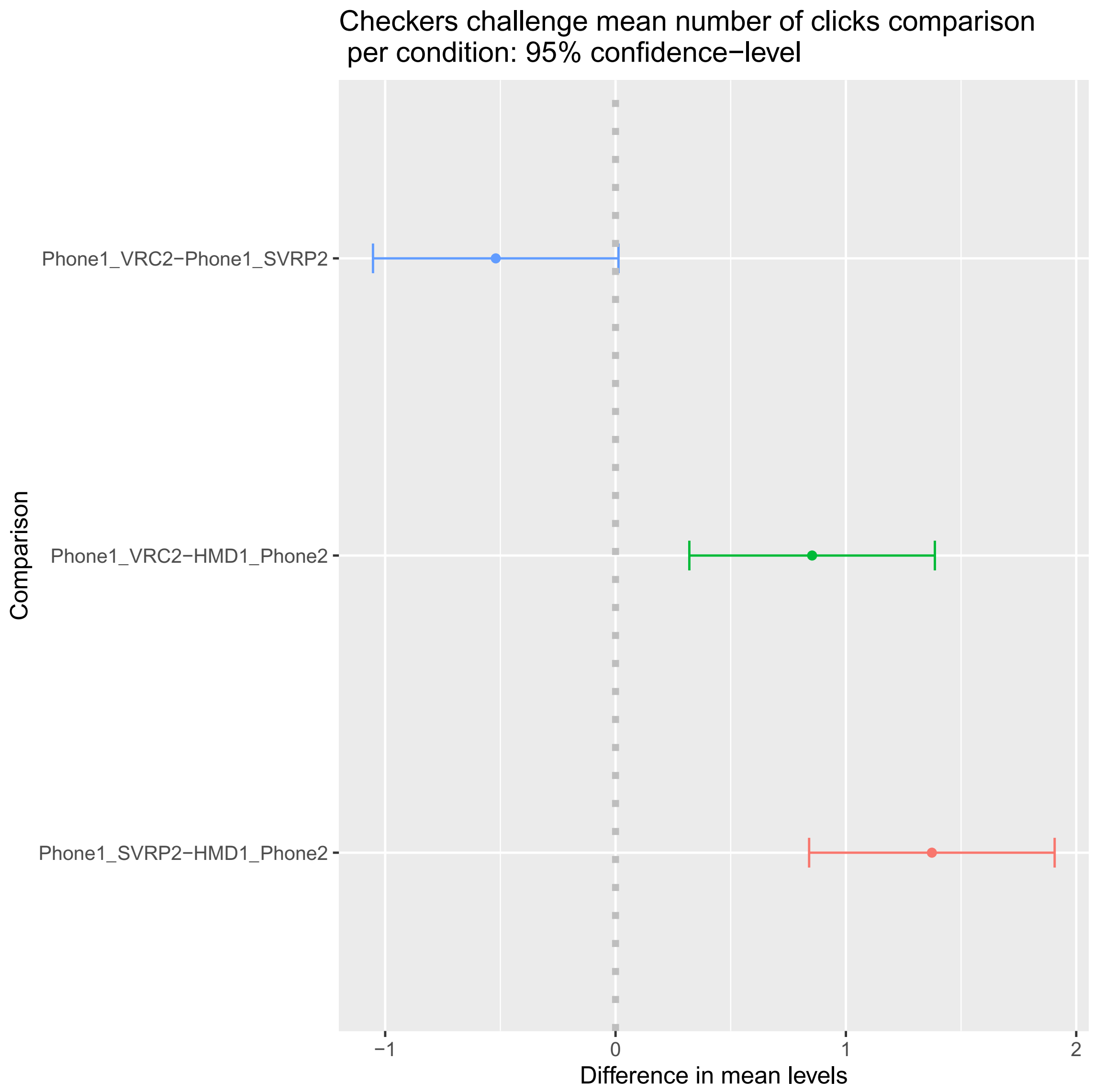


Figure E.16: The figure presents Checkers challenge mean number of clicks comparison per condition: 95% confidence level.

