The (Un)suitability of Passwords and Password Managers in Virtual Reality

Emiram Kablo
Paderborn University
Germany

Yorick Last
Paderborn University
Germany

Patricia Arias-Cabarcos*
KASTEL Security Research Labs
Germany

Melanie Volkamer
Karlsruhe Institute of Technology
Germany

***Abstract*—As Virtual Reality (VR) expands into fields like healthcare and education, ensuring secure and user-friendly authentication becomes essential. Traditional password entry methods in VR are cumbersome and insecure, making password managers (PMs) a potential solution. To explore this field, we conducted a user study (n=126 VR users) where participants expressed a strong preference for simpler passwords and showed interest in biometric authentication and password managers. On these grounds, we provide the first in-depth evaluation of password managers in VR. We report findings from 91 cognitive walkthroughs and expert reviews, revealing that while PMs improve usability, they are not yet ready for prime time. Key features like cross-app autofill are missing, and user experiences highlight the need for better solutions. Based on consolidated user views and expert analysis, we make recommendations on how to move forward in improving VR authentication systems, ultimately creating more practical solutions for this growing field.**

***Index Terms*—Virtual reality, password managers, security, authentication, usability**

I. Introduction

The emerging field of Virtual Reality (VR) is expected to see growing adoption beyond entertainment, expanding into domains such as the military, healthcare, industry, and education. Therefore, it is crucial to implement user authentication mechanisms that make sure only authorized individuals have access to VR services and related data. The most prevalent authentication method in VR, passwords, has reached a breaking point due to their lack of usability [43]. Entering secrets using VR controllers or free-hand interactions is cumbersome, slow, and error-prone, particularly when dealing with complex and lengthy character combinations. From a security perspective, these gestures lack shoulder-surfing resistance, leaving them vulnerable to external observation attacks [22, 12, 44].

To approach the VR authentication problem, current research is mostly focused on proposing solutions that leverage VR capabilities to support immersive and user-friendly mechanisms [32, 25, 44, 22], but the process from research to real-world deployment will take time. As it happened in other scenarios like authentication for web services or smartphones, moving away from passwords completely becomes challenging due to inertia and their easiness to deploy [5].

To facilitate this transitory period dealing with passwords in VR, we research: 1) the experience with current methods and desires of users for alternative authentication mechanisms; and 2), the suitability of password managers (PMs) to support VR users. We investigate PMs since they are a recognized approach to enhance both security and usability in dealing with passwords [4, 35]. Our survey indicates a growing interest in integrating PMs into VR, a trend supported by recent releases of VR-specific PMs. The demand is expected to grow given that web browsing is a non-negligible use-case in VR, and that passwords remain the most frequent authentication method encountered by VR users [43]. However, no prior studies explore password managers' applicability to VR. Our research questions and contributions are summarized below.

[RQ1] What are user experiences with authentication in VR, their password manager behaviors and suggested improvements?

We conducted a survey-based user study (n=126) with VR users to explore their interactions with authentication in VR, covering used mechanisms and their usability and security perceptions, partially building on prior work [43]. We substantially extended the scope to cover user needs and suggested improvements for authentication in VR, as well as password manager adoption. We have also considered a more diverse sample (less biased towards males and using VR for purposes other than gaming).

Our findings indicate that users choose simpler passwords for convenience, confirming previous research [43]. New insights revealed challenges in account creation, with limited authentication options and no automated password generation. 27% of our participants used PMs for VR accounts, while 67% of non-users considered adopting a PM on their headset to simplify logins. This usage statistics and interest on PMs motivates our second research question.

[RQ2] How suitable are current password manager solutions for VR as evaluated by experts?

In response to our survey results highlighting demand, we conduct the first comprehensive review of password managers' suitability and features in VR. Specifically, we conduct qualitative expert reviews of seven popular PMs on two VR headsets, including PMs that are specifically designed for VR, and covering standalone, browser-based, extension-based, and web-based versions. We analyzed the usability through 91 cognitive walkthroughs (7 PMs across 13 tasks)

*Current affiliation: European Commission, Joint Research Centre (JRC), Ispra, Italy.

[23], heuristic evaluations using Nielsen's rules [31], and VR-specific usability principles [30]. We further expanded the evaluation with a 29-criteria framework covering usability, deployability, accessibility, and security aspects [43, 5].
Password managers in VR reduce the need to switch between real and virtual worlds by eliminating the hassle of recalling passwords, outperforming traditional VR password input in usability but with key limitations. The only standalone VR PM lacks features like autofill, password editing, and secure configuration. No PM could autofill across apps, highlighting the need for better integration. A VR-specific browser PM had vulnerabilities exposing usernames and stored site data despite passcode protection, which could be easily circumvented as well. Common design flaws included nested menus, icon overuse, and poor password strength indicators.

Our findings show that most participants rely on passwords and engage in risk-prone behaviors in VR. They see potential in password managers and desire broader availability. We recommend enhancing authentication tools, including PMs, to address current research gaps in VR authentication.

II. Related Work

Authentication methods in VR. Previous studies proposed modified or novel authentication schemes for VR, developed in the lab and evaluated for performance and usability. However, many of these prototypes were not based on prior user studies and did not address actual user needs. We complement this line of work by surveying users and confirming that ongoing research indeed aligns to user needs.

George et al. [12] found PINs and patterns generally usable and secure for VR, though 18% of 400 secrets were guessed within three attempts due to visible controller movements. Länge et al. [22] showed 4-digit PINs were highly usable but vulnerable to shoulder surfing, while newer schemes improved security at a usability cost. Sadik and Ruoti [39] observed that users weaken passwords without managers and struggle with virtual keyboards. Overall, our findings confirm that PINs and patterns offer high usability but lower perceived security, whereas passwords are harder to enter yet seen as more secure.

Several studies have proposed novel authentication schemes, predominantly biometric-based [25, 36]. Our research confirms that this trend aligns with user needs, as we included a more diverse sample compared to previous studies [17]. In 2021, Jones et al. [17] reviewed VR authentication literature, emphasizing studies with user participation. They found a lack of diversity, with more male participants than female, often without gender reporting, and a significant absence of elderly individuals.

Our survey was partially built on Stephenson et al.'s work from 2022 [43]. They evaluated authentication mechanisms in AR and VR, surveying 139 AR/VR users and developers and theoretically analyzing novel research and existing technologies. While their work did not cover password managers, their findings highlight that traditional passwords are impractical in VR, leading to workarounds, and suggesting the integration and adoption of PMs in VR. Similarly, recent work by Düzgün et al. [9] recommended PMs to support current knowledge-based authentication methods after conducting with security and HCI experts to collect 123 concept ideas. This underscores the need for our study, focusing on password management technology.

Bonneau et al. [5] developed a framework to evaluate authentication schemes based on Usability, Deployment, and Security criteria. Their analysis of 33 web authentication mechanisms schemes and two desktop PMs highlighted the challenges of replacing passwords, as no alternative scheme fully meets all criteria. Password managers, however, showed significant advantages, aiding users in managing passwords effectively. Their analysis framework has been adapted for mobile authentication [21], and for AR and VR, incorporating accessibility criteria to address the unique interaction methods of these environments. We rely on these criteria for conducting our expert evaluation of password managers in VR.

Password Managers. While no prior research has addressed the usability and adoption of password managers in VR, and therefore remaining underexplored, many researchers have studied password managers in other contexts such as desktop PCs [4, 42], mobile phones [41], or educational institutions [26], and among different user groups [35, 37]. Other studies explored credential audits [19, 15], setup and migration behaviors [1, 29].

Apart from user studies, Simmons et al. [42] categorized PM use cases and design paradigms, using cognitive walkthroughs to evaluate desktop PMs. They found extension-based PMs challenging to set up, browser-based ones lacking functionality and a locking feature, and interface issues like nested menus and excessive icon use. We build on their approach to review seven password managers in VR, comparing findings to gain insights into their usability in this context.

