2023 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW) | 979-8-3503-4839-2/23/$31.00 ©2023 IEEE | DOI: 10.1109/VRW58643.2023.00319

DBA: Direction-Based Authentication in Virtual Reality

Yuxuan Huang[*,†] Danhua Zhang[*,†] Evan Suma Rosenberg[†]

University of Minnesota

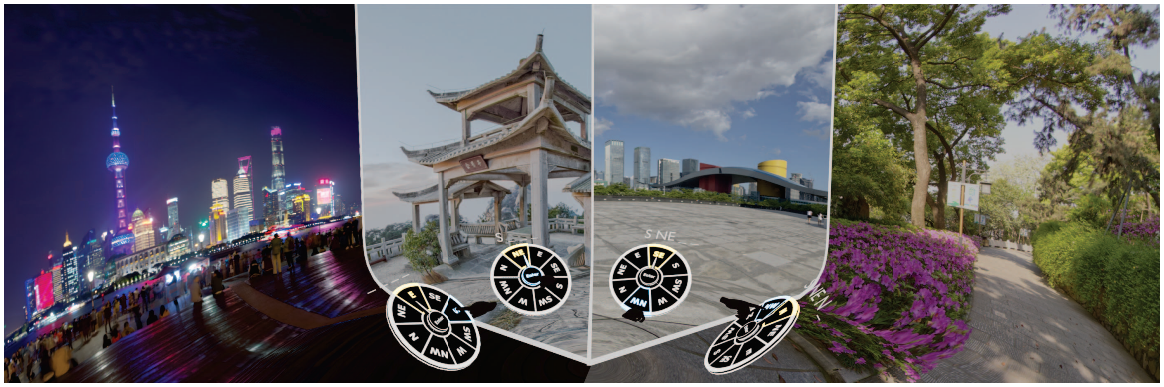


Figure 1: Direction-Based Authentication (DBA) is an authentication method where the user visits a sequence of 4 different environments and selects a direction in each of them as a symbol of the password. DBA combines text-based and context-based authentication methods in an intuitive manner.

Abstract

To protect the privacy and security in the emerging metaverse, various authentication methods have been designed for virtual reality. In this paper, we propose a novel selection-based authentication method called the Direction-Based Authentication (DBA). To enter a password, the user visits a sequence of four different environments and selects a direction in each of them as a symbol via either physical turning or panel-controlled snap-turning. The goal is to provide an authentication technique that is both memorable and efficient to use without compromising its security. Preliminary testing shows that the entry time of DBA can be as short as 6-12 seconds.

Index Terms: Human-centered computing—Human computer interaction (HCI)—Interaction paradigms—Virtual reality; Security and privacy—Human and societal aspects of security and privacy—Usability in security and privacy

1 Introduction

With the envisioning of the metaverse getting closer to reality, concerns associated with the data security in such settings are also gaining increased attention. The unique characteristics of virtual reality (VR) provide both opportunities and challenges for privacy protection, and various types of authentication methods have been proposed to provide more secured and efficient user authentication specifically for VR. State-of-the-art authentication methods in VR can be divided into 4 categories: knowledge-based, biometric-based, token-based, and multi-factor authentication [3]. These authentication methods differ vastly in nature, and this work focuses primarily on on knowledge-based authentication because it can leverage the features of a 3D virtual environment.

Knowledge-based authentication is known for its simplicity in implementation, high accuracy in identification, and independence of hardware, in comparison to biometric authentication. It also does not require the removal of headset or a secondary device for multi-factor authentication. However, security is a major concern for knowledge-based authentication compared to other authentication methods. Even though the head-mounted-display (HMD) provides a private screen, it also blocks out the real-world from the users' view, making their authentication procedures prone to observational attacks from bystanders. Therefore, traditional 2D authentication methods such as PINs and patterns are not ideal because they could be readily imitated, and effective knowledge-based authentication should ideally be resistant to observational attacks.

2 Related Work

Existing knowledge-based authentication methods for VR can be roughly divided into two types based on the type of password user has to remember. Symbolic input methods aggregate text, digits, or other characters on a single panel, allowing for efficient entry. One example is *RubikAuth* proposed by Mathis et al., where the user interacts with a 3D cube and enter the color-digit combinations on the sides of the cube [2]. The use of a 3D cube as the password interface instead of a traditional 2D panel enhances security by increasing the difficulty of cracking the password based on the movement of the user, but this increased complexity also makes it more difficult for users to remember.

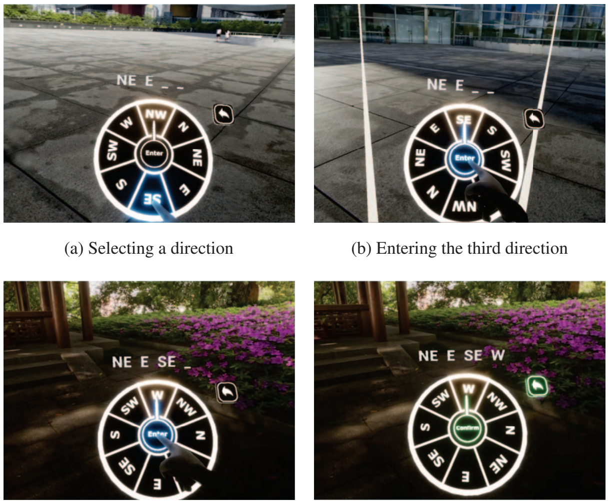
Context-based methods involves recalling knowledge that is qualitatively different from symbolic characters. For example, in *RoomLock* proposed by George et al., the user enters the password by selecting a sequence of objects in a virtual room [1]. To protect this process against observational attacks, the positions of the user and the objects are randomized. Context-based authentication can achieve good memorability by providing context to what the user remembers, but it is associated with longer entry time because the user has to search for the objects in the environment.