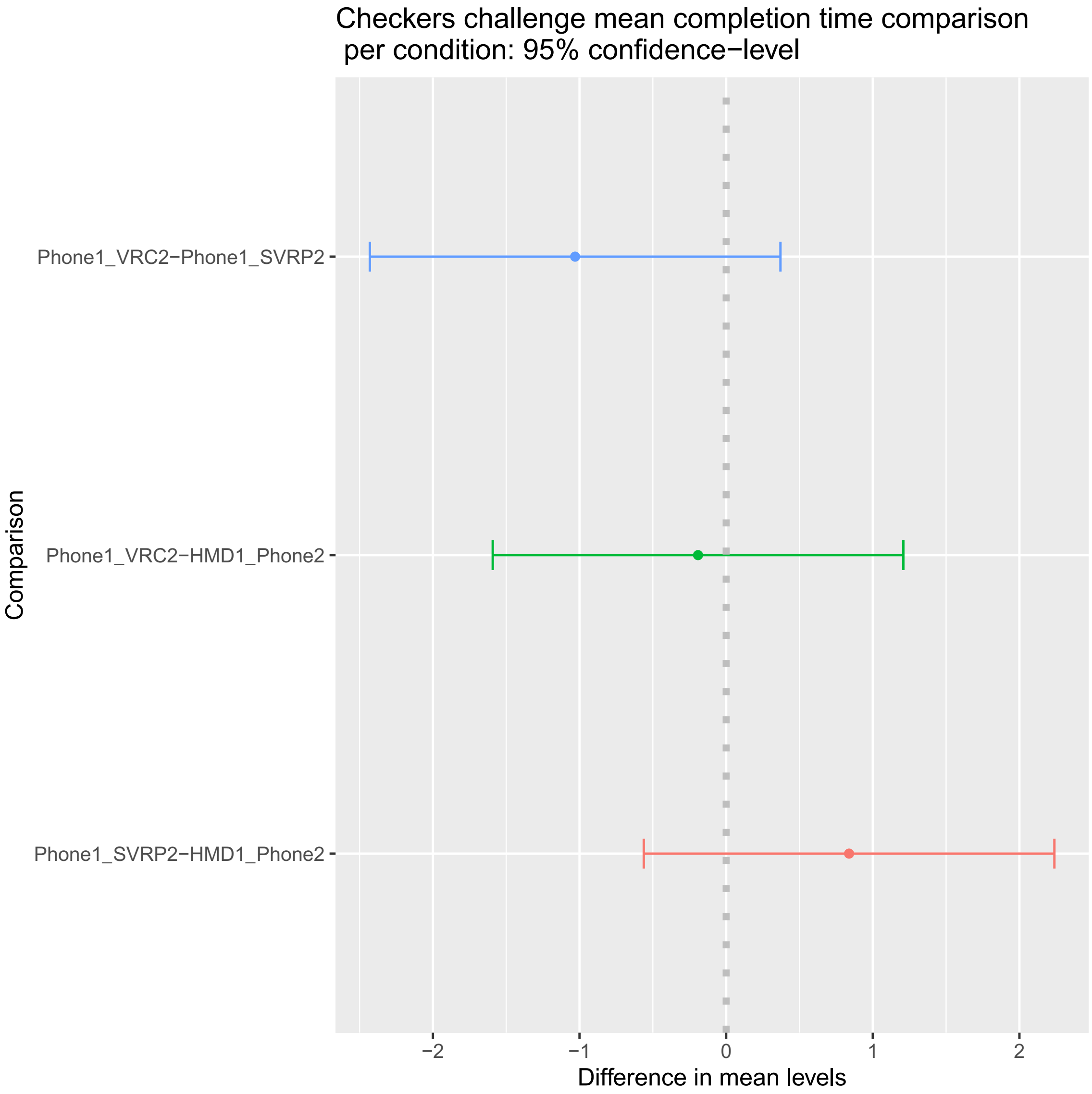


Figure E.17: The figure presents Checkers challenge mean completion time comparison per condition: 95% confidence level.