Further, a significant amount of research exists focusing on the security of password managers [11, 34, 33]. Fahl et al. [11] analyzed the security of 22 mobile password managers, including LastPass and 1Password, revealing that Android apps could exploit clipboard functionality to access copied credentials without requiring permissions. They found all PMs used Advanced Encryption Standard for vault protection. Oesch et al. [34] later showed that generated passwords in browser- and extension-based PMs remain vulnerable to guessing attacks. By 2021, Oesch et al. [33] reported mobile PMs to be less secure than desktop versions. We evaluated the security of password managers in virtual reality using a theoretical framework.

III. User Survey Methodology

Study Design. To explore users' experiences and needs in VR authentication, we conducted a survey, consisting of four blocks of questions, and demographics. The first block (Q1-Q4) asked when participants had to authenticate in VR, which methods they used, and their overall satisfaction. The second block (Q5-Q8) focused on perceived usability and security, where participants rated specific VR authentication methods on a five-point Likert scale and explained their

ratings. The third block (Q9-Q14) addressed account creation, password creation behaviors, and password management on VR devices. The fourth block (Q15-Q21) gathered suggestions for improving VR authentication and investigated participants' willingness to adopt password managers.

The first two blocks of questions are based on Stephenson et al.'s questionnaire [43]. Our extended questionnaire was designed to provide deeper insights into user-centered authentication improvements and the potential use of PMs for VR users.

Recruitment. Participants were recruited via Prolific. Eligibility required being over 18, fluent in English, and a VR user. A screening questionnaire assessed VR usage and authentication experience; only eligible respondents were invited to the main survey. A target sample of N = 120 was set for this survey. Prior guidance suggests that qualitative survey datasets often include dozens to 100+ respondents to ensure sufficient thematic and conceptual coverage [6]. The selected sample size therefore supports robust inductive coding and pattern identification following established qualitative analysis approaches [28]. A pilot test with six participants helped refine questions and estimate completion time.

Data Analysis. Our analysis focused on capturing under-explored perspectives in VR authentication, so we limited quantitative data analysis to descriptive statistics without statistical testing. Open-ended questions were analyzed using an iterative, inductive coding approach [28]. One researcher developed a codebook, and coded the dataset while a second researcher used the same codebook to code the same dataset independently. Intercoder reliability, assessed using Cohen's Kappa [7], with 0.71-0.93, indicated substantial to almost perfect agreement [27].

The survey questionnaires, and the final codebook including kappa values are available in the Appendix.

Ethics. The user study was approved by our university's Institutional Review Board. The survey complied with GDPR regulations, and all data collection was conducted using a LimeSurvey instance hosted on university servers. The consent form is provided along with the survey. Participants were fairly compensated, receiving 1 EUR for the 5-minute screening questionnaire and 4 EUR for the main 20-minute survey.

IV. Survey Results

The survey was conducted between June 2023 and April 2024, with 797 participants completing the screening. Among them, 195 (24.5%) reported never having authenticated in VR. Non-smartphone VR users most commonly cited that authentication was unnecessary for their device or app (44%) or that they did not own the device (41%), which was often shared or owned by others. Additionally, 16% had someone else authenticate for them, typically for convenience, while four noted that authentication was unnecessary for private or personally owned devices.

Following our sampling strategy, we selected 126 active VR users distributed across usage categories. The sample consisted primarily of young adults (80% aged 18–34), with 65% identifying as male, 32% as female, and 3% as non-binary or not responding. Participants showed relatively high education (see external Appendix for an overview of demographic details). Although recruitment targeted users from four different domains, authentication experiences and perceptions were found to be broadly similar across them.

A. RQ1 - VR Authentication Experiences

We asked participants to list their three most frequently used VR apps to understand their authentication exposure. We then tested these apps on VR devices to investigate their authentication methods. Most apps require textual passwords, paired accounts, or software-based tokens. For example, YouTube VR on Meta Quest devices requires a 6-symbol code and Google account login on a secondary device. Authentication in VR browsers varies by website, using methods like passwords, one-time passwords, single sign-on, and federated identity systems. Overall, textual passwords were the most common authentication method.

80% reported that authentication was required during the initial device setup. Additionally, 55% mentioned having to authenticate either while setting up or after opening an app for the first time. 29% needed to authenticate before making a purchase, 17% had to authenticate each time they opened an app, and 13% required authentication before every device usage. The most used authentication method in VR by our participants were passwords (68%). The second most used method was pairing with another device (57%), followed by entering a PIN (54%).

Perceived Usability and Security. Figures 1 and 2 present the frequency of authentication methods used and the corresponding mean ratings for perceived easiness and security. Overall, participants rated most authentication methods as easy to use in VR. PINs achieved the highest usability score (M = 4.63, SD = 0.67), described as quick to enter (24), easy to remember (16), and well suited to VR due to their short numeric format (5). Passwords followed (M = 4.07, SD = 1.14); despite being familiar (9), users reported difficulties with text input (19) and recalling complex credentials in immersive settings (11). One person noted frustration when relying on external password managers, showing that perceived ease depended on integration rather than the mechanism itself.

For perceived security, passwords again ranked highest (M = 4.38, SD = 0.92). Participants linked this to confidence in their own password practices and (21), while two trust the VR platform. The visual masking of input reinforced feelings of security for one person, though four participants still voiced concern about being observed while entering credentials. Unlock patterns were seen as least secure (M = 3.75, SD = 1.29) because gestures could reportedly easily be observed or replicated (9).

Account Creation. Roughly 40% of participants had created an account for or within a VR environment. These accounts were mainly for gaming, device setup, or accessing applications. The average satisfaction with the account creation process was slightly positive (M = 3.76, SD = 1.01), largely

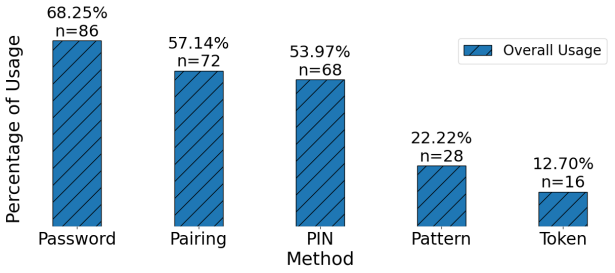


Fig. 1: Authentication methods used by participants (in percentages and absolute numbers), sorted from highest to lowest.

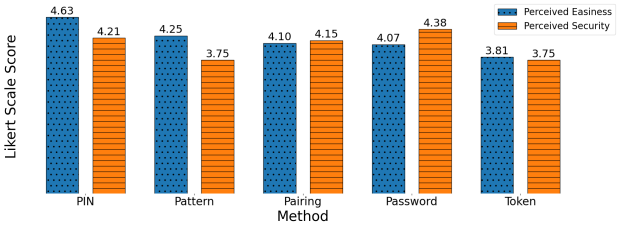


Fig. 2: Perceived ease and security of authentication methods rated by participants on a Likert scale from 1 (very hard to use/not secure) to 5 (very easy to use/very secure), sorted by ease scores (highest to lowest).

due to participants' familiarity with similar procedures on other devices. One participant mentioned having no issues because they use the same password for all accounts.

Nevertheless, several participants expressed frustration with aspects of the VR account setup, such as difficulties with controller input (8) or the lack of alternative authentication options (1). When selecting passwords for new accounts, some participants (5) reported choosing simpler passwords for convenience and easier input in VR. Others (18) preferred reusing the same or similar passwords across accounts to simplify memorization.

B. RQ1 - PMs and Improvements

Password Managers. A high number of participants (81%) reported using a PM in general, both within and outside VR. The primary reasons for adoption were convenience and security: 45 participants valued not having to remember multiple credentials, and 11 appreciated the secure storage of passwords. The main reasons for non-adoption were trust issues (15), including concerns about potential breaches, fear of losing access, or reluctance to rely on PMs for critical accounts. Additionally, seven participants preferred managing passwords manually, while others mentioned lack of awareness, cost, or limited time for setup.

