CLUE HOG: An Immersive Competitive Lock-Unlock Experience using Hook On Go-Go Technique for Authentication in the Metaverse

Alexander Giovannelli* Francielly Rodrigues Shakiba Davari Ibrahim A. Tahmid Logan Lane
Cherelle Connor Kylie Davidson Gabriella N. Ramirez Brendan David-John Doug A. Bowman

Center for Human-Computer Interaction
Department of Computer Science, Virginia Tech, Blacksburg, VA, USA

Figure 1: 3DUI authentication virtual environment with HOG interaction technique used in this paper: (A) Selectable authentication token highlighted. (B) Authentication token highlight on selection. (C) Updated virtual environment on successful authentication with verified token highlights.

Abstract

This paper presents our solution to the 2023 3DUI Contest challenge. Our goal was to provide an immersive VR experience to engage users in privately securing and accessing information in the Metaverse while improving authentication-related interactions inside our virtual environment. To achieve this goal, we developed an authentication method that uses a virtual environment's individual assets as security tokens. To improve the token selection process, we introduce the HOG interaction technique. HOG combines two classic interaction techniques, Hook and Go-Go, and improves approximate object targeting and further obfuscation of user password token selections. We created an engaging mystery-solving mini-game to demonstrate our authentication method and interaction technique.

Index Terms: Human-centered computing—Human computer interaction (HCI)—Interaction paradigms—Virtual reality; Human-centered computing—Human computer interaction (HCI)—Interaction techniques

1 Introduction

As virtual reality (VR) head-worn displays (HWDs) become more commercially applicable for businesses, including healthcare and manufacturing, as well as everyday consumers for entertainment and social applications, a critical task is to secure user-sensitive information available on the device. This motivates exploiting the capabilities that VR provides to design efficient authentication methods resistant to privacy attacks.

Current authentication methods have explored the use of knowledge-based, biometric-based, and gaze-based methods for authentication [6]. Knowledge-based methods such as 3D patterns and PINs have high usability but have been shown to be highly susceptible to observation and brute-force attacks [7]. Biometric-based methods can be difficult to implement on a large scale due to sensor availability and decreased accuracy given many individuals [4].Gaze-based methods, although resilient to observation attacks, are more cognitively taxing and less time efficient than their alternatives [1].

In this paper, we introduce a token-based authentication method using a combination of Hook and Go-Go interaction techniques [3, 5]. The combination of these two techniques allows users a means of comfortably interacting with targets at various distances. Furthermore, this combination provides our method with increased obfuscation of selected objects and efficient object selection, overall making our method more resistant to over-the-shoulder attacks. To showcase our authentication method, we have designed a competitive immersive experience in which users are tasked with collecting evidence in order to solve a crime. They are required to use an authentication method to secure their discoveries from competitors.

2 Design Process

Our design process started with weekly group meetings dedicated to the design of our authentication method. We explored the criteria for the design of authentication methods and the capabilities that VR can offer over traditional 2D authentication methods. We also investigated the previous research on this topic and its advantages and disadvantages. During this process, we designed and prototyped multiple authentication techniques, and chose one as our authentication method for the contest. In order to enhance our authentication method and provide a memorable experience for users, we then divided into groups to focus on the story and interaction technique for authentication. The final program we created in Unity with the OpenXR framework, which supports flexibility in the user's choice of HWD for our experience.

3 Authentication Method

To provide efficient authentication, the ideal authentication processes should be fast to enter, easy to memorize, secure to password attacks and external observation, and not limited to specific hardware. VR has reduced the efficiency of many traditional authentication methods due to challenges such as keyboard-based text entry limitations, obfuscation of password entry, and biometric safety with personal data privacy concerns [6]. Researchers have leveraged new peripherals and capabilities of VR HWDs, such as using input mapping reconfigurations for controllers and rotational manipulation of objects, as well as swipe patterns in 3D space as an alternative to

*e-mail: agiovannelli@vt.edu

text-entry-based passwords [6]. These methods, however, are slower, difficult to remember, or limited to specific hardware.

As virtual environments (VEs) present unique opportunities to re-imagine authentication processes, we brainstormed multiple authentication methods and identified which of our criteria each design covers. For example, one of our proposed authentication methods was *Paintbrush*, in which the user performs a brush gesture on a canvas to select a sequence of paint colors on a palette, which acts as the password for the system. The randomization of color position on the palette would be used to prevent external observation attempts. We did not implement this design due to accessibility concerns related to color vision deficiencies.

VR provides additional opportunities to use 6DoF and the 3D environment interactions for authentication. For this reason, we decided to develop an authentication method that would leverage interacting with the unique objects comprising a given VE as tokens to create a unique, personal identification token sequence (PITS) lock. This authentication method is comprised of three components: (1) lock environment, (2) locomotion, and (3) token selection. Users are able to create or specify their own lock environment in the first component. This environment would be populated with user-selected objects positioned by the user, which act as potential tokens. Similar to traditional keyboard-based passwords, where the number of unique combinations of characters determines strength against brute-force attacks, the number of available tokens, as well as token selection combinations, can be tailored to the security needs of each system. For the second component, users are able to move freely within their lock VE via raycast teleport or physical movement within their established VR boundary. In the third component, users are capable of selecting any sequence of objects in their lock environment to act as their authentication PITS. The number of tokens comprising the user's PITS is user-specified and can include duplicate selections of tokens.