To achieve the best of both worlds, we propose the Directional-Based Authentication (DBA) for VR, which allows text-based and

[*] these authors contributed equally to this work

[†] e-mail: {huan2076, zhan5954, suma}@umn.edu

979-8-3503-4839-2/23/$31.00 ©2023 IEEE
DOI 10.1109/VRW58643.2023.00319



(a) Selecting a direction

(b) Entering the third direction

(c) Entering the fourth direction

(d) Confirming the password

Figure 2: (a) With a current direction of *NW*, a user presses the *SE* button on the compass. (b) The user is reoriented towards the *SE* direction. Note that a glossy frame visualizes the boundary of the scene corresponding to *SE* after the rotation. The user then presses the enter button to enter *SE* as the third direction of the password. (c) In the next environment, the user enters *W* as the the last direction in the password. (d) The enter button turns into a confirm button for final confirmation.

context-based authentication to be treated in a unified manner. More details of DBA are discussed in the following section.

3 Methods

In DBA, a password is a sequence of four directions in which the user is looking at in four different environments. Each direction can be one of the eight options: *N*, *E*, *S*, *W*, *NE*, *SE*, *NW*, and *SW*. The use of directions instead of numbers makes the password less guessable, since numerical passwords are commonly chosen to be known facts about the user, e.g., birthdates. The use of 360° high dynamic range images (HDRIs) to represent a surrounding environment provides context and graphical information to facilitate memorization.

During the authentication process, the user will find themselves in four different environments where they enter the directions as the password. The user will see a compass floating slightly below their line of sight with their real-time direction highlighted. Each time the user changes their viewing direction, a glossy frame will highlight the corresponding part of the environment to their new direction for one second before fading out. The user will look around and remember a point of interest in the surroundings, along with the direction associated with it. The entered directions will also be shown above the compass. The user can choose to memorize the visual information or the text. Therefore, our password is both text-based and context-based but integrated in an intuitive manner.

The user can change their viewing direction by either physically turning their head or by pressing the direction buttons on the compass, which will trigger a snap turn (Fig.2a). The rationale behind our design is that physical turning allows the user to look around to gather visual information in a more natural way, which is helpful for recalling the password when they are unfamiliar with the direction sequence. Additionally, the text-based button interaction allows the user to skip the searching process and enter the password efficiently when they already know which direction needs to be entered.

To enter the selected direction and proceed to the next environment, the user will press the enter button while they are facing that direction (Fig.2b, 2c). The enter button is placed at the center of the compass. The user can always be aware of the current direction when entering the password. When the user enters an incorrect direction, they can press the backspace button which loads the previous environment to re-enter the direction. In the last environment after entering the password, a confirm button will replace the enter button so that the user can review the direction sequence before submitting it for authentication (Fig.2d). The user can modify the password by pressing the backspace button if needed. All virtual buttons being pressed will glow in blue and generate haptic feedback on the hand associated with the interaction.

The user's initial direction in each environment is also randomized, so that the motion associated with the same password entry is different each time. Therefore, we expect this improve robustness against observational attacks of the physical user's motion.

Apart from the advantages discussed above, our method is highly customizable. The virtual scenes used in the authentication can be customized on a per-application basis, allowing the authentication to be integrated as part of the applications in a seamless manner.

4 Preliminary Testing

The software was developed using Unreal Engine 5.1 and tested on a workstation with Nvidia GeForce RTX 3080Ti, Intel i7-11700K 3.6GHz and 32GB RAM. To test the efficiency of the authentication, we considered the time from the first entry until all four directions are entered in the snap-turning-only and physical-turning-only conditions. The two developers each repeated the authentication five times for each condition. The entry time was 6.20-12.07 seconds ($M = 8.48$, $SD = 2.01$) in the snap-turn condition and 6.42-12.14 seconds ($M = 9.21$, $SD = 1.90$) in the physical-turn condition.

5 Conclusion and Future Work

In this paper, we presented Direction-Based Authentication (DBA) for VR, a novel authentication scheme where the passwords are defined by a sequence of view directions. DBA combines text-based and context-based password to facilitate memorization and allows both physical-turning and panel-controlled snap-turning to enhance memorability without compromising efficiency. Our intention in creating DBA is to put forward an authentication method for VR that balances the benefits of symbolic and context-based input. Randomization is also introduced to ensure the security of our method against observational attacks. However, knowledge-based methods are not robust to observational attack if the application is being run on a PC and the window is visible on the computer screen, so it is suggested to disable the virtual view on PC.

Our preliminary testing suggested that authentication can be completed efficiently by expert users. However, formal user studies will be needed to evaluate efficiency, memorability, and security of this method with a general population.

Acknowledgments

The authors wish to thank www.51hdr.com for supporting the project with HDRI images.

References

[1] C. George, M. Khamis, D. Buschek, and H. Hussmann. Investigating the third dimension for authentication in immersive virtual reality and in the real world. In *2019 ieee conference on virtual reality and 3d user interfaces (vr)*, pp. 277–285. IEEE, 2019.

[2] F. Mathis, J. Williamson, K. Vaniea, and M. Khamis. Rubikauth: Fast and secure authentication in virtual reality. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*, pp. 1–9, 2020.

[3] S. Stephenson, B. Pal, S. Fan, E. Fernandes, Y. Zhao, and R. Chatterjee. Sok: Authentication in augmented and virtual reality. In *2022 IEEE Symposium on Security and Privacy (SP)*, pp. 1552–1552. IEEE Computer Society, 2022.