Regarding VR, 27% of participants reported using a PM in VR. Among the remaining participants, including non-users, 67% indicated that they would consider using one in the future. Two thirds of this group preferred using a PM directly on the VR device, citing reasons such as the convenience of automated logins (8), cross-device synchronization (6), and reduced frustration with password input (3). Two participants emphasized avoiding the need to remove the headset, and another noted willingness if the tool became available on their device. The rest favored using a PM on an external device, motivated by better input methods (7) and stronger perceived security (4), while two expressed distrust toward PMs integrated into VR. Despite the potential benefits, 33% of participants remained hesitant to adopt PMs for their VR use, repeating similar concerns noted among current non-adopters. One participant also mentioned difficulty typing their PM's primary password in VR and therefore preferred entering individual passwords manually.

Suggested Improvements. When asked if VR authentication could be improved, 61% of our participants responded affirmatively. As alternative methods, 23 participants suggested biometric solutions, such as iris scanning, fingerprint, voice, or facial recognition. Seven participants specifically mentioned the need for VR-friendly solutions. Thirteen participants recognized VR as an innovative technology that is still evolving and thus requires improvement, including the development of novel solutions: *"Right now, most VR platforms rely on usernames and passwords to verify users' identities, you'd think we could come up with something more innovative."* (P209). Fifteen participants suggested using more secure mechanisms, such as blocking external screens while authenticating, introducing more complex and longer methods, multifactor authentication (MFA), or releasing regular security updates.

Further, 28 participants made suggestions regarding usability, interface, and interaction aspects, such as faster authentication, better input methods, and a larger virtual keyboard. Three participants specifically mentioned the importance of integrating PMs into the VR environment.

V. Expert Review Methodology

To address the survey findings indicating interest on PMs and the potential to improve current authentication flows, we examined the availability and features of PMs for virtual reality. To get an impression of how those flows look like in VR, we included an example in Figure 3.

We chose seven PMs for review based on their type, availability, and popularity, and tested them in the most frequently used device by our survey participants (Meta Quest). We consider four types of PMs:

VR-Standalone PM: A VR-native app, i.e., an application specifically designed for VR environments, which can be downloaded from the app store and installed on the headset.

Browser-based PM: PMs that are directly integrated into VR web browsers.

Extension-based PM: Browser extensions that can be downloaded and installed in a VR browser.

Web-based PM: Password managers accessible through a web interface on any device with a browser.

Our list of selected PMs to review includes the only VR-standalone PM (LastPass for Meta Quest), one browser-based

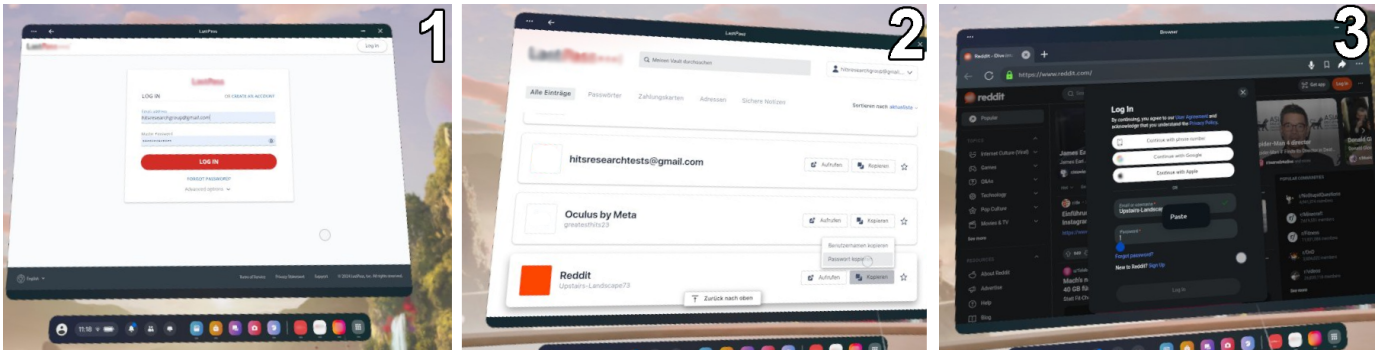


Fig. 3: Example authentication flow in VR, showing a login process to Reddit with the LastPass password manager app, where credentials were copy and pasted into the dedicated fields in the browser.

PM (Meta Quest browser password manager), an available extension for the Meta Quest browser (LastPass extension), and four web-based PMs (LastPass, 1Password, Dashlane, Bitwarden). The selected web-based PMs are among the most popular, according to rankings [10]. We used premium versions of LastPass, 1Password, and Dashlane, as free versions lack multi-device support and typical users own more than one device. While other PMs can be installed through sideloading, we focus exclusively on those available through official app stores or extension marketplaces within VR. Screenshots of the selected PMs are in the external Appendix, Figure 3.

Cognitive Walkthroughs. We evaluate all selected managers on a common set of cognitive walkthrough (CW) tasks that are relevant when dealing with textual passwords to ensure a fair comparison and determine feature availability across all PMs. We based on the tasks from the analysis of desktop PMs conducted by Simmons et al. [42], tailoring them to our VR scenarios. We cover 13 tasks: setup the password manager in VR, registering a credential in the manager, login with stored and unstored credentials, updating a credential and login with it, removing a credential stored in the manager, login from a VR without a PM, creating an account, (un-)locking the PM, ensuring safe settings, and storing non-credential data in the PM. VR users increasingly authenticate to web services, social platforms, productivity applications, virtual marketplaces, and gaming applications that require authentication. Thus, users need to perform tasks from the core password-management lifecycle in VR: need to store and retrieve credentials, create accounts, update passwords, and manage access to the password manager directly in VR. These tasks are shaped by VR-specific constraints: textual input through virtual keyboards, controllers, hand tracking, or gaze can be cumbersome and error-prone, while authentication may interrupt immersive activities by transitions between real and virtual world or expose credentials to nearby observers. Locking and unlocking the manager is particularly important because VR headsets are often shared among household members, friends, or colleagues. We test these tasks to identify challenges in performing core password-management activities in VR. None of the tasks required authentication methods beyond textual passwords, either within or outside VR, such as pairing. Consequently, we did not assess such methods in our expert reviews. Though some existing passwords were created on other devices and used in VR to login, or store. While the reference study evaluated managers across 17 different tasks, we have removed four tasks which do not fit into our context, namely: login from multiple subdomains, set up and sync on a secondary device, complete a credential audit, and recover access to the manager. We expect these tasks to be more complex or infrequent, and therefore likely to be carried out on the user's primary device(s), such as desktop or mobile devices, rather than in VR.

Heuristic Evaluation. During the CWs, we applied usability heuristics to identify design problems in the PMs' interfaces. According to the Nielsen Norman Group, their 10 usability heuristics are also applicable in the context of VR [18]. Additionally, Murtza et al. [30] introduced a new set of heuristics for usability inspections of VR systems: *Immersion* (referred to visual realism including resolution, lens flares, frame rates, and sounds), *Glitchiness* (referred to streamlined experience by keeping systematic glitches low), and *Minimize switching between actual and virtual world* (the system should be able to rely on itself for all usage). From the latter, most heuristics are related to 3D apps in virtual environments, or consider physical movement. Since PMs in VR, and the inputs for passwords, for VR are only available as 2D applications, we chose three relevant heuristics from the list and added them to our list of heuristics.

VR-UDAS Framework. To extend the evaluation of managers beyond interface usability, we have employed the evaluation framework to assess and compare authentication mechanisms initially developed in [5] and subsequently adapted for AR/VR in [43]. The framework includes 20 Deployability, Usability, Accessibility, and Security criteria from Stephenson et al. [43], focusing on benefits relevant for users. We also added the 9 security criteria from the original framework by Bonneau et al. [5] in order to provide a more solid analysis of the security of PMs. Since [43] used the framework for both AR and VR, we have minimally adapted the descriptions to be VR-specific (i.e., *Mature-for-VR*). We call this 29-criteria

framework **VR-UDAS** and apply it to compare how well PMs perform in VR with respect to relevant authentication methods available in VR, passwords and iris scanning, as evaluated in [43].