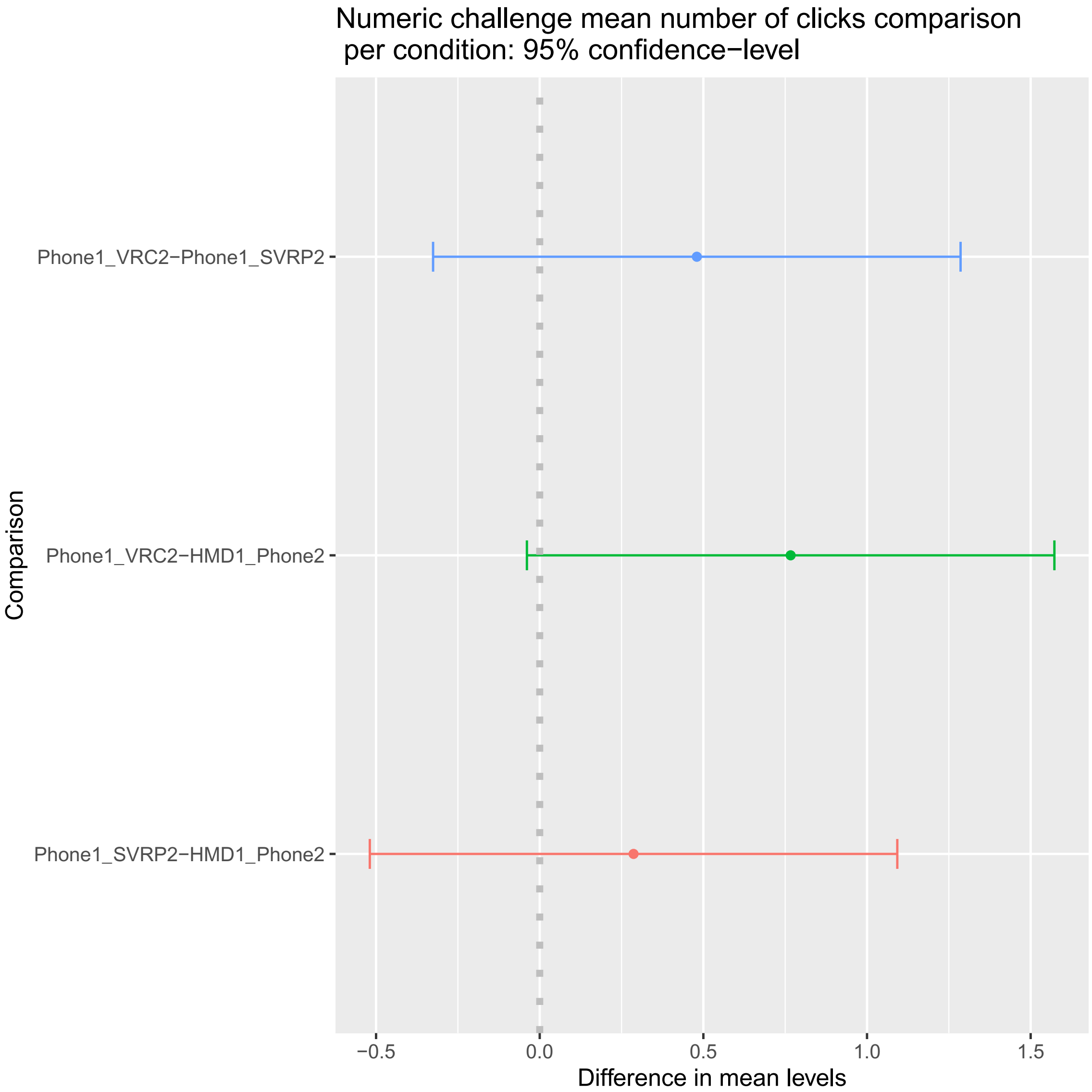


Figure E.18: The figure presents Numeric challenge mean number of clicks comparison per condition: 95% confidence level.