Combining all three components of our authentication method, each user creates a unique and memorable authentication experience. External observers are faced with the new complexities introduced by our method: the unique composition of a user's lock environment, position and movement within the environment, and the user PITS value. To further enhance the efficiency and privacy of the PITS setup process, we developed a novel selection technique described in the following section.

4 Interaction Technique

Initially, we considered using the RoH WiM interaction technique [2] to provide users with a means to perform their PITS authentication selection. However, as part of the emphasis on locomotion to obfuscate token selection in our method, we opted to develop our own technique. The major objectives of our interaction technique are 1) efficient object selection and 2) obfuscation of selected objects. Our approach, HOG, combines two traditional interaction techniques: Go-Go and Hook.

The Go-Go technique works to facilitate precise object selection by providing a mapping function to extend a virtual hand. Through a "growing-arm" metaphor, Go-Go provides the ability to select both near and far objects without the need to navigate the environment [5]. In the Hook method, the best-scored object will "hook" to the virtual hand, where an object's *score* is calculated based on its distance to the virtual hand [3].

By combining Go-Go's growing arm and Hook's item selection technique, HOG enables quick object selection within the environment. In addition to efficient selection, HOG provides obfuscation through the hook method. In our implementation of hook selection, the user can select an object without the item attaching to the virtual hand. This helps obfuscate the authentication process by allowing the user to move their virtual hand around the selectable items quickly and select an object in secret.

5 Story and Gameplay

Our story takes place in the year 2040 when a detective agency uses digital twins of crime scenes for inspection and investigation. A new case has been issued for the agency regarding an isolated arson attack against an influential businessman's private mountainside estate. It is urgent to solve this case since there are suspicions that the culprit has planned similar attacks on other influential people in the town. The user, acting as the lead detective on the case, is tasked by the agency to solve the mystery of the arson case. Due to the urgency of the case, the case is assigned to multiple teams and agencies and a handsome reward is offered to the winning team.

The user is first required to secure their discoveries from the competing teams, using our authentication method. Prior to investigating the crime scene, they must set their authentication tokens by selecting their token objects using the HOG interaction technique. The user then navigates the various rooms and uses HOG to select potential evidence they find at the crime scene. After selecting evidence for lab review, the user is able to receive feedback on whether the evidence reported was incriminating or not after authenticating it into their remote Metaverse information facility. Once the user finds the incriminating evidence successfully, the game ends and gives them a score for their investigation according to time spent at the crime scene.

6 Conclusion

We implemented a novel authentication method in VR using VE assets as tokens, as part of our PITS locking mechanism. To enhance our authentication method, we developed an interaction technique, HOG, to improve the user experience during the token selection process and further mask token selections from external observers. To demonstrate the capabilities and encourage the adoption of these novel contributions to security, we created an immersive VR experience where users use our authentication method and interaction technique to solve a mystery.

References

[1] M. Khamis, L. Trotter, V. Mäkelä, E. v. Zezschwitz, J. Le, A. Bulling, and F. Alt. Cueauth: Comparing touch, mid-air gestures, and gaze for cue-based authentication on situated displays. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 2(4):1–22, 2018.

[2] L. Lisle, F. Lu, S. Davari, I. A. Tahmid, A. Giovannelli, C. Llo, L. Pavanatto, L. Zhang, L. Schlueter, and D. A. Bowman. Clean the ocean: An immersive vr experience proposing new modifications to go-go and wim techniques. In *2022 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*, pp. 920–921, 2022. doi: 10.1109/VRW55335.2022.00311

[3] M. Ortega. Hook: Heuristics for selecting 3d moving objects in dense target environments. In *2013 IEEE Symposium on 3D User Interfaces (3DUI)*, pp. 119–122, 2013. doi: 10.1109/3DUI.2013.6550208

[4] K. Pfeuffer, M. J. Geiger, S. Prange, L. Mecke, D. Buschek, and F. Alt. Behavioural biometrics in vr: Identifying people from body motion and relations in virtual reality. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pp. 1–12, 2019.

[5] I. Poupyrev, M. Billinghurst, S. Weghorst, and T. Ichikawa. The go-go interaction technique: non-linear mapping for direct manipulation in vr. In *Proceedings of the 9th annual ACM symposium on User interface software and technology*, pp. 79–80, 1996.

[6] 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. 267–284, 2022. doi: 10.1109/SP46214.2022.9833742

[7] Z. Yu, H.-N. Liang, C. Fleming, and K. L. Man. An exploration of usable authentication mechanisms for virtual reality systems. In *2016 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*, pp. 458–460, 2016. doi: 10.1109/APCCAS.2016.7804002