A detailed description of the thirteen tasks, the heuristics used, and the framework criteria are available in the external Appendix.

Review Execution. Three researchers conducted the expert review independently, aligning with Nielsen's recommendation to involve 3–5 evaluators [31]. This range has been shown to balance effectiveness and efficiency, as three reviewers are sufficient to identify the majority of usability issues while maintaining a manageable scope for analysis. Two evaluators are junior researchers specializing in usable security, with one focusing specifically on VR security and privacy. Both work as teaching assistants in the field and conduct workshops on usability testing at their institution, demonstrating proficiency in the methodologies. The third evaluator is a senior researcher and lecturer with extensive experience in usable security and privacy, further enhancing the rigor and depth of the evaluation. The evaluation consisted of documenting heuristic violations and compliance issues encountered during task completion. The evaluators employed the think-aloud method, recording both the VR device screen and their verbal comments to enhance the quality of post-task evaluation. The four analysis questions from the CW approach were considered and addressed [40].

The evaluation proceeded by applying the VR-UDAS framework criteria to conduct a semi-structured assessment of the managers, following guidelines in [43, 5]. The analysis was based on insights gathered from our CW and heuristic evaluation, supplemented by recorded material and hands-on testing with the actual device when necessary. This review was conducted by the first two authors. Similar to the methodological approach in [5], one reviewer began by scoring each scheme column, followed by the second one reviewing the scores. Disagreements were discussed and resolved collaboratively between the two authors, involving a third member of the team to facilitate the discussion when consensus could not be reached.

We conducted the reviews of all PMs using the Meta Quest Pro running Meta Horizon OS build version 66.0 and the Meta Quest 2 with version 68.0 (see external Appendix for version details). The reviews were conducted on different days; however, we ensured that the PM and operating-system versions remained unchanged throughout the evaluation. Before each reviewer evaluated a PM, we reset the manager to its initial state, ensuring that every review was conducted independently and without influence from prior configurations or stored data.

VI. Expert Review Results

A. RQ2 - Password Manager Usability in VR

We describe the findings of the cognitive walkthroughs starting with a comparative overview of supported features, summarized in Table I, then identify critical usability issues.

Supported Features. At first glance, we can observe that the only VR-native application, LastPass VR app, offers the fewest features. It provides a basic view of the vault, allowing users to launch websites and copy credentials. It does not support autofill, editing or adding items, or ensuring secure settings. The main feature it offers is to manually copy the credentials and paste them into a website or an application for authentication. These credentials should be previously added in another device or through the web interface so they are synchronized and appear in the VR App. This involves considerably more steps compared to the autofill features for the Meta Quest browser PM and for the LastPass browser extension (illustrations in the external Appendix Figures 4, 5, and 6). Moreover, the app suffered from technical issues, leading to credentials not being shown or updated in the vault, and requiring us to switch to another account for the review (as of writing, the app has not been updated since October 2022). It is possible to lock the PM by using an OS-based functionality, helping mitigate vulnerabilities (see Section VI-A).

While all the web-based PMs we reviewed offer similar features up to task 9, Bitwarden is the only one that does not provide feedback on credential strength, Dashlane does not fully feature (un-)locking capabilities and 1Password does not support safe settings for critical credentials. None of the web managers provide autofill functionality for other websites, which is unsurprising, as websites typically cannot access content across different browser tabs or domains. All reviewed managers lacked capability to autofill credentials into other apps across the system. This hampers their usefulness outside the browser, requiring users to manually copy-paste credentials across apps.

Exceptions include the Meta Quest browser PM and the LastPass extension, which support autofill for progressive web apps (PWAs) available via the Meta Quest store. As PWAs run in browser instances, PMs can detect and fill credential fields. Extending this functionality to non-PWAs would require access to application rendering pipelines.

In conclusion, the LastPass browser extension offered the best VR password manager experience in terms of supported features. All tasks were completed easily, and all core functions were available. The only limitation was the locking mechanism, which required manual activation in settings; while browser-closure logout failed, the time-limit option worked as intended.

Usability Issues During Setup. The setup process was cumbersome for all PMs except the Meta Quest browser PM. Web-based managers required typing the primary password and confirming device authorization on another device. In 1Password, the inability to unmask the primary password and the need for a 40-character secret key further complicated setup. Web PMs also advertised browser extensions, but these flows were misleading in VR: 1Password misidentified Meta Quest as Chrome. When clicking on the link to install the extension for Chrome, the browser announces that it is not available for Meta Quest. Similarly, LastPass web provides

TABLE I: Password manager feature comparison based on cognitive walkthrough tasks.

Task	Feature	LastPass VR app[1]	Meta browser[1]	LastPass extension[2]	LastPass web[3]	Bitwarden web[3]	Dashlane web[3]	1Password web[3]
1: First time setup	Streamlined Setup	o	✓	o	o	o	o	o
2: Registering a credential	Adding credentials		o	✓	✓	✓	✓	✓
3: Login with unstored credential	Auto-saving credentials		✓	✓				
4: Updating a credential	Editing credentials			✓	✓	✓	✓	✓
5: Login with updated credential	Auto-updating credentials		✓	✓				
6: Removing a stored credential	Removing credentials		✓	✓	✓	✓	✓	✓
7: Login with stored credential	Autofill credentials	o	✓	✓	o	o	o	o
8: Login without PM	Using PM on another device	✓		✓	✓	✓	✓	✓
9: Creating an account	Password generation on account creation			✓	o	o	o	o
	Strength feedback of generated passwords			✓	✓		✓	✓
10: Locking PM	Locking			o	✓	✓		✓
11: Unlocking PM	Unlocking			✓	✓	✓		✓
12: Ensuring safe settings	Item access protection		o	✓	✓	✓	✓	
13: Storing & autofilling non-credential data	Storing & autofilling other data			✓	o	o	o	o

✓ : feature available — o : feature partially available — *empty* : feature not available. [1]Native application — [2]Browser extension — [3]Web application

a link to download the extension, but the browser displays that no extension is available, while it can be found in the Meta Quest browser settings, which was then straightforward to install. The LastPass VR app is not linked from its web manager but is easy to find and install via the Meta Quest app store; both the app and extension require typing the primary password. The Meta Quest browser PM, enabled by default, needs no installation or primary password, making it the simplest but least secure option. It also interacts with other PMs, offering to save their primary passwords during setup. Overall, having to type complex (sometimes masked) primary passwords in VR might lead users to change them for weakest secrets [14] or store them in the built-in browser manager, impacting security negatively. Interference of PMs and usage of multiple managers have been observed in previous studies outside VR [34, 42], with its implications requiring more research attention.

Usability Issues Related to PM Locking. The ability to (un-)lock a PM is crucial for VR devices, especially when shared. Otherwise, individuals could gain access to credentials, leading to security and privacy risks. All PMs can benefit from access control options offered by Meta device's operating system (app- and headset-level 4-16 digit passcode protection). As this is dependent on the device and requires extra configuration outside the PM, we consider it does not support the feature. This protection also leads to a false sense of security, as anybody with access to the device could deactivate the protection without entering the passcode for confirmation. Four PMs fully provide vault locking options as configurable settings within the PM: "after X minutes (of inactivity)", "after closing the browser", when clicking a "lock" button. Bitwarden and 1Password provide the auto-locking feature activated by default.

Protecting access to specific items in the vault with a primary password enhances security by adding an extra layer of protection, even when the main PM is unlocked. We found configurable options to support credential protection in five PMs. For LastPass extension, LastPass web, Bitwarden, and Dashlane, dedicated options allow protection for all items or with fine-grained granularity targeting individual credentials. Meta device's passcode protection offers to lock stored passwords in the browser before autofilling those, though not being sufficiently secure, as mentioned above.

