Context or Digits? Balancing Memorability and Efficiency in Virtual Reality Authentication

Yuxuan Huang
yhuang94@ncsu.edu
North Carolina State University
Raleigh, North Carolina, USA

Qiao Jin
qjin4@ncsu.edu
North Carolina State University
Raleigh, North Carolina, USA

Tongyu Nie
nie00035@umn.edu
University of Minnesota
Minneapolis, Minnesota, USA

Victoria Interrante
interran@umn.edu
University of Minnesota
Minneapolis, Minnesota, USA

Evan Suma Rosenberg
suma@umn.edu
University of Minnesota
Minneapolis, Minnesota, USA

arXiv:2608.29531v1 [cs.CR] 30 Aug 2026

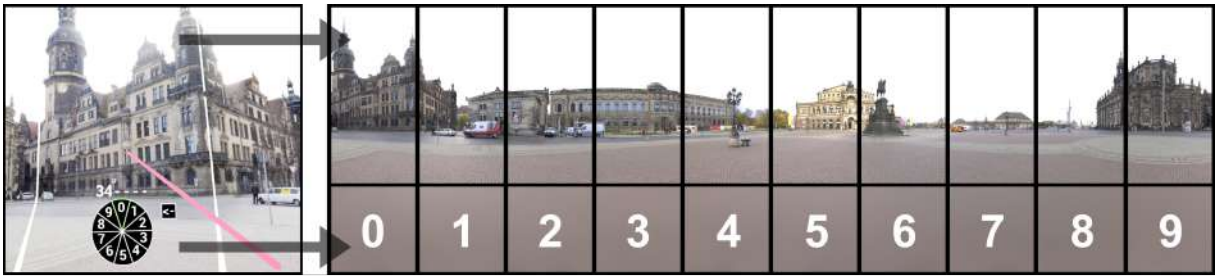


Figure 1: The Adaptive Direction-Based Authentication. The method consists of 6 virtual environments, each divided into 10 directions. Each direction is mapped to a digit from 0-9. Users can rely on the context cues for better memorability when unfamiliar with the digit sequence. They can also enter the digits directly for higher efficiency after gaining sufficient familiarity.

Abstract

We present Adaptive Direction-Based Authentication (ADBA), a knowledge-based authentication method for Virtual Reality that decouples users' needs temporally by enforcing password creation based on virtual environment context while supporting both context- and digit-based entries during authentication. This design prioritizes memorability for new passwords and offers both efficient and memorable options to support users' evolving needs. We conducted a remote longitudinal study with 66 participants comparing ADBA against 6-digit PINs over 2-3 weeks. The results demonstrated that ADBA achieved superior memorability and lower perceived task load. Interestingly, no participant chose to enter via digits in the study, yet they still perceived ADBA to be highly efficiency despite longer objective entry times. ADBA also provided security benefits through randomly-generated digit representations, though some degree of password homogeneity was observed in specific virtual environments. Our findings suggest that ADBA offers solid advantages to the traditional PINs, and successfully addresses the tradeoffs between efficiency, memorability, and security under the usage scenarios considered in the study.

CCS Concepts

• **Security and privacy → Usability in security and privacy**; • **Human-centered computing → Empirical studies in interaction design**.

Keywords

Virtual Reality, Authentication, Security, Privacy, Usability

ACM Reference Format:
Yuxuan Huang, Qiao Jin, Tongyu Nie, Victoria Interrante, and Evan Suma Rosenberg. 2018. Context or Digits? Balancing Memorability and Efficiency in Virtual Reality Authentication. In *Proceedings of Make sure to enter the correct conference title from your rights confirmation email (Conference acronym 'XX)*. ACM, New York, NY, USA, 11 pages. https://doi.org/XXXXXXX.XXXXXXX

1 Introduction

As Virtual Reality (VR) becomes increasingly adopted in different fields, ensuring data security and protecting user privacy becomes a critical task [8, 32, 39], and many different user authentication methods have been proposed for VR [3, 5, 27, 36, 43, 45].

Knowledge-based authentication is most widely-used due to its simplicity, hardware independence, and users' familiarity [46]. However, an apparent drawback is that it requires explicit memorization and entry for authentication, which introduces trade-offs

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
Conference acronym 'XX, Woodstock, NY
© 2018 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 978-1-4503-XXXX-X/2018/06
https://doi.org/XXXXXXX.XXXXXXX

between efficiency, memorability, and security [46]. For example, despite longer PINs theoretically provide stronger security by offering a larger password space, research has shown that the benefit is offset by users' tendency to choose weaker passwords [26, 31, 40]. Some authentication methods were designed to enhance memorability by utilizing picture memory, but they usually come at the cost of slower entry [9, 10], and conversely, methods that excel at efficiency are generally less memorable, especially with strong passwords [29]. Moreover, the 3D nature of the spatial interaction in VR gives rise to shoulder-surfing attacks during user authentication [4, 7] because the gestures and head movement associated with password entry can give away information about the password, and users typically lack the awareness of their surroundings when immersed in a VR headset, leaving ample opportunities for malicious attackers to exploit this vulnerability [11, 30, 42].

Very few methods have attempted to optimize efficiency, memorability, and security concurrently. The direction-based authentication (DBA) [17, 18] combines symbol entry and context cues to offer efficient entry method and memorable cues, and utilizes randomization to counter shoulder-surfing attack. Despite promising results, the method offered symbols and contexts in a simplistic manner without considering the temporal factor in users' needs.

We note that while both efficiency and memorability are critical for usability, they are rarely considered equally important at all times. Users are unlikely to complain about efficiency when they still struggle with memorability. Similarly, users are also unlikely still uncertain about the passwords when efficiency becomes their main concern. Therefore, although efficiency and memorability are difficult to achieve concurrently, the conflict may be resolved by prioritizing what is most needed by the users at a given time.

Additionally, prior work on VR authentication typically adopts single- or double-session experiments in which participants complete a series of tasks in laboratories [9, 12, 27, 33]. Although such designs allow efficient data collection and better control over the procedure, they compromise ecological validity. Both the experimental tasks and settings differ significantly from real-world authentication scenarios, which raises questions of whether the results of these experiments generalize to real-world contexts [28].

In this work, we tackled both research gaps identified above. Our contributions to the advancement of knowledge-based authentication in VR are as follows:

(1) We introduced a novel perspective to decouple the conflict between efficiency and memorability temporally.
(2) We revised DBA to prioritize efficiency or memorability based on users' needs.
(3) We conducted a remote longitudinal study to enhance the ecological validity of evaluation by emulating real-world authentication. To our knowledge, this is the first evaluation study for VR authentication methods with such a design.
(4) We empirically demonstrated that users do not prioritize sheer entry efficiency even under daily authentication.

2 Related Work

Knowledge-based authentication in VR can be divided into symbol-based, and context-based methods depending on the type of information users need to remember [17].

2.1 Symbol-Based Authentication

Symbol-based methods define passwords as a sequence of symbols, such as text or digits, and are widely used in our daily life. However, their usability in VR often relies on a small symbol set (e.g., a Numpad) [12, 33], since text entry with full VR keyboard is relatively error-prone and inefficient [13]. This reduction in symbol variety introduces security vulnerabilities to shoulder-surfing attacks [22, 42, 44] because the movements associated with the password entry become easier to exploit. Therefore, symbol-based authentication methods specifically designed for VR often incorporate strategies to mitigate the risk of shoulder-surfing.