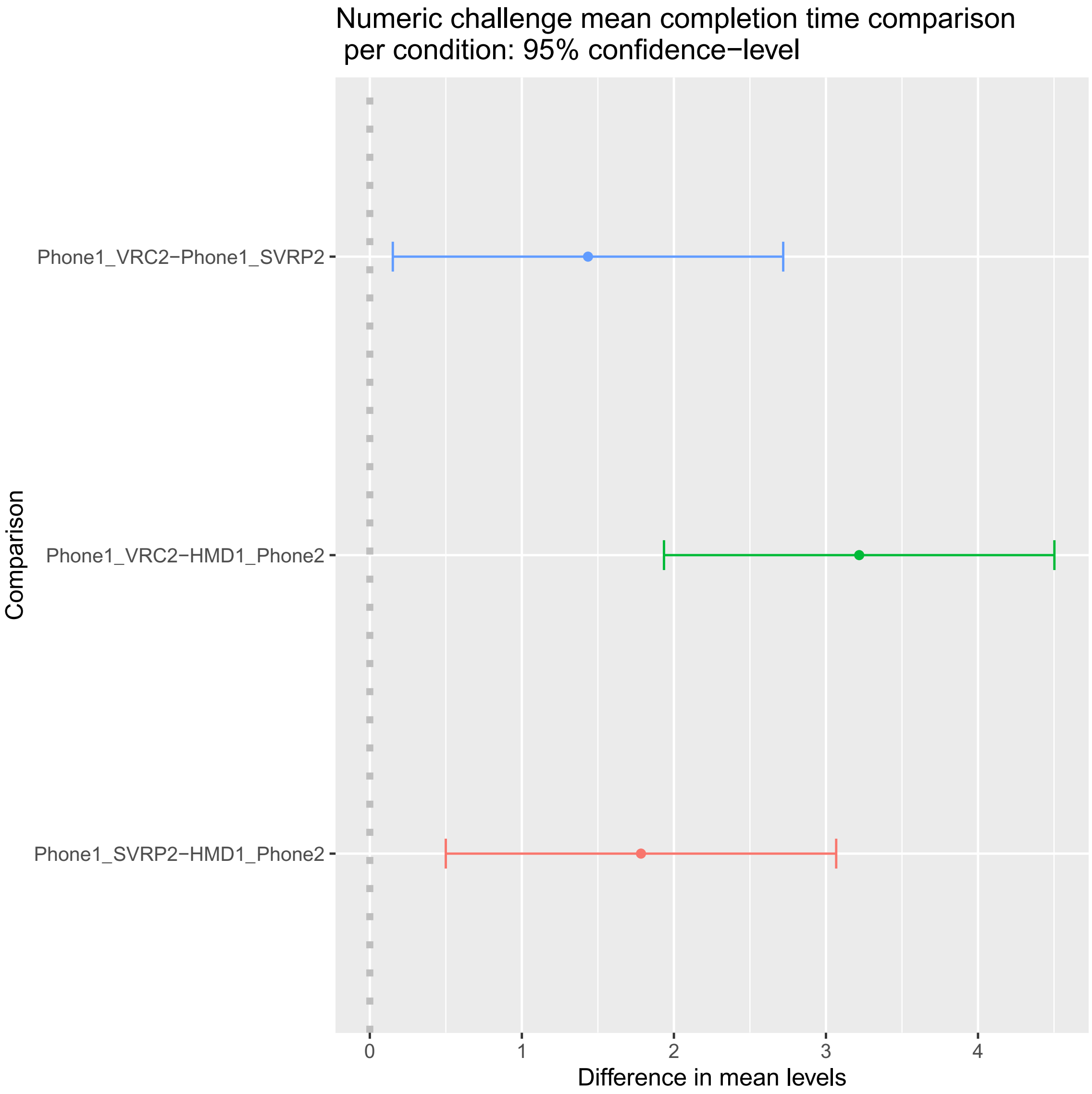


Figure E.19: The figure presents Numeric challenge mean completion time comparison per condition: 95% confidence level.