From a usability perspective, lacking options to secure individual credentials (LastPass App, Bitwarden) violates the flexibility and efficiency heuristic, leaving users with higher security needs underserved, e.g., those sharing VR devices. PMs with locking features offered unclear or hard-to-find documentation, risking weak configurations. Dashlane also failed to indicate that its lock activates only after five minutes, which can foster mistrust or a perception of the software being unreliable. Secure defaults [41] and in-context setup guidance are needed, especially for PMs relying on system-wide access controls. For instance, even with passcode protection, the Meta Quest browser PM still exposes usernames, emails, and site data in settings. Simmons et al. [42] observed similar problems in browser-based PMs where users' credentials could still be accessed after logging out from the browser.

Usability Issues with Password Generation. Automated password generation is a cornerstone feature to guarantee the security benefits of having a PM and one of the most valued functionalities by users [41]. The Meta Quest browser manager and LastPass app lack this feature, limiting users' ability to create strong passwords. Users would have to choose passwords themselves, risking weaker secrets, or use external generators, adding usability friction.

All web-based PMs and the LastPass extension include password generators, but differ in integration and customization. Bitwarden, Dashlane, and 1Password include a password generator in the credential creation pane. In Dashlane and 1Password, it is fully integrated and highly customizable, while Bitwarden's version has no customization options, though a more advanced generator is available in the settings. Users can customize passwords to be memorable, easy to use or say, adjust their length, and exclude special or ambiguous characters—features that simplify input in VR. LastPass web

and extension present a mixed experience: the web interface does not integrate the generator in the credential creation pane, but hides a parametrizable generator within nested settings menus. The browser extension offers a customizable generator which appears directly while creating a new password. Therefore, LastPass extension is the only PM that fulfills complete support for password generation. In terms of usable security, for managers that cannot interact with websites, integrated parametrizable passwords are the best option (only covered in two of the analyzed PMs: 1Password and Dashlane).

One method to raise risk awareness of weak passwords is through password strength meters, e.g., as a colored bar, accompanied by labels. Those indicators can help in selecting secure passwords [42], in particular VR users who chose to generate an easy-to-enter password. These were available during password generation in four PMs: 1Password, LastPass extension, LastPass web, and Dashlane. Those PMs report using the *zxcvbn* library [8] to measure password robustness, though the interface does not explain in detail what exactly makes a good password, additional labels could support further.

General Interface Issues. Relying solely on small icons can confuse users [42]. While examining heuristic violations, we found that Bitwarden used three unlabeled icons next to the password field in the add/edit window. Their functions—checking for breaches, generating passwords, and counting symbols—were only revealed upon clicking. In VR, every additional click requires effort and should be avoided. We also encountered hidden features that increased search time, such as nested settings, as criticized before [42]. The password generator in LastPass web is buried under Advanced Settings → Improve Security → Generate Password. Similarly, in the Meta Quest browser PM interface, the delete option is hidden behind a three-dots menu, as the only feature there. Further, assisting users with input in VR can be extremely valuable. The Meta Quest browser PM and LastPass VR app lack support for storing non-credential data (e.g., phone numbers, addresses). All web-based PMs support these fields, but only the LastPass extension effectively autofills them.

Providing users with feedback is essential, as highlighted in the first heuristic: Visibility of system status. 1Password and the Meta Quest browser PM do not offer feedback in form of small notification windows, when a new item was added to the vault, or when an item was modified and saved, ensuring users remained informed, as the others do.

On the negative side, some PMs do not offer a warning and confirmation question before deleting credentials, which could prevent users from accidentally removing passwords.

Many managers included help buttons next to icons that opened documentation pages. While this can be useful, it may be less critical in a VR context, as VR users are likely using the manager on their primary devices outside the virtual environment and may already be familiar with most of the manager's features.

B. RQ2 - Extended Analysis: UDAS in VR

We now summarize key findings from the VR-UDAS framework evaluation, with results shown in Table II.

Usability. The most crucial usability feature for VR PM users is autofill. So we measure *Efficient-to-Use* by the availability of this feature. As seen in Table I, it is only supported by Meta Quest browser PM and LastPass extension. Using the autofill feature to log into a website will take around 1–3 seconds, depending on if an extra click into the password field is required. Other PMs provide copy-paste functionality, which, while still simplifying the process by avoiding the need to switch between devices, is only *quasi-Efficient-to-Use*, a point also highlighted in our CW. Using this feature instead of manual input is estimated to take around 30 seconds. This involves copying the username from the PM interface to the clipboard, switching between apps, pasting the username into the designated field, and repeating the steps for the password.If the information (password, username or email address) is remembered, meaning there is no need to switch devices, manual typing will take around 40–60 seconds, depending on system familiarity and complexity of the data, meaning the copy-paste functionality might still be quicker. All time estimates are based on our CWs.

None of the PMs were *Physically-Effortless* due to the input methods used in the form of hand or head movements, which is not surprising for interactions in VR. Additionally, all PMs require users to remember one secret: the primary password, resulting in *quasi-Memorywise-Effortless*. The exception is the Meta Quest browser PM, which does not require a primary password, only an optional passcode to access the stored passwords, as noted before. Therefore, Meta Quest browser PM is the only manager that is *Memorywise-Effortless*, at the cost of less protection.

However, all PMs are *Easy-to-Learn* based on our expert review assessment, despite the lack of user studies as the interfaces are not complicated to explain. Further, there is *Nothing-to-Carry*, and *Infrequent-Errors* during authentication, as well as considered *Acceptable-in-Public* because they do not involve any unusual movements.

Deployability. Only the Meta Quest browser PM meets the *OS-Supported* criterion, as it comes pre-installed and activated on the device. LastPass VR app, LastPass extension, and the Meta Quest browser PM are specifically designed for VR. Due to the reported technical issues earlier in Section VI-A, we classify LastPass VR as *quasi-Mature-for-VR*, whereas the Meta Quest browser PM and the LastPass extension are deemed to be fully *Mature-for-VR*.

The Meta Quest browser PM is not *Platform-Agnostic*, as it is unavailable on other platforms, while the rest can be used on other devices and browsers. We consider LastPass VR app as *quasi-Platform-Agnostic* as other versions of LastPass exist for other platforms. Finally, all options satisfy the *Low-Power-Consumption* requirement. They involve running an app within the VR environment, which does not demand substantial power.

TABLE II: Evaluation of the password managers based on the framework by Bonneau et al. [5] and Stephenson et al. [43], including their evaluations of passwords and iris scanning as incumbent methods for comparison.

	Deployability				Usability							Accessibility					Security													
Password Manager	OS-Supported	Platform-Agnostic	Mature-for-VR	Low-Power-Consumption	Efficient-to-Use	Physically-Effortless	Memorywise-Effortless	Easy-to-Learn	Nothing-to-Carry	Infrequent-Errors	Acceptable-in-Public	Accessible-Visual	Accessible-Hearing	Accessible-Speech	Accessible-Mobility	Accessible-Cognitive	Resilient-to-Physical-Observation	Protects-User-Privacy	Multi-Factor	Resilient-to-Targeted-Impersonation	Resilient-to-Internal-Observation	Resilient-to-Leaks-from-Other-Verif.	Resilient-to-Phishing	Resilient-to-Theft	No-Trusted-Third-Party	Requiring-Explicit-Consent	Unlinkable	Resilient-to-Throttled-Guessing	Resilient-to-Unthrottled-Guessing
LastPass VR app	–	○	○	●	○	–	○	●	●	●	●	–	●	●	○	○	–	●	–	–	–	○	–	–	–	●	●	●	○
Meta Quest browser	●	–	●	●	●	–	●	●	●	●	●	–	●	●	○	○	–	●	–	–	–	–	●	–	●	●	●	–	–
LastPass extension	–	●	●	●	●	–	○	●	●	●	●	–	●	●	○	○	–	●	–	–	–	○	●	○	–	●	●	●	○
LastPass web	–	●	–	●	○	–	○	●	●	●	●	–	●	●	○	–	–	●	–	–	–	○	–	○	–	●	●	●	○
Bitwarden web	–	●	–	●	○	–	○	●	●	●	●	–	●	●	○	–	–	●	–	–	–	○	–	●	●	●	●	●	○
Dashlane web	–	●	–	●	○	–	○	●	●	●	●	–	●	●	○	–	–	●	–	–	–	○	–	○	○	●	●	–	○
1Password web	–	●	–	●	○	–	○	●	●	●	●	–	●	●	○	–	–	●	–	–	–	○	–	●	○	●	●	●	○
Password [43, 5]	●	●	●	●	–	–	–	●	●	–	–	–	●	●	–	–	–	●	–	○	–	–	–	–	●	●	●	●	–	–
Iris Scan [43, 5]	●	–	○	●	●	●	●	●	●	●	●	○	●	●	●	●	●	○	–	–	–	–	–	–	●	○	–	●	●