One approach is to randomize the password interface [19, 24, 25]. For example, Lange et al. [21] proposed three authentication schemes using different symbol sets with randomized layout. Some approaches authenticate with subtler movements, such as *VR Pursuit* [20], which selects moving digits with continuous eye-gaze, along with other eye-gaze-based methods [2, 23, 35]. Some adopt more complicated password interfaces, such as *RubikAuth*[29], which utilizes a virtual 3D cubic PIN-pad attached to one controller. To mitigate the usability drawback, Weiss et al. [41] proposed hand redirection during PIN entry, which offsets users' actual hands by a random displacement, causing them to reach toward different locations even when choosing the same input.

Symbol-based methods are generally efficient thanks to the ease of selecting symbols on a compact PIN-pad. For example, the authentication time for RubikAuth can be under 5 seconds for a 4-digit password. However, a major shortcoming is the conflict between memorability and security as discussed earlier. RubikAuth achieves a successful recall rate of 95.24% after a week for weak passwords, but the number plummets to 61.9% and 42.86% for medium and strong passwords, respectively.

2.2 Context-Based Authentication

Context-based methods authenticate using virtual environment contexts and improve memorability by leveraging the picture superiority effect, i.e., a well-established theory that people remember pictures better than words [34]. For example, in *RoomLock*, the password is defined a sequence of objects in a virtual room [10, 11]. *LookUnlock* [9] defines the password as a combination of virtual and real-world targets. *3DPass* presents a virtual home environment and defines the "password" as a series of navigation and actions, such as entering the kitchen and turning on the lights [14].

While context-based methods generally achieves high memorability, the tasks associated with the authentication procedure, such as visual search and locomotion, can be inefficient. For example, the *3DPass* achieved a successful recall rate of 98% after a week, but the authentication took 21 seconds on average.

2.3 Direction-Based Authentication

To strike a balance between efficiency and memorability, Huang et al., proposed Direction-Based Authentication (DBA), which offers both symbols and contexts under a unifying framework [17]. Passwords in DBA are defined as a sequence of directions, corresponding to both direction symbols on a compass, and environment contexts users see in the directions. While prior work demonstrated the efficiency and memorability benefits of DBA [18], it did not

address the nuanced tradeoffs between efficiency and memorability across different usage scenarios, nor did it empirically validate the memorability advantage of DBA.

One such nuance not explicitly considered in DBA is the temporal separation of priority between efficiency and memorability, as mentioned in the introduction. Additionally, research has demonstrated the environmental reinstatement effect [38], according to which information retrieval improves when the environmental context is consistent between encoding and retrieval [37].

Based on these insights, we noted that the context cues can not only serve as easy-to-remember data on their own but may also facilitate the memorization of their symbol counterparts by providing additional environmental context for symbol recall. This is in line with our envisioning that the conflict between efficiency and memorability can be resolved temporally by prioritizing what is most needed by the users at any given stage. We revised DBA and conducted a longitudinal study with a remote design emphasizing the ecological validity of the experiment for evaluation.

3 The Adaptive Direction-Based Authentication

We present Adaptive Direction-Based Authentication, or ADBA, which is built upon DBA with revisions aimed at adapting to users' priorities. ADBA consists of a sequence of 6 virtual environments, each divided into 10 directions corresponding to the digits 0 through 9. Users create their password by selecting one direction in each environment. See Figure 1 for visual illustration.

Password Creation. In contrast to the original DBA where users can choose either symbol or context, ADBA requires users to create passwords based on context by displaying only the virtual environment but not the digits corresponding to each direction. Users point their controller at a direction to select it. A glossy frame will highlight the part of the context corresponding to the selected direction. They can then press trigger button on the controller to confirm their selected direction as part of their password.

This enforced context-based password creation offers both memorability and security benefits. The context is inherently easier to remember due to the picture superiority effect, which is more important than a quick yet potentially less memorable password setup. Additionally, since the users do not know the digit correspondence during password setup, they cannot choose weak passwords like 123456. Instead, we generate random digit sequences as the digit representations to enhance security.

Password Entry. During authentication, users are presented with both the virtual environment and a virtual radial PIN-pad that floats in front of them. The PIN-pad provides an alternative "symbol-based" entry method, and rotates as the users physically turn, similar to a compass, ensuring that the digit corresponding to the forward direction is always in front. This emphasizes the correspondence between the directions and the digits, and offers additional security against shoulder-surfing attack because the digits are not in fixed locations as in standard PIN-pads. Above the PIN-pad, a sequence of digits corresponding to the directions entered in the previous virtual environments is displayed.

Users can select either digits or contexts depending on whether they point at the PIN-pad or the environment. In either case, both the digit and the context corresponding to the selected direction will be highlighted. Users press the trigger button to confirm selection. A backspace button is also provided for correcting mis-entries.

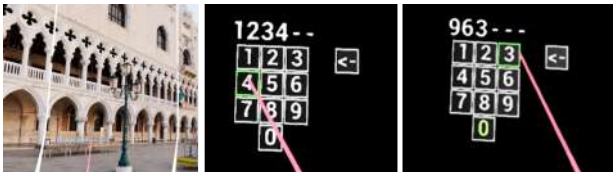


Figure 2: ADBA (left), 6-digit-PIN (middle), and random-PIN (right) during password setup. Note that the radial PIN-pad is hidden during password setup with ADBA. The two PIN-based methods share the same interface, but for random-PIN the next digit to choose is randomly-determined and highlighted in green (0 in the screenshot).

By continuing to provide context-based entry, ADBA supports users continuing to prioritize memorability over efficiency. By providing additional symbol-based entry, ADBA enables a more efficient alternative for users who has already remembered the digit representations and choose to prioritize efficiency. Additionally, the presence of the context may also cue the recall of the corresponding digit, which facilitates memorization. Overall, ADBA is a context-only method during password setup, and either remains context-only, transitions into symbol-only, or exists as a hybrid method during authentication depending on users' varying needs.

4 Methods

4.1 Study Design

We conducted a between-subject remote longitudinal study to evaluate the efficiency, memorability, and security of ADBA. The between-subject design reduces the interference between conditions, and the remote and longitudinal design allows participants to authenticate in their own environments, at their own pace, with their personal setups, and at realistic frequencies. These together contribute to a scenario that closely resembles the real-world authentication compared to within-subject or lab-based experiments.

The study consists of three conditions: 1) ADBA, 2) user-selected 6-digit-PIN and 3) randomly assigned 6-digit-PIN. See Figure 2 for visual illustrations of the three conditions. We chose to compare ADBA against PIN-based approaches because they are widely adopted and remain more efficient than the recent knowledge-based schemes. They are also structurally comparable given the identical theoretical password space (10^6). While six random digits are impractical for adoption due to memorization difficulty, they represent an ideal security scenario for 6-digit-PINs, identical to the digit representation of ADBA except without context information.

4.2 Materials

The study software was developed using Unreal Engine 5.3, and deployed as a PC-based VR application compatible with both steam VR and Meta Quest Link. The app would automatically upload data to the server every time a participant completed a password entry on their end. The virtual environments were represented by 360° high dynamic range images (HDRIs) obtained from HDRI haven [1].

4.3 Procedure

Participants first completed the screening, verified software compatibility with their setup, and provided informed consent.