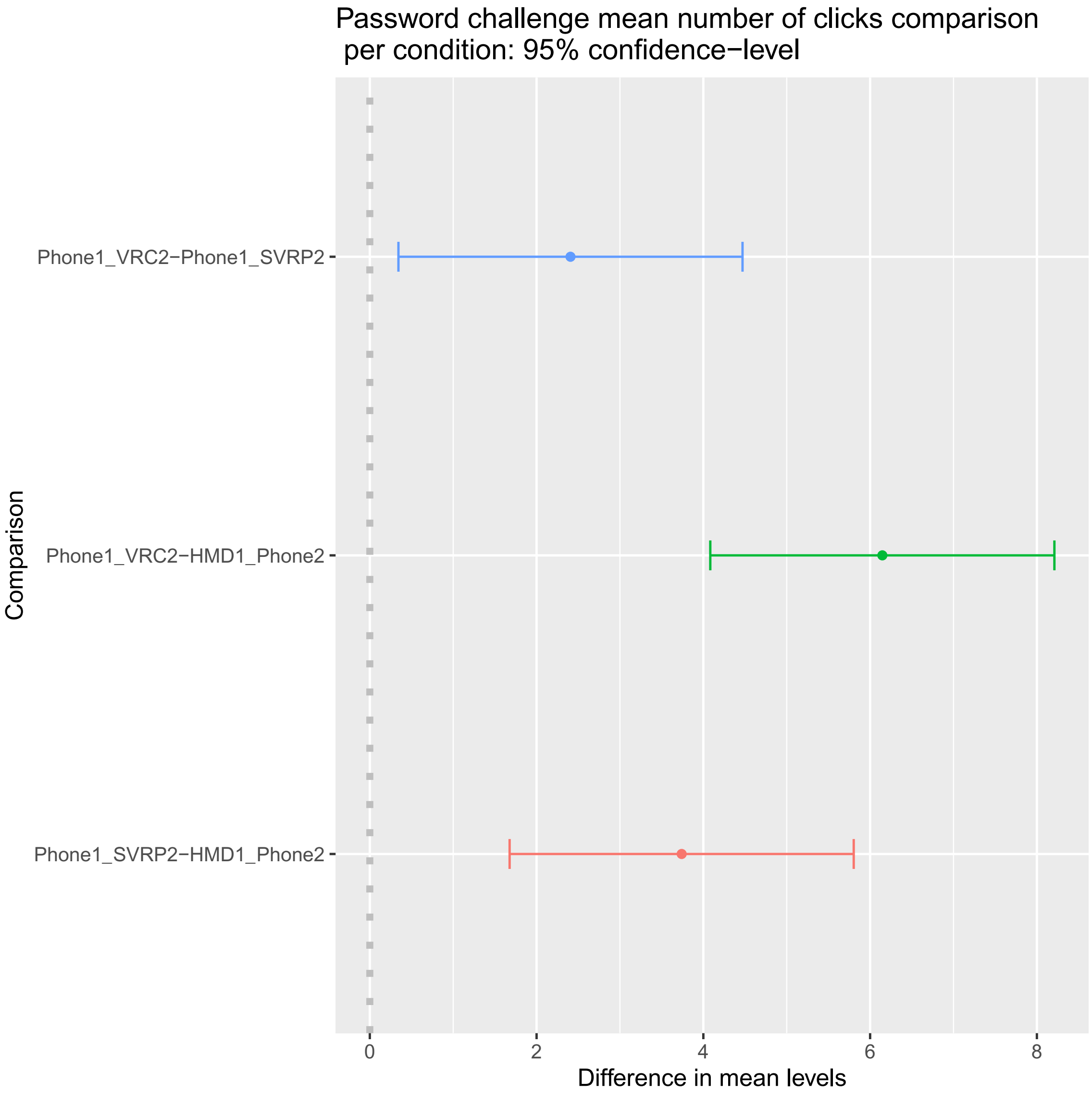


Figure E.20: The figure presents Password challenge mean number of clicks comparison per condition: 95% confidence level.