● = PM fulfills criterion; ○ = PM quasi-fulfills criterion; – = PM does not fulfill criterion.

Accessibility. All PMs perform similarly regarding accessibility criteria. None are *Accessible-Visual*, as users need to see the interface. All PMs quasi-fulfill *Accessible-Mobility*, as interacting with them requires physical movement of controllers, head, or hands, but no more than general interaction with the device would. This criterion is similar to the criterion *Physical-Effortless* but allows for speech-interaction, while most PMs are not *Accessible-Cognitive*, as users must remember a password. The Meta Quest browser PM allows for the optional passcode, thereby only partially fulfilling this criterion. The same applies for the LastPass VR app and LastPass extension as the user needs to enter the primary password once, then stays logged in.

Security. The primary password is evaluated as not *Resilient-to-Guessing* following the same appreciation as previous studies [5, 43] which have shown that users often struggle to choose secure passwords. For the Meta Quest browser PM, the use of the numeric passcode is optional. Even when enabled, we do not consider it to be *Resilient-to-Guessing*. The same applies to *Resilient-to-Physical-Observation*; a user entering a password or passcode on a virtual keyboard is susceptible to shoulder surfing attacks in VR. However, since the framework defines passwords as not being considered sensitive user data, all PMs fulfill the criterion for *Protects-User-Privacy*. Most managers support storing non-credential data, though this is optional.

We interpret the *Multi-Factor* criterion as applying an additional security layer (enforced by the PM) to the initial login into an PM account. This is not fulfilled for any PM. While web PMs generally offer the possibility to configure biometric or token-based authentication as additional factors, these settings are not available for use in VR, reducing security when changing to this platform.

Following the argumentation in [5], all PMs are classified as not *Resilient-to-Targeted-Impersonation*. Attackers could target the primary password to compromise the system. In the case of the Meta Quest browser manager, an attacker with physical access could retrieve credentials if no additional control options are configured. Even the passcode can be circumvented easily, as mentioned before. None of the PMs are *Resilient-to-Internal-Observation* since attackers can impersonate the user by intercepting the user's input from inside the VR device or by eavesdropping on cleartext communication between prover and verifier.

From the examined PMs, Meta Quest browser PM and LastPass extension stored the correct URL alongside the credentials on registration, ensuring that credentials will only be autofilled on legitimate websites. We assume, similar to [5], that sites follow best practices and implement TLS. Therefore, we consider PMs offering autofill to be *Resilient-to-Phishing*. PMs that do not support autofill rely on users to manually store URLs and launch the login process directly from the PM. While this approach reduces the risk of phishing if the process is followed correctly, it places significant responsibility on the user to behave consistently and accurately. We classify these PMs as not *Resilient-to-Phishing*, as their effectiveness against phishing attacks is not inherent to the system design.

We consider the Meta Quest browser PM and LastPass app as not *Resilient-to-Theft*, since locking is only an optional system-wide access control (via passcodes). Bitwarden and 1Password auto-lock the vaults by default after a few minutes of inactivity, making them *Resilient-to-Theft* when the VR device gets stolen. The other PMs do not auto-lock by default but provide options to configure locking or permit closing the

session by signing off, making them *quasi-Resilient-to-Theft*. All PMs with cloud storage employed a client-side "zero-knowledge", encryption model that does not rely on a trusted third party. Closed-source clients (such as those provided by LastPass and 1Password) make this hard to verify. Given LastPass' history of security incidents, we agree with Bonneau et al. [5] that caution is warranted in trusting its client.

All PMs satisfy the criterion of *Requiring-Explicit-Consent*, as the initiation of the authentication process mandates that users input a secret. This criterion is also considered met by the Meta Quest browser PM, which employs autofill for credentials, but still requires user action (a press to submit) for completion. Similar to Bonneau et al. [5], we assume that each site applies salt to passwords, ensuring that even weak passwords remain *Unlinkable*.

Five PMs throttle guessing the primary password by temporarily limiting password entries after repeated failed attempts. All LastPass PMs lock access for 5 minutes after 8 consecutive failed attempts. Bitwarden and 1Password, while not imposing a strict limit on attempts, implement mechanisms to slow down the submission process. Dashlane allows entering the primary secret an unlimited number of times. We categorize all PMs, except for Meta Quest browser PM and Dashlane as *Resilient-to-Throttled-Guessing*. Providing resilience to unthrottled guessing depends on the strength of the primary password. Except for the Meta Quest browser PM (which does not support a primary password) and 1Password (which only requires a minimum length), all tested PMs set requirements for password makeup and/or length, and make a reasonable effort at recognizing weak passwords. However, it remains an imperfect solution and only randomly generated passwords can provide proper resilience against unthrottled guessing. Therefore, every PM is *quasi-Resilient-to-Unthrottled-Guessing*, except for the Meta Quest browser PM. Only LastPass suggests, but does not require, a randomly generated primary password.

VII. Discussion and Recommendations

A. The (Un)suitability of Passwords

While it is clear that passwords are not convenient for VR input and can induce bad security practices, they remain the most common mechanism in place. In our study, participants reported choosing simpler passwords for convenience when entering secrets in VR systems using controllers, citing difficulties such as longer input times and the complexity of selecting keys on virtual keyboards. Choosing weak secrets can pose security risks, highlighting the urgent necessity for more user-friendly authentication solutions in VR. These findings align with the survey results in [43], and we confirm them in a more diverse population.

Further comparisons show that our participants rated passwords as more usable than in a previous study [43], partly because some users relied on autofill. This suggests they considered the entire VR authentication flow involving multiple devices and software. PMs with autofill therefore enhance usability, which aligns with over 80% of our sample being PM users. Familiarity with password-based authentication may also explain the high ratings [45].

Our and prior findings [14] show that masked passwords can both give users a sense of security and make entering long, complex passwords cumbersome. In VR, since physical external observers cannot see the virtual environment, masking is generally unnecessary, except when recording or streaming. Systems could detect to adjust this setting automatically, or offer an option to toggle masking passwords while unmasking is the default status.

B. The (Un)suitability of Password Managers

Similar to our observations, participants in previous studies expressed frustration over the lack of PMs in VR, noting the challenges of adapting such managers to new platforms [43].

We observed that key features such as autofill, password generation, editing and adding credentials, were missing for the deployed VR PMs. No PM could autofill across the system, such as within applications. Our results show that PMs are currently unsuitable for most VR authentication use cases, such as device setup, app setup or access, purchases, and device activation, due to limited cross-app interoperability. Platform providers should provide OS integration for PMs, allowing both first and third party PMs to provide autofill functionality for password fields in any app. Such solutions are already present in mobile operating systems such as iOS and Android . Additionally, PMs currently lack VR-awareness and could detect when users are in VR to offer tailored options, for instance, passwordless alternatives or adjust their password generation tools to create secure but easier-to-enter/memorable passwords when manual input is unavoidable, while still offering strong passwords. Additionally, our heuristic evaluation also showed that navigating through the PMs VR interfaces can create physical burdens because of nested menus, unlabeled icons, or lack of feedback.