The study had 4 stages that spanned across 2-3 weeks:

- **Password Setup**: Participants scheduled a Zoom meeting, during which the experimenter explained the instructions and the participants set up their password.
- **Low Frequency Entry**: Participants entered the password every 6-8 days for two times.
- **High Frequency Entry**: Participants entered the password every 1-2 days for four times.
- **Exit Survey**: Participants filled out the usability and demographics surveys.

For password setup, participants assigned to the ADBA condition were instructed to check out all directions before selecting a direction. They were also advised to focus on less noticeable details. The underlying digit representations were six randomly generated, non-sequential, non-repeated digits (e.g., no "123456" or "123246"). For consistency, participants assigned to the user-selected 6-digit PIN condition were required to choose distinct, non-sequential 6-digit sequence. They were also instructed not to use their real-world PINs for their own privacy. The randomly-generated PINs follow the same rule. Participants assigned to this condition selected the pre-determined digits highlighted in green during setup. To confirm memorization upon creation, participants must correctly enter their passwords three times to proceed. Participants were also be explicitly instructed not to write down their passwords. To minimized the incentive for participants to cheat, they were informed that, while they should try their best to remember the passwords, forgetting had no negative impact on their compensation and they would simply be reminded of the password if that happened.

Over the subsequent weeks, participants performed authentication tasks at their convenience following the required frequencies. No pre-schedule was needed as data collection happened automatically. We considered both a low and a high frequency because frequency may affect users' preferences or priorities between efficiency and memorability. Participants entered the recovery mode after 3 failed authentication attempts. In the PIN-based conditions, the correct digits were highlighted in green. In the ADBA condition, the digits were hidden and the correct directions were indicated by a green frame. We decided to remind instead of reset passwords to ensure all participants remembering a single password throughout, avoiding confounding factors for memorability.

4.4 Participants

66 participants (18F, 46M, 2NB, aged between 18 and 74) were recruited and completed the study, among which 33 were recruited through Prolific, and 33 from the university community. The sample size was calculated using G*Power with a large effect size of 0.4 and to achieve a power of 0.8 for a fixed-effects, omnibus one-way ANOVA. Participants were required to have access to a PC-VR setup for the duration of the study. They received $20 if they completed all parts of the study, prorated if they dropped out early. The study was approved by the university's institutional review board (IRB).

Due to the longitudinal nature of the study, some participants ran into unforeseeable scheduling conflicts. We decided to accept submissions that were less than 24 hours early or late. Only 6 out of the 462 task submissions fell into this category.

4.5 Measures

Entry Efficiency. We recorded the time it took for each password entry, from the time participant pressed the start button to load the authentication interface to the time the last entry was completed.

Memorability. We evaluated memorability using both the *recall rate* and the *number of entries per authentication*. Since users were allowed to correct their input, submitting incorrect passwords is more likely due to memorability issues rather than input errors.

Usability and Task Load. We administered the System Usability Scale (SUS) [6] and the raw NASA TLX [15] surveys. We also included a custom usability survey in which we asked participants to indicate their perceived efficiency and memorability in 7-point likert scale. For participants assigned to the ADBA condition, we asked if they tried to remember the digits associated with each environment. If they responded yes, we asked them to indicate the perceived effort required to remember the digits in 7-point likert scale. Lastly we asked participants for open-ended feedback.

Password Homogeneity. We focused on password homogeneity as the primary security indicator, as this was identified as a key potential vulnerability in DBA [18]. Specifically, we computed the Shannon entropy of the directions selected by users within each environment, where lower values suggest more homogeneous choices. While shoulder-surfing resistance is also an important security aspect, we omitted it due to practicality and potential privacy concerns in the remote setup. Additionally, the robustness of similar interfaces has already been demonstrated in [16, 18].

4.6 Hypotheses

Our hypotheses are as follows:

- **H1:** Participants would remember the password better with ADBA compared to both PIN-based methods.
- **H2:** There would exist an interaction effect where ADBA would be the slowest from the start, but the difference would diminish for the last entry.
- **H3:** Participants would report better usability with ADBA compared to the PIN-based methods.
- **H4:** Participants would report lower task load with ADBA compared to the PIN-based methods.

We hypothesized that ADBA would be the most memorable due to picture superiority effect (H1). We expected participants to initially experience slower entries with ADBA when searching for context, but the difference may diminish if they prioritized efficiency and shifted to digit-based entry during high frequency entries (H2). We anticipated that ADBA would result in higher perceived usability (H3) and lower reported task load (H4), as participants could authenticate in a most comfortable manner.

4.7 Data Analysis

We used Bayesian generalized linear mixed model (Bayesian GLMM) analysis for multi-observations, and Bayesian generalized linear

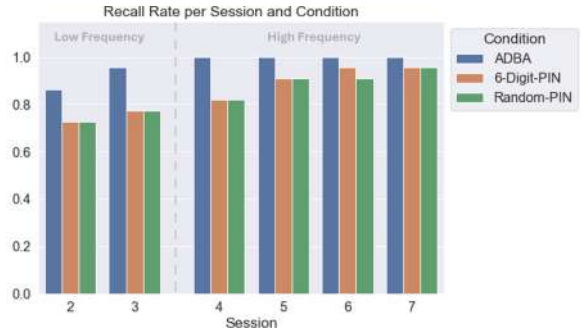


Figure 3: Recall rate per session. ADBA yielded higher recall rate consistently. Bayesian GLMM indicated P(ADBA > 6-Digit-PIN) = 0.92 and P(ADBA > Random-PIN) = 0.95 during the low-frequency entry stage.

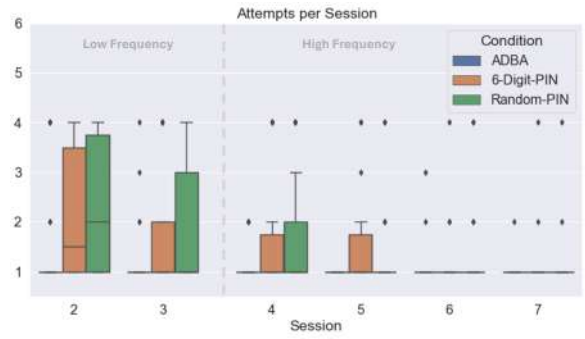


Figure 4: Number of attempts per session. Bayesian GLMM indicated P(ADBA < 6-Digit-PIN) = 0.92 and P(ADBA < Random-PIN) = 0.97 during the low-frequency entry stage.

models (Bayesian GLMs) analyses for single-observation. The analyses were performed using the 'brms' package (2.20.1) in R (4.3.1.).

We adopted GLMMs because they capture the hierarchical structure of our data: each participant completed varying number of entries across multiple sessions. A Bayesian approach was preferred over frequentist methods because it performs more robustly with small-to-medium sample sizes (22 per condition) and yields a more informative continuous estimates of posterior probabilities.

5 Results

We report descriptive statistics as mean (SD) when Shapiro–Wilk tests do not indicate departures from normality; otherwise we report median (IQR). The reported results were achieved using brm default bayesian prior (flat priors for population-level regression coefficients and Student-t priors for intercepts and group-level standard deviations). For sensitivity test, we used weakly informed priors for coefficients and the resulting posterior probabilities were generally similar to those obtained under the default priors, and substantive conclusions remained unchanged. Models were estimated using four chains with 4,000 iterations per chain, including 1,000 warm-up iterations, using the NUTS sampler. All regression models achieved good convergence ($\hat{R} = 1$). Effects were considered reliable if their 95% highest posterior density (HPD) intervals did not include zero. We report all effects with posterior probability > 85%, as Bayesian results do not rely on a binary cutoff.

