NELI-AUTH: Authentication System Based on Non-equal-length Input for Virtual Environment

Haopai Shi[1], Yaxin Wang[1], Yuxuan Fan[1], Tiemeng Li[1,2*]
[1] Beijing University of Posts and Telecommunications, China
[2] Beijing Key Laboratory of Network System and Network Culture, China, 100876.

ABSTRACT

Existing authentication approaches for virtual reality are either inefficient or susceptible to observation attacks. In this work, we present NELI-AUTH, a non-equal-length input-based identity authentication system for virtual reality. The user may enter the password using the alternative operation of two controllers and the non-equal-length item input procedure to form the final password. This scheme's confirmation operation is difficult to observe, which not only provides a high level of security but also ensures the consistency of the input operation in each verification process, thereby significantly enhancing the input's efficiency in the verification process.

Index Terms: Virtual reality—Authentication—Human-computer interaction—

1 INTRODUCTION

We present NELI-AUTH (Figure 1), an authentication scheme for virtual reality where users can perform non-equal-length input through controllers and thumbsticks to achieve efficient and secure identity authentication.

In contrast to the majority of current knowledge-based authentications that use numbers and characters as encoding, the input technique that employs physical location as encoding is unknown to the majority of users, and as a consequence, may incur substantial learning costs. Since the password element is structured based on randomization, NELI—AUTH fixes the issue that the user must re-recognize the interface every time. And the efficiency and recognizing accuracy of using the controller to input is much greater than gesture input, while the input method corresponds with the user's physical location, resulting in a significant increase in the efficiency of a single input by the user.

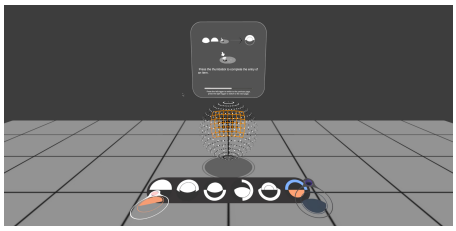

Figure 1: NELI-AUTH demo system

2 RELATED WORK

Knowledge-based authentication and biometric authentication are two prevalent authentication methods in virtual reality.

*e-mail: tiemeng2000@gmail.com

The results of biometric authentication were promising. However, these works have stringent hardware requirements and cannot be utilized in many situations.

Knowledge-based authentication avoids the issues above. However, existing knowledge-based authentication methods such as PIN [2], pattern, or gesture-driven authentication [1] are observable bystanders, resulting in a substantial reduction in security.

Other schemes use random numbers, resulting in a substantial reduction in security. To ensure safety, each verification process involves elements that generate information discrepancies between operators and bystanders. However, this scheme requires users to reestablish their grasp of the input system during each verification procedure, making it impossible to verify fast.

Therefore, we require knowledge-based authentication that can guarantee security and provide the same layout for each verification process.

3 CONCEPT OF NELI-AUTH

NELI-AUTH consists of three parts: the visual sphere that indicates the current input, the controller proxy that facilitates the operation, and the password box that records the outcome.

3.1 The Visualizing Sphere

The sphere is divided into twelve areas. In the vertical direction, there are three levels: Upper, Middle, and Lower. In each horizontal level, there are four positions: front, back, left, and right. A user can select one of these 12 areas using the controller (Figure 2) and the current state displayed on the sphere represents the last operation the user has carried out.

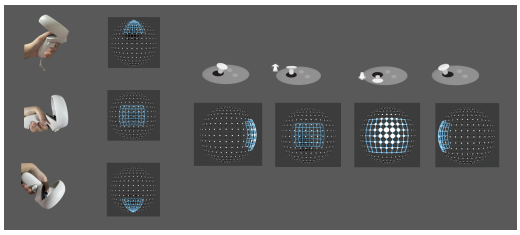

Figure 2: Sphere state corresponding to controller operation

3.2 The Controller Agency

To help the users comprehend the password input for different operations, we have created new agencies for the two controllers in the immersive space. In general, the agency is composed of the following two parts.

3.2.1 Tilting the controller

By tilting the controller upwards and downwards, the user can change the vertical level of the sphere. The tilting operation will be reflected instantly on the small ball model in front of the control agency.