PMs appear as a plausible solution to support users with passwords in VR, during the transition to more suitable solutions, or in combination with them. Comparing our evaluation of PMs with the evaluation of passwords in VR [43], we find that password managers in VR, despite current limitations, still fulfill important usability criteria, whereas traditional passwords fall short in these areas. The immersive nature of VR differs from traditional 2D interfaces, and this shift requires designers and developers to address challenges, such as minimizing users' physical effort with autofill capability to reduce the need for users to switch between the real and virtual worlds for looking up passwords on a secondary device or manually inputs. This is not only relevant from the usability perspective, but also to enhance security. If properly supported, users can have strong automatically generated passwords in VR and avoid typing them, the latter being susceptible to attacks like shoulder-surfing attacks.

C. Improving Authentication in VR

Users, as in previous research [43], show a preference for biometric authentication in VR. They also acknowledge the

(currently unexploited) potential of VR to provide tailored solutions. We believe future work could focus on synergistic approaches, like leveraging VR-specific biometrics to complement PMs. This could enable a seamless experience where the user wears the device, authenticates biometrically (e.g., iris scan [16], eye-tracking [24], or EEG [2]), and unlocks the PM. This will solve usability and security limitations of having to type a primary password in VR and current issues with (un-)locking the PM safely. Apple is incorporating iris scanning for authentication in the Apple Vision Pro (Optic ID), a development that could significantly benefit other VR devices too. Biometric approaches also entail security and privacy risks. Biometric traits cannot easily be changed after compromise, and VR sensors may collect sensitive behavioural or physiological data beyond what is needed for authentication [20, 38]. Their reliability may further vary with headset fit, fatigue, or motion, causing false rejections or acceptances. Therefore, these approaches require further exploration. Further, risk-based authentication adapts requirements according to the risk of a user's login, evaluating contextual factors [3] to balance security and usability. Exploring it in VR could reveal context-aware methods that streamline authentication (including PM logins) while maintaining security and reducing effort.

Another passwordless solution are passkeys, cryptographic key pairs based on the FIDO standard [13]. Already supported by many PMs on desktop and mobile as a replacement for (primary) passwords or MFA, they are not yet available in VR, making their integration a recommended next step.

Our survey revealed that VR users often allow others to authenticate on shared devices, posing security risks as the owner's personal information could be exposed. We recommend implementing solutions, such as easy multiprofile management, or a guest mode with quick profile switching, without the need to create accounts for short sessions. Further, proper locking mechanisms for PMs are essential when VR devices are shared. Most PMs we evaluated lacked this feature, i.e., part of stored credentials in the Meta Quest PM were exposed even after entering an additional passcode, which could be easily bypassed for autofilling passwords, posing a significant security risk.

D. Limitations and Future Research

Our study relies on self-reported survey data, though attention checks were implemented to filter poor responses. When listing possible VR authentication mechanisms, we observed misconceptions, likely due to the complexity of authentication across devices and accounts. Some non-expert participants reported using unsupported methods, such as eye-tracking, facial, fingerprint, or movement-based authentication; these were excluded from usability and security analyses. Online surveys may therefore miss nuances of user experience that could be captured through observational or task-based studies.

Regarding PMs in VR, further user studies are needed to examine usability challenges, accessibility concerns, and how the continued use of less secure browser-based PMs limits security benefits. The tasks and usability issues identified in our study can inform such work, using established benchmarks and mental-load measures. Our role-play testing is also limited by differences between expert and typical user behavior [31], highlighting the need for studies involving end users.

The expert review was conducted in November 2024 and reflects PMs available on Meta devices at that time. As VR platforms evolve rapidly, subsequent developments, such as Meta's integration of Dashlane, Bitwarden, Proton Pass, and 1Password in November 2025, and the Proton Pass VR app in January 2026, were not included. Our evaluation also focused solely on Meta devices, which may differ from other VR platforms in interaction and authentication workflows.

Finally, the extended VR-UDAS analysis is based on heuristics and assumptions. As noted by Bonneau et al. [5], context-based weighting could improve accuracy. The ratings should not replace independent analyses or consideration of unassessed factors, such as attack-specific vulnerabilities.

VIII. Conclusion

The focus of current research lies predominantly on proposing solutions to improve the VR authentication experience, without fully considering real-world user needs. Understanding user experiences, and integrating their suggested improvements, is vital before implementing novel VR-specific authentication methods. To address this, we conducted a user study to gain a comprehensive understanding of users' challenges and needs in VR authentication. Our contribution fills a gap in the literature by explicitly examining user experiences with authentication, account creation, and the adoption of password managers in VR. Following this, we evaluated seven password managers to assess how well they support password management within VR. Insights from our study can guide researchers and practitioners in advancing authentication practices in VR, thereby ultimately enhancing user security and safety in virtual environments.

Use of Large Language Models. OpenAI's GPT-5 model was used to assist with editing and improving the writing of this paper. All findings are solely our own, informed by our expertise, the study data, and the cited literature.

Acknowledgments

This work was supported by funding from the project "Engineering Secure Systems" of the Helmholtz Association (HGF) [subtopic 46.23.01 Methods for Engineering Secure Systems] and by KASTEL Security Research Labs.

Appendix

Surveys, study details (demographics, background, VR usage, PM screenshots and versions), further analysis material (complete codebook, kappa values), expert review material (cognitive walkthrough tasks, heuristics, evaluation criteria), and the anonymized dataset are available at www.osf.io/pa49w/?view_only=6cbaeb63b081429f9df62767eb3f9755.

References

[1] Sabrina Amft, Sandra Höltervennhoff, Nicolas Huaman, Yasemin Acar, and Sascha Fahl. "would you give the same priority to the bank and a game? i do not!" exploring credential management strategies and obstacles during password manager setup. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*, pages 171–190, 2023.

[2] Patricia Arias-Cabarcos, Matin Fallahi, Thilo Habrich, Karen Schulze, Christian Becker, and Thorsten Strufe. Performance and usability evaluation of brainwave authentication techniques with consumer devices. *ACM Transactions on Privacy and Security*, 26(3):1–36, 2023.

[3] Patricia Arias-Cabarcos, Christian Krupitzer, and Christian Becker. A survey on adaptive authentication. *ACM Computing Surveys (CSUR)*, 52(4):1–30, 2019.

[4] Patricia Arias-Cabarcos, Andrés Marín, Diego Palacios, Florina Almenárez, and Daniel Díaz-Sánchez. Comparing password management software: toward usable and secure enterprise authentication. *IT Professional*, 18(5):34–40, 2016.

[5] Joseph Bonneau, Cormac Herley, Paul C Van Oorschot, and Frank Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *2012 IEEE symposium on security and privacy*, pages 553–567. IEEE, 2012.

[6] Virginia Braun and Victoria Clarke. *Successful Qualitative Research: A Practical Guide for Beginners*. SAGE Publications Ltd, London, 2013.

[7] Jacob Cohen. A coefficient of agreement for nominal scales. *Educational and psychological measurement*, 20(1):37–46, 1960.

[8] Dropbox Inc. Daniel Lowe Wheeler. zxcvbn tests. [Online] https://lowe.github.io/tryzxcvbn/, 2016. Visited on 25/05/2026.

[9] Reyhan Düzgün, Philip Klostermeyer, Lena Swienty, Sascha Fahl, and Karola Marky. Towards secure and usable xr authentication schemes for head-mounted displays: A co-creation study with experts. In *Proceedings of the 2025 31st ACM Symposium on Virtual Reality Software and Technology*, VRST '25, New York, NY, USA, 2025. Association for Computing Machinery.

[10] Erik Emanuelli. Top 10 password managers for 2025. [Online] www.tribulant.com/blog/security/top-10-password-managers-for-2025, 2025. Visited on 25/05/2026.