5.1 Memorability

We present the memorability results across all sessions to illustrate the overall trend. However, the statistical analysis focuses on the low-frequency entry stage because memorability is most critical when passwords are newly created and infrequently used.

Password Recall. Figure 3 shows the recall rate per session. Recall rate for ADBA was the highest (Session 2: 86%; Session 3: 95%), while the 6-Digit-PIN and Random-PIN conditions showed identical performance (Session 2: 73%; Session 3: 77%).

A Bayesian GLMM with a Bernoulli likelihood and logit link was fitted to participants' binary recall outcomes, with *Condition* and *Session* as fixed effects, and random intercepts for participant ID. The posterior median estimates for condition effects, relative to ADBA, were -2.81, 95% HPD [-7.44, 0.71] for 6-Digit-PIN and -3.14, [-7.87, 0.18] for Random-PIN, both on the log-odds scale.

Pairwise contrasts indicated that ADBA yielded higher recall rates than both 6-Digit-PIN (median log-odds difference = 2.63, [-0.96, 6.90]) and Random-PIN (2.88, [-0.25, 7.73]). Although the 95% HPD intervals included zero, the posterior probabilities that ADBA outperformed the other two conditions were: P(ADBA > 6-Digit-PIN) = 0.92 and P(ADBA > Random-PIN) = 0.95. These results support H1 that participants were able to recall better in ADBA.

Entry per Session. Figure 4 shows the number of entries per session. ADBA required the fewest entries ($Mdn = 1, IQR = 0$ in both session 2 and 3), followed by 6-digit-PIN (Session 2: $Mdn = 1.5, IQR = 2.5$; Session 3: $Mdn = 1, IQR = 1$), and Random-PIN (Session 2: $Mdn = 2, IQR = 2.75$; Session 3: $Mdn = 1, IQR = 2$).

A Bayesian Poisson mixed-effects model was fit to participants' entry counts, with *Condition* and *Session* as fixed effects and random intercepts for participant ID. The posterior median estimates for condition effects, relative to ADBA, were 0.30, [-0.06, 0.67] for 6-Digit-PIN and 0.39, [0.05, 0.75] for Random-PIN.

Posterior pairwise comparisons revealed that ADBA required fewer entries than Random-PIN (Mdn difference = -0.39, [-0.75, -0.05]) and 6-Digit-PIN (-0.30, [-0.67, 0.07]). The posterior probability that DBA required fewer entries were P(ADBA < 6-Digit-PIN) = 0.92 and P(ADBA < Random-PIN) = 0.97. This result also supports H1 that ADBA required fewer attempts to authenticate successfully.

5.2 Efficiency

Figure 5 shows the entry time per session. We included the correct entries only, excluding entries during password setup and recovery.

Across all six entry sessions, the ADBA condition yielded the slowest entries ($Mdn = 25.2, IQR = 12.9$ secs), whereas the 6-Digit-PIN ($Mdn = 5.5, IQR = 3.4$ secs) and Random-PIN ($Mdn = 5.9, IQR = 3.6$ secs) conditions were substantially faster.

A Bayesian linear mixed-effects model was fit to entry times, with *Condition*, *Session*, and their interaction as fixed effects, and random intercepts for participant ID. The posterior median estimates indicated a strong main effect of condition: relative to ADBA,

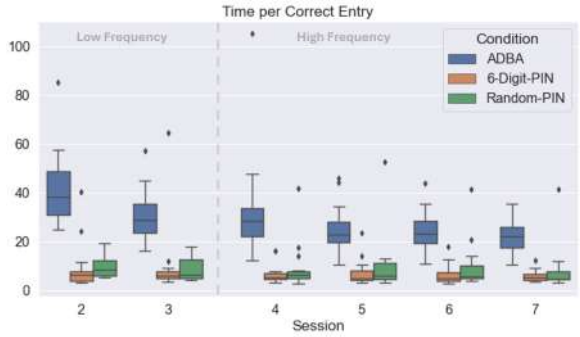


Figure 5: Correct entry time per session. Bayesian GLMM indicated main effects of Condition (ADBA was slower), Session (Entry time decreased over sessions), and the interaction (ADBA entry time decreased faster over session).

both the 6-Digit-PIN (-21.52, [-24.82, -18.28]) and Random-PIN (-19.95, [-23.30, -16.57]) showed substantially shorter entry times. Entry time also decreased across sessions (-14.34, [-18.00, -10.59]), with notable interaction effects: entry times for ADBA decreased more steeply than for the other two methods (6-Digit-PIN × Session: 11.17, [5.67, 16.54]; Random-PIN × Session: 13.12, [7.59, 18.63]).

Posterior contrasts confirmed that ADBA was consistently slower than both PIN-based methods in all sessions (median difference range: 14.4-32.1 seconds, all 95% HPD intervals excluding zero). However, ADBA demonstrated a faster improvement rate.

Interestingly, only 2 participants in the ADBA condition indicated that they attempted to remember the digits. They further indicated "disagree" and "somewhat disagree" to the statement *"It was difficult to remember the digits"*. Notably, neither switched to using digits as their primary entry method.

These findings partially support H2, as a significant interaction effect between condition and session was observed. However, this improvement was not sufficient to close the performance gap in entry speed by the end of the study, because no participant in the ADBA condition switched to the digit-based entry.

5.3 Usability

System Usability Scale. The SUS scores were similar across all conditions: 6-Digit-PIN ($Mdn = 87.5, IQR = 10.0$); ADBA ($Mdn = 83.8, IQR = 18.1$); Random-PIN ($Mdn = 83.8, IQR = 15.0$).

A Bayesian linear model revealed no credible differences across conditions: ADBA - 6-Digit-PIN = -1.79 [-9.42, 5.30]; ADBA - Random-PIN = 0.52 [-6.93, 7.94]; 6-Digit-PIN - Random-PIN = 2.42 [-5.28, 9.48]. These results do not support H3.

Perceived Efficiency and Memorability. Figure 6 summarizes participants' perceived efficiency and memorability. Bayesian ordinal logistic regression models revealed higher perceived efficiency for ADBA than for 6-digit-PIN (Mdn difference = 1.02, [-0.08, 2.21], P(6-digit-PIN < ADBA) = 0.90), contrary to its slower entry time.

ADBA was perceived as more memorable than 6-digit-PIN (Mdn difference = 1.00, [-0.12, 2.17], P(ADBA > 6-digit-PIN) = 0.89), and Random-PIN (Mdn difference = 0.905, [-0.312, 2.03], P(ADBA > Random-PIN) = 0.87), consistent with objective memorability.

These findings support H3, although the 95% credible intervals for all contrasts included zero, indicating some uncertainty.

5.4 Task Load

Figure 7 shows the NASA TLX result and a breakdown of the subscales. Participants reported the lowest perceived task load for ADBA ($M = 14.5, SD = 9.5$), followed by the Random-PIN ($M = 18.5, SD = 12.0$), and the 6-digit-PIN ($M = 20.0, SD = 15.6$).

A Bayesian linear model indicated lower perceived task load for ADBA than for the PIN-based methods. The posterior differences were ADBA - 6-Digit-PIN = -5.54, [-13.3, 1.92], and ADBA - Random-PIN = -4.05, [-11.7, 3.41]. Posterior probabilities suggested moderate evidence of lower workload for ADBA: P(ADBA < 6-Digit-PIN) = 0.93 and P(ADBA < Random-PIN) = 0.86. These result supports H4.