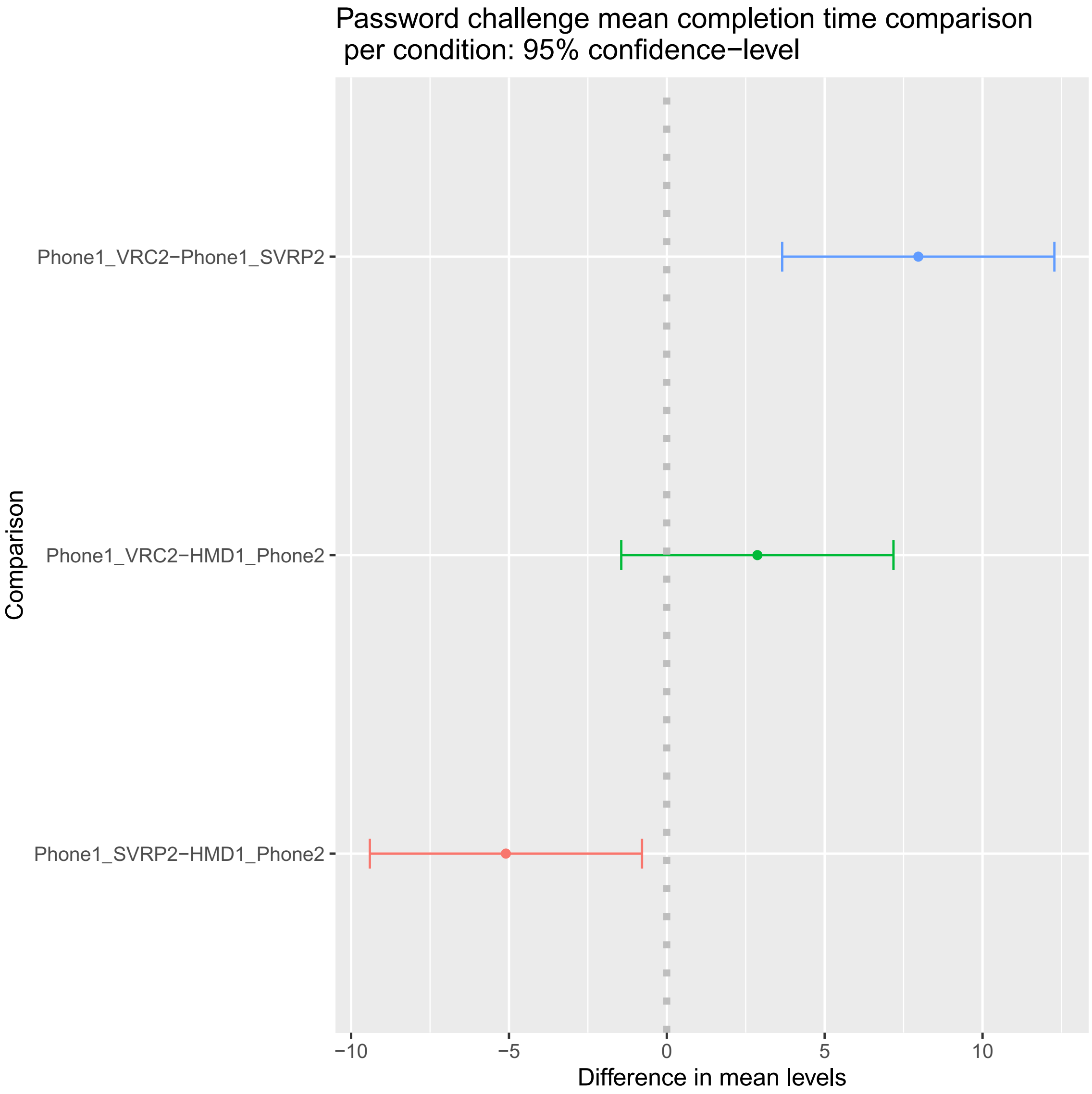


Figure E.21: The figure presents Password challenge mean completion time comparison per condition: 95% confidence level.