[11] Sascha Fahl, Marian Harbach, Marten Oltrogge, Thomas Muders, and Matthew Smith. Hey, you, get off of my clipboard: On how usability trumps security in android password managers. In *Financial Cryptography and Data Security: 17th International Conference, FC 2013, Okinawa, Japan, April 1-5, 2013, Revised Selected Papers 17*, pages 144–161. Springer, 2013.

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

[13] Sanam Ghorbani Lyastani, Michael Schilling, Michaela Neumayr, Michael Backes, and Sven Bugiel. Is fido2 the kingslayer of user authentication? a comparative usability study of fido2 passwordless authentication. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 268–285, 2020.

[14] Yuqi Hu, Suood Alroomi, Sena Sahin, and Frank Li. Unmasking the security and usability of password masking. In *Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security (CCS '24)*, page to appear. ACM, 2024. Distinguished Paper Award.

[15] Adryana Hutchinson, Collins W. Munyendo, Adam J Aviv, and Peter Mayer. An analysis of password managers' password checkup tools. In *Extended Abstracts of the 2024 CHI Conference on Human Factors in Computing Systems*, CHI EA '24, New York, NY, USA, 2024. Association for Computing Machinery.

[16] Brendan John, Sanjeev Koppal, and Eakta Jain. Eyeveil: degrading iris authentication in eye tracking headsets. In *Proceedings of the 11th ACM Symposium on Eye Tracking Research & Applications*, pages 1–5, 2019.

[17] John M Jones, Reyhan Duezguen, Peter Mayer, Melanie Volkamer, and Sanchari Das. A literature review on virtual reality authentication. In *Human Aspects of Information Security and Assurance: 15th IFIP WG 11.12 International Symposium, HAISA 2021, Proceedings 15*, pages 189–198. Springer International Publishing, 2021.

[18] Alita Joyce. 10 usability heuristics applied to virtual reality. [Online] www.nngroup.com/articles/usability-heuristics-virtual-reality, 2021. Visited on 25/05/2026.

[19] Emiram Kablo, Katharina Kader, and Patricia Arias-Cabarcos. "i'm actually going to go and change these passwords": Analyzing the usability of credential audit interfaces in password managers. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2024.

[20] Emiram Kablo, Melina Kleber, and Patricia Arias-Cabarcos. Privaci in vr: Exploring perceptions and acceptability of data sharing in virtual reality through contextual integrity. In *34th USENIX Security Symposium (USENIX Security 25)*, pages 1531–1548, 2025.

[21] Douglas Kunda and Mumbi Chishimba. A survey of android mobile phone authentication schemes. *Mobile Networks and Applications*, 26(6):2558–2566, 2021.

[22] Tobias Länge, Philipp Matheis, Reyhan Düzgün, Melanie Volkamer, and Peter Mayer. Vision: Towards fully shoulder-surfing resistant and usable authentication for virtual reality. In *Proceedings of the 2024 Symposium on Usable Security and Privacy (USEC)*, 2024.

[23] Jonathan Lazar, Jinjuan Heidi Feng, and Harry Hochheiser. *Research methods in human-computer interaction*. Morgan Kaufmann, 2017.

[24] Shiqing Luo, Anh Nguyen, Chen Song, Feng Lin,

Wenyao Xu, and Zhisheng Yan. Oculock: Exploring human visual system for authentication in virtual reality head-mounted display. In *2020 Network and Distributed System Security Symposium (NDSS)*, 2020.

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

[26] Peter Mayer, Collins W Munyendo, Michelle L Mazurek, and Adam J Aviv. Why users (don't) use password managers at a large educational institution. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 1849–1866, 2022.

[27] Mary L McHugh. Interrater reliability: the kappa statistic. *Biochemia medica*, 22(3):276–282, 2012.

[28] Matthew B Miles and A Michael Huberman. *Qualitative data analysis: An expanded sourcebook*. Sage, 1994.

[29] Collins W. Munyendo, Peter Mayer, and Adam J. Aviv. "i just stopped using one and started using the other": Motivations, techniques, and challenges when switching password managers. CCS '23, page 3123–3137, New York, NY, USA, 2023. Association for Computing Machinery.

[30] Rabia Murtza, Stephen Monroe, and Robert J Youmans. Heuristic evaluation for virtual reality systems. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, volume 61, pages 2067–2071. SAGE Publications Sage CA: Los Angeles, CA, 2017.

[31] Jakob Nielsen and Rolf Molich. Heuristic evaluation of user interfaces. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 249–256, 1990.

[32] Naheem Noah, Peter Mayer, and Sanchari Das. A proposal to study shoulder-surfing resistant authentication for augmented and virtual reality: Replication study in the us. In *Companion Publication of the 2023 Conference on Computer Supported Cooperative Work and Social Computing*, pages 317–322, 2023.

[33] Sean Oesch, Anuj Gautam, and Scott Ruoti. The emperor's new autofill framework:a security analysis of autofill on ios and android. In *Proceedings of the 37th Annual Computer Security Applications Conference*, ACSAC '21, page 996–1010, New York, NY, USA, 2021. Association for Computing Machinery.

[34] Sean Oesch and Scott Ruoti. That was then, this is now: A security evaluation of password generation, storage, and autofill in Browser-Based password managers. In *29th USENIX Security Symposium (USENIX Security 20)*, pages 2165–2182. USENIX Association, 2020.

[35] Sarah Pearman, Shikun Aerin Zhang, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Why people (don't) use password managers effectively. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, pages 319–338, 2019.

[36] Ken Pfeuffer, Matthias J Geiger, Sarah Prange, Lukas Mecke, Daniel Buschek, and Florian 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*, pages 1–12, 2019.

[37] Hirak Ray, Flynn Wolf, Ravi Kuber, and Adam J. Aviv. Why older adults (don't) use password managers. In Michael D. Bailey and Rachel Greenstadt, editors, *30th USENIX Security Symposium, USENIX Security 2021, August 11-13, 2021*, pages 73–90. USENIX Association, 2021.

[38] Alia Saad, Verena Winterhalter, Marvin Strauss, and Stefan Schneegass. "i feel more worried about my privacy" public perceptions of biometric traces in everyday interactions. In *Proceedings of the Extended Abstracts of the 2026 CHI Conference on Human Factors in Computing Systems*, CHI EA '26, New York, NY, USA, 2026. Association for Computing Machinery.

[39] John Sadik and Scott Ruoti. A large-scale survey of password entry practices on non-desktop devices. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 9(3):1–30, 2025.

[40] Kim Salazar. Evaluate interface learnability with cognitive walkthroughs. [Online] www.nngroup.com/articles/cognitive-walkthroughs, 2022. Visited on 25/05/2026.

[41] Sunyoung Seiler-Hwang, Patricia Arias-Cabarcos, Andrés Marín, Florina Almenares, Daniel Díaz-Sánchez, and Christian Becker. "i don't see why i would ever want to use it" analyzing the usability of popular smartphone password managers. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pages 1937–1953, 2019.

[42] James Simmons, Oumar Diallo, Sean Oesch, and Scott Ruoti. Systematization of password manager use cases and design paradigms. In *Proceedings of the 37th Annual Computer Security Applications Conference*, pages 528–540, 2021.

[43] Sophie Stephenson, Bijeeta Pal, Stephen Fan, Earlence Fernandes, Yuhang Zhao, and Rahul Chatterjee. Sok: Authentication in augmented and virtual reality. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 267–284. IEEE, 2022.

[44] Zhen Yu, Hai-Ning Liang, Charles Fleming, and Ka Lok Man. An exploration of usable authentication mechanisms for virtual reality systems. In *2016 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*, pages 458–460. IEEE, 2016.

[45] Verena Zimmermann and Nina Gerber. The password is dead, long live the password–a laboratory study on user perceptions of authentication schemes. *International Journal of Human-Computer Studies*, 133:26–44, 2020.