Bayesian ordinal logistic regression models for TLX subscales indicated strong evidence that ADBA was associated with higher physical demand than Random-PIN (P(ADBA > Random-PIN) = 0.98), and weak evidence of advantages for ADBA in mental demand (P(ADBA < 6-Digit-PIN) = 0.87; P(ADBA < Random-PIN) = 0.89) and performance: P(ADBA < 6-Digit-PIN) = 0.86.

5.5 Security

Environment	1	2	3	4	5	6
Entropy (bits)	2.56	2.18	2.77	2.36	2.61	2.70

Table 1: Shannon Entropy per Environment.

Password Homogeneity. Figure 8 visualizes the selected directions in each environment in ADBA. The Shannon Entropy for each environment is summarized in table 1. For reference, the maximum possible entropy for a 10-digit system is $\log_2 10 \approx 3.322$ bits. The entropy for each digit in the 6-digit-PIN ranged from 2.81 to 3.14 bits, and for Random-PIN, from 2.99 to 3.17 bits. Both the figure and the entropy values indicate that Environments 2 and 4 were associated with relatively low entropy. Environments 3 and 6 exhibited higher entropy, although still lower than the entropy observed in the 6-Digit-PIN condition. These results suggest that participants' choices of directions within each of the six environments were less diverse than choices of digits in the 6-digit PINs.

Vulnerability of 6-digit-PINs. Despite instructions to choose secure passwords, participants still showed a preference for weak passwords. A large portion of the passwords exhibits recognizable patterns, such as "012378", "123475", "782345", "547632", etc. Additionally, several participants asked if they could use memorable information such as birth dates or phone numbers as passwords. While this was allowed per study design and not recognizable to the experimenter, they may introduce additional vulnerabilities.

5.6 Open-Ended Feedback

Among the feedback provided by the 66 participants, 26 addressed memorability, 10 were related to interaction and visualization, 6 discussed technical difficulties, and 4 mentioned security. Notably, no participants commented on efficiency.

Most participant responses focused on the their memorization strategies. Interestingly, similar approaches were reported for the

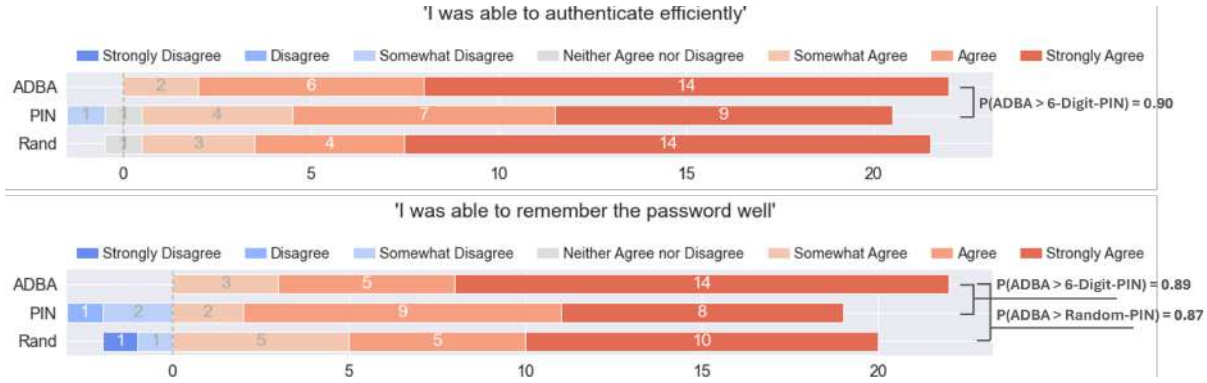


Figure 6: Likert-type responses to *"I was able to authentication efficiently"* and *"I was able to remember the password well"*. Bayesian GLMM indicated better subjective efficiency of ADBA than 6-digit-PIN, and better subjective memorability of ADBA than both PIN-based conditions.

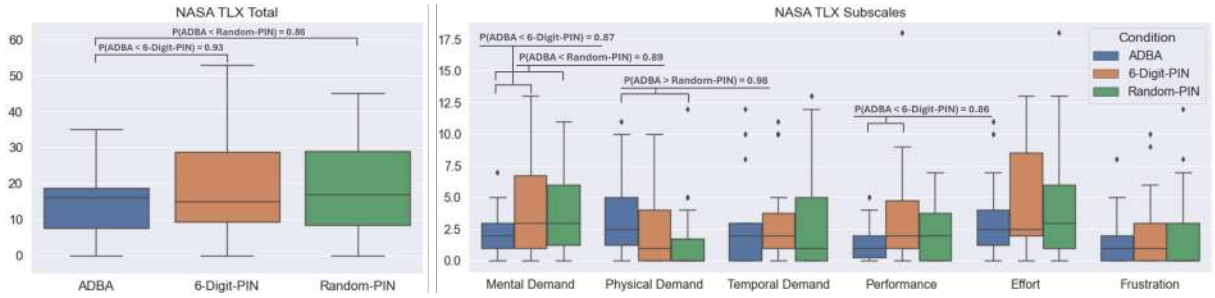


Figure 7: NASA TLX Scores and Subscale Scores. Bayesian GLMM indicated lower perceived task load with ADBA, particularly regarding lower mental demand than both 6-digit-PIN and random-PIN, and better performance than 6-digit-PIN. However, the reported physical demand for ADBA was higher than Random-PIN.

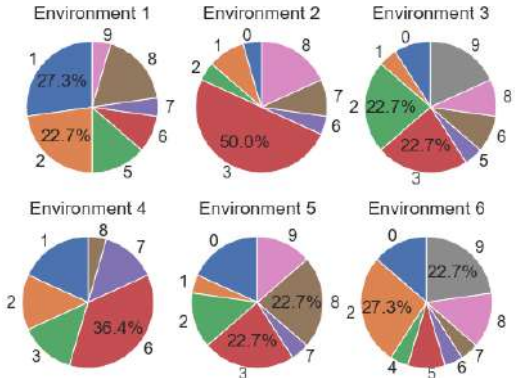


Figure 8: Summary of chosen directions. The digits represent the direction indices. The percentages indicate the proportion of participants choosing the corresponding direction. Environment 2 and 4 demonstrated noticeable homogeneity.

two PIN-based conditions. 3 participants in 6-digit-PIN condition and 5 in random-PIN condition mentioned using spatial relationships to facilitate memorization rather than relying solely on the digits. Examples include: *"My strategy was to pick a digit combination with geometric symmetry"*, *"The PIN pad was definitely the reason I was able to remember the code. I used the visualization of the button placements to memorize the code"*. Another commonly reported memorization strategy was repetition. Several participants noted that they mentally repeated the digits regularly. For instance: *"I tried to think about the password even when I didn't need to enter it"*, *"my brain naturally kept repeating the number at the end of the day"*, *"the first weeks I would occasionally remember the study (when unlocking my phone for example) and repeat to myself the password"*.

In contrast to the PIN-based passwords, most participants in the ADBA condition appeared to remember their passwords without any explicit strategy or effort. For example: *"It was surprisingly easy to remember the password. I didn't have to think about it after the initial step!"*, *"The image was near impossible to forget despite the fact that I barely tried to put to memory ... I felt significantly more confident I would remember the images over the numbers."*.