Appendix F

Tables

Condition	**CAPTCHA**	**Numeric**	**Checkers**	**Password**
HMD1_Phone2	17.76 ± 10.46	**10.68 ± 3.27**	13.63 ± 5.18	33.45 ± 19.22
Phone1_SVRP2	12.92 ± 4.16	12.47 ± 4.79	14.47 ± 6.50	**28.35 ± 9.33**
Phone1_VRC2	**12.41 ± 5.02**	13.90 ± 5.92	**13.44 ± 9.33**	36.32 ± 18.05
Average ± sd	14.36 ± 7.5	**12.35 ± 4.95**	13.85 ± 5.29	32.71 ± 16.44

Table F.1: Mean completion times (in seconds) and standard deviation per condition for each of the four challenges. The lowest mean completion time per challenge and the lowest overall average completion time are highlighted.

Factor	**CAPTCHA**		**Numeric**		**Checkers**		**Password**	
	F-value	p-value	F-value	p-value	F-value	p-value	F-value	p-value
Condition	30.02	$\mathbf{5.99 \times 10^{-13}}$	17.45	$\mathbf{5.09 \times 10^{-8}}$	1.69	0.185	9.69	$\mathbf{7.62 \times 10^{-5}}$
Round	12.13	$\mathbf{2.31 \times 10^{-09}}$	3.17	0.014	3.49	**0.008**	1.90	0.11
Order	15.28	$\mathbf{3.83 \times 10^{-07}}$	1.75	0.175	7.14	**0.0009**	6.88	**0.001**

Table F.2: ANOVA results of completion times per challenge. P-values less than 0.01 are highlighted.

Condition	**CAPTCHA**	**Numeric**	**Checkers**	**Password**	**Average**
HMD1_Phone2	85%	97%	**92%**	88%	90%
Phone1_SVRP2	94%	**99%**	89%	**91%**	**93%**
Phone1_VRC2	**96%**	93%	91%	87%	91%
Average ± sd	91.67% ± 5.86%	**96.33**% ± **3.06**%	90.67% ± 1.53%	88.67% ± 2.08%	91.83%

Table F.3: Success rate per condition for each of the four challenges. The highest success rate per challenge and the highest overall average success rate are highlighted.

Category	**CAPTCHA**	**Numeric**	**Checkers**	**Password**	**Total**
Best challenge	2.38%	4.76%	14.29%	0.00%	**21.43%**
Good challenge	7.14%	11.90%	11.90%	2.38%	**33.33%**
Bad challenge	7.14%	7.14%	0.00%	19.05%	**33.33%**
Worst challenge	2.38%	0.00%	0.00%	9.52%	**11.90%**
Balance	**0.00%**	**9.52%**	**26.19%**	**-26.19%**	**9.52%**

Table F.4: Summary of participants' comments regarding the challenges encountered during the experiment. The last row shows the balance of the percentages of positive comments minus the negative ones.

Category	**HMD1_Phone2**	**Phone1_SVRP2**	**Phone1_VRC2**	**Total**
Mostly Positive	0.00%	21.43%	9.52%	**30.95%**
Positive	7.14%	14.29%	14.29%	**35.71%**
Negative	9.52%	2.38%	7.14%	**19.05%**
Mostly Negative	9.52%	0.00%	4.76%	**14.29%**
Balance	**-11.90%**	**33.34%**	**11.91%**	**33.32%**

Table F.5: Summary of participants' comments regarding the conditions encountered during the experiment. The last row shows the balance of the percentages of positive comments minus the negative ones.