3.2.2 Moving the thumbstick

By moving the thumbstick, the user can select a position. In the controller agency mode, the position of the semicircle with high brightness indicates the thumbstick's current state.

3.3 The password box

The password box is used to store and display the password currently entered. NELI-AUTH proposes a graphic coding scheme to differentiate between *items* and *elements* (Figure 3).

Figure 3: Composition of code

3.3.1 Password capacity

A password string should contain multiple *items*. An item can contain as few as one *element* or as many as three. From the interior to the exterior, an item's constituent elements are represented by 1-3 concentric circles.

3.3.2 Encoding

In each *element*, the position of the semicircle filled with color indicates the horizontal position, and the semicircle shape signifies the vertical level. The semicircle protruding outward indicates the upper level of the operation, the semicircle normal indicates the middle level, and the semicircle sunken indicates the lower level. (Figure 4)

Figure 4: The encoding of NELI-AUTH

4 Implementation of NELI-AUTH

4.1 Confirmation in NELI-AUTH

Figure 5 shows the operation process of NELI-AUTH.

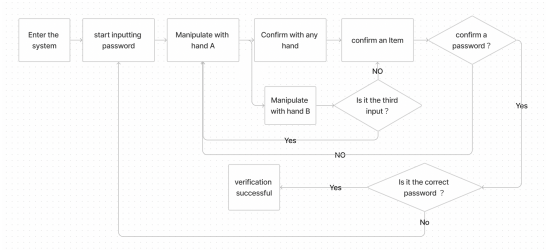

Figure 5: The flowchart of NELI-AUTH

There are three types of confirmation operations included in the flow to guide the input process:

- Confirming an *element*: Keep one controller in the input state and start the input of another controller, which is regarded as the confirmation of the *element* input by the first controller.
- Confirming an *item*: When three *elements* are entered consecutively, they are automatically identified as one *item* and the input of the next *item* begins. As an alternative, users may press the thumbstick to complete the entry of an *item* in advance.
- Confirming a password: For completing the password input, users could press the A or X buttons, and for returning to previous *items*, they could press the B or Y buttons.

4.2 Development

The scheme prototype was developed with the Unity platform, implemented with Oculus SDK, and packaged and released as Android applications.

5 Innovation

5.1 About Security and Concealment

NELI-AUTH enables users to confirm *items* by either pressing a thumb or entering three *elements* continuously. During continuous thumbstick operation, it is difficult for bystanders to observe the action of pressing the thumbstick. Even if they record the direction in which the thumbstick is operated, it is also difficult for them to identify the password by correctly dividing the operation sequence. This is the essence of NELI-AUTH.

For example, in figure 6, it can be observed by bystanders that the user's hand movements for the four sets of passwords are exactly the same. However, due to the different timings for confirmation, the results are completely different.

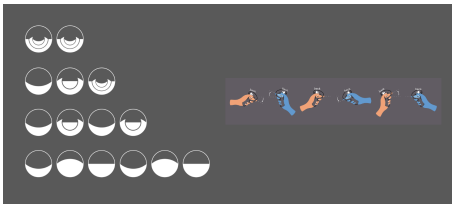

Figure 6: Four passwords produced by the same elements selection

5.2 About Usability

This scheme utilizes the pitch and orientation of the thumbstick to select the spherical area, which corresponds to the users' habit of holding the controller with a handle and their awareness of three-dimensional space.

Moreover, an effective 3D user interface displays the spherical area, a dotted plane indicates the sphere's surface, and the rotating sphere enhances the user's spatial perception.

In addition, the design of graphic codes makes it easier for users to recall passwords.

References

[1] G. Hadjidemetriou, M. Belk, C. Fidas, and A. Pitsillides. Picture passwords in mixed reality: Implementation and evaluation (2019). *ACM SIGCHI Human Factors in Computing Systems (CHI 2019)*, 2019.

[2] M. Khamis, F. Alt, M. Hassib, E. von Zezschwitz, R. Hasholzner, and A. Bulling. Gazetouchpass: Multimodal authentication using gaze and touch on mobile devices. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, pp. 2156–2164, 2016.