Beyond discussions of memorization strategies, three participants noted that selecting small targets on a PIN pad in VR using a laser pointer was not the most usable experience. For example: *"It's a little bit hard to point to the pin pad sometimes"*, and *"I feel the VR hand control method of entering the PIN was much harder than just a keypad for example."*.

6 Discussion

6.1 Memorability

ADBA demonstrated a clear memorability advantage over the PIN-based methods across both subjective and objective measures. This highlights that enforcing context-based password creation is key to achieving superior memorability, whereas in [18], DBA did not show such an advantage as some participants relied on symbols during password setup for convenience.

The memorability advantages can be largely attributed to the well-established picture superiority effect. An additional contributing factor lies in ADBA's reduced interference between different environments, in contrast to the reuse of the same ten digits in PIN-based systems. We observed that many incorrect PIN entries resulted from confusion about ordering (e.g., attempting "6-9-8", "6-8-9", or "8-6-9"). In contrast, ADBA users did not experience such confusion, as each of the six environments was unique.

More broadly, the reduced confusion in ADBA can extend from the positional to the password level. It is common for users to forget which PIN corresponds to which account. ADBA may mitigate this problem by using distinct environments for different authentications. Although certain visual similarities may persist across environments, they still preserve more differences than traditional PINs, where every position is drawn from the same ten digits.

A somewhat counterintuitive finding from our study was that the 6-digit PIN condition did not yield better memorability than the Random-PIN condition. A likely explanation is that participants in the 6-digit PIN condition often chose weak, patterned combinations that they assumed would be easy to recall. In contrast, participants assigned to the Random-PIN condition appeared more deliberate and attentive in memorizing their passwords.

6.2 Efficiency

Throughout the study, participants required more time to correctly enter a password using ADBA compared to the PIN-based methods. However, in contrast to this objective inefficiency, participants rated ADBA as even more efficient than the 6-Digit-PIN. This seemingly paradoxical result carries several important implications.

First, shorter entry time does not necessarily translate to more efficient authentication. Most prior authentication studies have operationalized efficiency through repeated entry of given passwords, and use the entry time as a proxy of efficiency [11, 12, 18, 20, 30]. While such tasks reasonably estimate the lower bound of input time for a given method, they do not always reflect practical efficiency during real-world authentication scenarios. In our study, participants performed full authentication tasks rather than repeated entries. Many participants using ADBA were able to authenticate successfully on the first attempt without deliberate recall. In contrast, those in the PIN-based conditions often made several incorrect attempts, potentially spending additional time for recall and only then succeeded. Thus, although the per-entry time of ADBA was longer, the total authentication duration including recall and unsuccessful attempts was not necessarily longer. Unfortunately, similar to prior work, we recorded only the time required for each individual entry and did not measure the time participants spent between entries. Therefore, the results support this interpretation as a plausible explanation, but do not provide conclusive evidence that it reflects the overall authentication time. We encourage future studies to measure the full authentication time, including the intervals between entries, rather than isolated entry times.

Additionally, contrary to our expectation and the common assumption that an authentication taking more than 20 seconds would be too slow for practical use, no participants found it necessary or preferable to switch to the faster alternative available, even under daily or every-other-day authentication. No participants even commented on efficiency in the open feedback, implying that efficiency was unlikely part of their concerns. Of course, this finding may not generalize to all possible scenarios. Authentication at higher frequencies than considered in this study, such as multiple times a day, may influence how users perceive efficiency, but the overwhelming preference for the authentication method assumed to be slow under realistic authentication tasks highlights that focusing exclusively on benchmark values such as entry time may risks overlooking what users actually perceive and value for their experience.

Overall, the results indicate that ADBA was successful in supporting users' efficiency needs under the authentication frequencies considered in the study.

6.3 Security

ADBA offers 10^6 possible combinations, exceeding the commonly used 4-digit PIN. More importantly, the expanded password space does not compromise memorability, unlike the transition from 4- to 6-digit PINs [31]. In addition, because the digit representations of ADBA passwords are randomly generated, users are prevented from creating trivial or predictable digit sequences for convenience, a common issue with 6-digit PINs [26, 40].

ADBA's robustness against observation attacks is achieved through the randomized initial direction in each environment, which produces entirely different gestures and body movements even when entering the same password. Observation resistance was not directly measured in this study. Therefore, no conclusions can be drawn regarding its performance. For reference, the DBA study [18] demonstrated robustness to observation attacks for all ADBA entry methods (symbol-only, context-only, and hybrid), albeit using a different set of environments, with each environment divided into eight rather than ten directions. Thus, the extent to which these findings generalize to ADBA remains an open question.

Results from the present study, indicate that ADBA still exhibits a degree of password homogeneity in users' choices of context directions, which could increase the predictability of passwords. It should be noted that this homogeneity is highly environment-specific rather than being intrinsic to ADBA, so it should not be interpreted as ADBA being fundamentally insecure. Instead, it highlights that the security of ADBA relies on the careful selection of virtual environments to minimize homogeneity. One possible approach is to conduct pilot studies to identify environments producing diverse user preferences. For example, in our study, environments 4 and 6 yielded relatively balanced directional choices and could serve as suitable candidates. Such pilot studies require minimal effort from participants, who only need to indicate their preferred direction in each environment. Another approach is to assign a unique set of environments to each user. For instance, AI-based generation could be employed to automatically create visually distinct environments

with diverse directional features for each application or individual user. Even if certain directional biases persist at the population level, they would be far more difficult to exploit since each environment would be unique to a single user.

The vulnerabilities of digit-based PINs have been well-documented in prior literature [26, 40] and were also confirmed in our findings. Since existing passwords were not allowed, many participants tended to choose weak, easily memorable sequences. However, even with weak passwords, the memorability performance of 6-digit-PIN remained inferior to that of ADBA.

6.4 Usability and Task Load

Despite no reliable difference in SUS scores among the three conditions, ADBA resulted in a lower perceived task load than the PIN-based methods, particularly compared to the 6-Digit-PIN. The NASA TLX subscale scores indicated differences primarily in physical demand, mental demand, and perceived performance.

Participants reported higher physical demand with ADBA because they preferred turning and searching for target, which required more physical movement than entering digits on a PIN-pad.

Participants reported lower mental demand with ADBA, primarily due to its superior memorability, with comments such as *"near impossible to forget"* and *"didn't have to think"*. They also reported higher perceived performance with ADBA compared to 6-Digit-PIN, though no reliable difference was found between ADBA and Random-PIN. The higher perceived performance relative to 6-Digit-PIN can be attributed to participants' higher recall rates and fewer attempts required to successfully authenticate with ADBA. The lack of difference between ADBA and Random-PIN may appear counterintuitive given the objectively poorer performance of the latter. A plausible explanation is that participants' perceived performance is relative to their expectation: participants were likely more confident in memorizing self-chosen 6-digit PINs, whereas those assigned random PINs had lower expectations, and thus felt they performed better than anticipated despite lower objective success.

Taken together, the results demonstrate clear advantages of ADBA over widely adopted PIN-based methods, including improved memorability and perceived efficiency, lower overall task load, and more secure digit representations. With appropriate virtual environment selection, ADBA represents a highly promising knowledge-based authentication approach for VR, and we encourage researchers and practitioners to further examine the applicability of this method.

7 Limitations and Future Work

In this study, we prioritized comparing ADBA with widely adopted 6-digit PINs in ecologically valid settings because the primary goal was to evaluate its practical adoptability rather than to quantify its improvements over its predecessor. Because DBA was not included as a study condition for direct comparison, any improvements over DBA remain inferential rather than statistically validated.

While the remote design enhanced ecological validity, participants were unobserved during the study, which limited our control over the study procedure and the extent of the data that can be collected. This trade-off is worth noting in the study design.

The requirements on user-selected PINs in this study were imposed to ensure fair comparisons across conditions and protect user privacy. However, in some real-world scenarios, users may choose insecure PINs for memorability, thus the generalizability of our findings to real-world scenarios should be interpreted with caution.

The choice of low and high frequencies in this study was constrained by logistics, as frequencies that are too high or too low would be difficult to sustain. In practice, authentication can occur at both higher (e.g., multiple times per day) and lower frequencies (e.g., weeks between logins) than those examined here, so the results may not generalize to all real-world usage scenarios. Building on these results, future work can target higher usage frequencies, under which users may be more incentivized to prioritize efficiency, to have a more thorough understanding of the performance and preferences between digit- and context-based entries.

Additionally, despite good coverage of participants across different age groups, the study had a limited sample size for detecting between-subject effects and was gender-imbalanced, which may affect the generalizability of the findings. Recruiting and balancing demographics for a remote, longitudinal study requiring personal VR access is challenging. Due to practical constraints, we focused on the minimum eligibility requirements such as access to VR headsets, and did not explicitly control for demographics like gender.

Given the promising results, future research can investigate reliable methods for selecting or generating virtual environments that promote diverse preferences to mitigate password homogeneity, which is the primary limitation of ADBA identified in this study. Beyond the approaches discussed in Section 6.3, theories and methods from visual attention research may also offer valuable insights.

Under the authentication settings considered in this study, users overwhelmingly prioritized memorability over sheer entry efficiency even under daily authentication. Future studies can explore whether higher authentication frequencies, such as multiple times a day, would affect user preferences, and deepen our understanding of the factors that shape authentication usability.

8 Conclusion

In this paper, we built upon Direction-Based Authentication and proposed Adaptive Direction-Based Authentication (ADBA) to decouple users' needs of memorability or efficiency temporally. ADBA requires passwords to be chosen based on environment contexts, but provides both the environments and a digit-based entry method during authentication. The comparison between ADBA and the widely-used PIN-based methods over a longitudinal study with varying entry frequency periods demonstrated the superiority of ADBA in terms of better memorability, lower overall task load, and higher perceived efficiency even though the passwords took longer to enter compared to the PINs. ADBA also offered security benefits, alleviating memorability and usability issues associated with expanded password length for digit-based PINs, although depending on the environment used the choices of users may exhibit varying degree of homogeneity. The results of the study showed that ADBA is a promising user authentication technique for VR given the solid advantages over the widely-used PIN-based method, but future studies are warranted to explore and validate reliable environment selection methods to mitigate password homogeneity, and look further into users' prioritization of efficiency and memorability under different authentication frequencies and settings.

References

[1] [n. d.]. HDRI Haven. https://hdri-haven.com/.

[2] Yasmeen Abdrabou, Mohamed Khamis, Rana Mohamed Eisa, Sherif Ismael, and Amr Elmougy. 2018. Engage: Resisting shoulder surfing using novel gaze gestures authentication. In *Proceedings of the 17th International Conference on Mobile and Ubiquitous Multimedia*. 469–473.

[3] Ashwin Ajit, Natasha Kholgade Banerjee, and Sean Banerjee. 2019. Combining pairwise feature matches from device trajectories for biometric authentication in virtual reality environments. In *2019 IEEE International Conference on Artificial Intelligence and Virtual Reality (AIVR)*. IEEE Computer Society, 9–97.

[4] Leon Bošnjak and Boštjan Brumen. 2020. Shoulder surfing experiments: A systematic literature review. *Computers & Security* 99 (2020), 102023.

[5] Fadi Boutros, Naser Damer, Kiran Raja, Raghavendra Ramachandra, Florian Kirchbuchner, and Arjan Kuijper. 2020. Iris and periocular biometrics for head mounted displays: Segmentation, recognition, and synthetic data generation. *Image and Vision Computing* 104 (2020), 104007.

[6] J Brooke. 1996. SUS: A quick and dirty usability scale. *Usability Evaluation in Industry* (1996).

[7] Kreider Christopher and Omar El-Gayar. 2022. Reconceptualizing Knowledge Based Authentication for Augmented and Virtual Reality Context. (2022).

[8] Jaybie A De Guzman, Kanchana Thilakarathna, and Aruna Seneviratne. 2019. Security and privacy approaches in mixed reality: A literature survey. *ACM Computing Surveys (CSUR)* 52, 6 (2019), 1–37.

[9] Markus Funk, Karola Marky, Iori Mizutani, Mareike Kritzler, Simon Mayer, and Florian Michahelles. 2019. Lookunlock: Using spatial-targets for user-authentication on hmds. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–6.

[10] Ceenu George, Daniel Buschek, Andrea Ngao, and Mohamed Khamis. 2020. Gaze-roomlock: Using gaze and head-pose to improve the usability and observation resistance of 3d passwords in virtual reality. In *Augmented Reality, Virtual Reality, and Computer Graphics: 7th International Conference, AVR 2020, Lecce, Italy, September 7–10, 2020, Proceedings, Part I 7*. Springer, 61–81.

[11] Ceenu George, Mohamed Khamis, Daniel Buschek, and Heinrich Hussmann. 2019. 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)*. IEEE, 277–285.

[12] Ceenu George, Mohamed Khamis, Emanuel von Zezschwitz, Marinus Burger, Henri Schmidt, Florian Alt, and Heinrich Hussmann. 2017. Seamless and secure vr: Adapting and evaluating established authentication systems for virtual reality. NDSS.

[13] Jens Grubert, Lukas Witzani, Eyal Ofek, Michel Pahud, Matthias Kranz, and Per Ola Kristensson. 2018. Text entry in immersive head-mounted display-based virtual reality using standard keyboards. In *2018 IEEE Conference on Virtual Reality and 3D User Interfaces (VR)*. IEEE, 159–166.

[14] Jonathan Gurary, Ye Zhu, and Huirong Fu. 2017. Leveraging 3d benefits for authentication. *International Journal of Communications, Network and System Sciences* 10, 8 (2017), 324–338.

[15] Sandra G Hart. 2006. NASA-task load index (NASA-TLX); 20 years later. In *Proceedings of the human factors and ergonomics society annual meeting*, Vol. 50. Sage publications Sage CA: Los Angeles, CA, 904–908.

[16] Yuxuan Huang, Qiao Jin, Tongyu Nie, Victoria Interrante, and Evan Suma Rosenberg. 2026. Secure Text Entry using a Virtual Radial Keyboard with Dynamically Resized Keys and Non-Intrusive Randomization. *arXiv preprint arXiv:2601.05516* (2026).

[17] Yuxuan Huang, Danhua Zhang, and Evan Suma Rosenberg. 2023. DBA: direction-based authentication in virtual reality. In *2023 IEEE conference on virtual reality and 3D user interfaces abstracts and workshops (VRW)*. IEEE, 953–954.

[18] Yuxuan Huang, Danhua Zhang, and Evan Suma Rosenberg. 2024. Direction-Based Authentication: Combining Symbolic Input and Contextual Cues for Virtual Reality Password Entry. In *2024 IEEE International Symposium on Mixed and Augmented Reality (ISMAR)*. IEEE, 681–689.

[19] Seerwan Waleed Jirjees, Ahmed Raoof Nasser, and Ali Majeed Mahmood. 2021. RoundPIN: Shoulder Surfing Resistance for PIN Entry with Randomize Keypad. *Journal homepage: http://iieta. org/journals/ijsse* 11, 6 (2021), 697–702.

[20] Mohamed Khamis, Carl Oechsner, Florian Alt, and Andreas Bulling. 2018. VR-pursuits: Interaction in virtual reality using smooth pursuit eye movements. In *Proceedings of the 2018 international conference on advanced visual interfaces*. 1–8.

[21] Tobias Länge, Philipp Matheis, Reyhan Düzgün, Melanie Volkamer, and Peter Mayer. 2024. Vision: Towards Fully Shoulder-Surfing Resistant and Usable Authentication for Virtual Reality. In *Symposium on Usable Security and Privacy (USEC) 2024: Co-located with NDSS Symposium 2024, San Diego, CA, 26th February-1st March 2024*.

[22] Jiyeon Lee, Hyosu Kim, and Kilho Lee. 2023. VRKeyLogger: Virtual keystroke inference attack via eavesdropping controller usage pattern in WebVR. *Computers & Security* 134 (2023), 103461.

[23] Jonathan Liebers and Stefan Schneegass. 2020. Gaze-based authentication in virtual reality. In *ACM Symposium on Eye Tracking Research and Applications*. 1–2.

[24] Anindya Maiti and Kirsten Crager. 2017. Randompad: Usability of randomized mobile keypads for defeating inference attacks. In *Proceedings of the IEEE Euro S&P Workshop on Innovations in Mobile Privacy & Security (IMPS)*.

[25] Yogesh Kisan Mali and Arti Mohanpurkar. 2015. Advanced pin entry method by resisting shoulder surfing attacks. In *2015 International Conference on Information Processing (ICIP)*. IEEE, 37–42.

[26] Philipp Markert, Daniel V Bailey, Maximilian Golla, Markus Dürmuth, and Adam J Aviv. 2020. This pin can be easily guessed: Analyzing the security of smartphone unlock pins. In *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 286–303.

[27] Florian Mathis, Hassan Ismail Fawaz, and Mohamed Khamis. 2020. Knowledge-driven biometric authentication in virtual reality. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–10.

[28] Florian Mathis, Joseph O'hagan, Kami Vaniea, and Mohamed Khamis. 2022. Stay home! Conducting remote usability evaluations of novel real-world authentication systems using virtual reality. In *Proceedings of the 2022 International Conference on Advanced Visual Interfaces*. 1–9.

[29] Florian Mathis, John Williamson, Kami Vaniea, and Mohamed Khamis. 2020. Rubikauth: Fast and secure authentication in virtual reality. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–9.

[30] Florian Mathis, John H Williamson, Kami Vaniea, and Mohamed Khamis. 2021. Fast and secure authentication in virtual reality using coordinated 3d manipulation and pointing. *ACM Transactions on Computer-Human Interaction (ToCHI)* 28, 1 (2021), 1–44.

[31] Collins W Munyendo, Philipp Markert, Alexandra Nisenoff, Miles Grant, Elena Korkes, Blase Ur, and Adam J Aviv. 2022. " The Same {PIN}, Just Longer": On the ({In) Security} of Upgrading {PINs} from 4 to 6 Digits. In *31st USENIX Security Symposium (USENIX Security 22)*. 4023–4040.

[32] Blessing Odeleye, George Loukas, Ryan Heartfield, Georgia Sakellari, Emmanouil Panaousis, and Fotios Spyridonis. 2023. Virtually secure: A taxonomic assessment of cybersecurity challenges in virtual reality environments. *Computers & Security* 124 (2023), 102951.

[33] Ilesanmi Olade, Hai-Ning Liang, Charles Fleming, and Christopher Champion. 2020. Exploring the vulnerabilities and advantages of swipe or pattern authentication in virtual reality (vr). In *Proceedings of the 2020 4th International Conference on Virtual and Augmented Reality Simulations*. 45–52.

[34] Allan Paivio, Timothy B Rogers, and Padric C Smythe. 1968. Why are pictures easier to recall than words? *Psychonomic Science* 11, 4 (1968), 137–138.

[35] Vijay Rajanna, Adil Hamid Malla, Rahul Ashok Bhagat, and Tracy Hammond. 2018. DyGazePass: A gaze gesture-based dynamic authentication system to counter shoulder surfing and video analysis attacks. In *2018 IEEE 4th International Conference on Identity, Security, and Behavior Analysis (ISBA)*. IEEE, 1–8.

[36] Yiran Shen, Hongkai Wen, Chengwen Luo, Weitao Xu, Tao Zhang, Wen Hu, and Daniela Rus. 2018. GaitLock: Protect virtual and augmented reality headsets using gait. *IEEE Transactions on Dependable and Secure Computing* 16, 3 (2018), 484–497.

[37] Steven M Smith. 2013. Effects of environmental context on human memory. *Sage handbook of applied memory* (2013), 162–182.

[38] Steven M Smith and Edward Vela. 2001. Environmental context-dependent memory: A review and meta-analysis. *Psychonomic bulletin & review* 8 (2001), 203–220.

[39] Sophie Stephenson, Bijeeta Pal, Stephen Fan, Earlence Fernandes, Yuhang Zhao, and Rahul Chatterjee. 2022. SoK: Authentication in Augmented and Virtual Reality. In *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, 1552–1552.

[40] Ding Wang, Qianchen Gu, Xinyi Huang, and Ping Wang. 2017. Understanding human-chosen pins: characteristics, distribution and security. In *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*. 372–385.

[41] Yannick Weiss, Steeven Villa, Jesse W Grootjen, Matthias Hoppe, Yasin Kale, and Florian Müller. 2024. Exploring Redirection and Shifting Techniques to Mask Hand Movements from Shoulder-Surfing Attacks during PIN Authentication in Virtual Reality. *Proceedings of the ACM on Human-Computer Interaction* 8, MHCI (2024), 1–24.

[42] Yi Wu, Cong Shi, Tianfang Zhang, Payton Walker, Jian Liu, Nitesh Saxena, and Yingying Chen. 2023. Privacy leakage via unrestricted motion-position sensors in the age of virtual reality: A study of snooping typed input on virtual keyboards. In *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE, 3382–3398.

[43] Shanhe Yi, Zhengrui Qin, Ed Novak, Yafeng Yin, and Qun Li. 2016. Glassgesture: Exploring head gesture interface of smart glasses. In *IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications*. IEEE, 1–9.

[44] Tongyu Zhang, Yiran Shen, Ning Chen, Guoming Zhang, and Yuanfeng Zhou. 2025. AirtypeLogger: How Short Keystrokes in Virtual Space Can Expose Your Semantic Input to Nearby Cameras. *IEEE Transactions on Visualization and Computer Graphics* (2025).

[45] Huadi Zhu, Wenqiang Jin, Mingyan Xiao, Srinivasan Murali, and Ming Li. 2020. Blinkey: A two-factor user authentication method for virtual reality devices. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 4, 4 (2020), 1–29.

[46] Moshe Zviran and Zippy Erlich. 2006. Identification and authentication: technology and implementation issues. *Communications of the Association for Information Systems* 17, 1 (2006), 4.

Received 20 February 2007; revised 12 March 2009; accepted 5 June 2009