Investigating Security Indicators for Hyperlinking Within the Metaverse

Maximiliane Windl, *LMU Munich and Munich Center for Machine Learning (MCML);*
Anna Scheidle, *LMU Munich;* Ceenu George, *University of Augsburg and TU Berlin;*
Sven Mayer, *LMU Munich and Munich Center for Machine Learning (MCML)*

https://www.usenix.org/conference/soups2023/presentation/windl

This paper is included in the Proceedings of the Nineteenth Symposium on Usable Privacy and Security.

August 7–8, 2023 • Anaheim, CA, USA

978-1-939133-36-6

Open access to the Proceedings of the Nineteenth Symposium on Usable Privacy and Security is sponsored by USENIX.

Investigating Security Indicators for Hyperlinking Within the Metaverse

Maximiliane Windl[1,2], Anna Scheidle[1], Ceenu George[3,4], Sven Mayer[1,2]
[1] *LMU Munich, Germany*
[2] *Munich Center for Machine Learning (MCML), Germany*
[3] *University of Augsburg, Germany*
[4] *TU Berlin, Germany*

Abstract

Security indicators, such as the padlock icon indicating SSL encryption in browsers, are established mechanisms to convey secure connections. Currently, such indicators mainly exist for browsers and mobile environments. With the rise of the metaverse, we investigate how to mark secure transitions between applications in virtual reality to so-called sub-metaverses. For this, we first conducted in-depth interviews with domain experts (N=8) to understand the general design dimensions for security indicators in virtual reality (VR). Using these insights and considering additional design constraints, we implemented the five most promising indicators and evaluated them in a user study (N=25). While the visual blinking indicator placed in the periphery performed best regarding accuracy and task completion time, participants subjectively preferred the static visual indicator above the portal. Moreover, the latter received high scores regarding understandability while still being rated low regarding intrusiveness and disturbance. Our findings contribute to a more secure and enjoyable metaverse experience.

1 Introduction

At the latest, when Facebook renamed itself to Meta and put most of its research efforts into creating an immersive virtual world, the notion of the "metaverse" attracted the public's attention. While employing different approaches, other companies also focus on creating such "shared, open, and perpetual virtual worlds" [32]. For example, Microsoft is creating a collaborative, mixed-reality experience mainly for meetings[1]; Niantic is developing outdoor-capable AR glasses aiming to enrich the real world instead of cutting people out of it[2], and EPIC games and LEGO are developing a secure metaverse experience for children[3]. While many develop on independent applications, the idea of the metaverse links all single applications to one big network, much like the world-wide-web with hyperlinks to transition between them. Therefore, users will transition between different metaverses via hyperlinking frequently and consequently take their identity to unknown environments. Thus, it is only a matter of time before known security risks from browser and mobile environments become relevant threats [23]. As such, the same need as in the world-wide-web will occur – marking and ensuring safe transitions to a new service before revealing one's identity to the new provider. Moreover, users will frequently need to decide whether to consciously enter applications with unknown origins [39]. Hence, we require effective security indicators within the metaverse.

Prior research has shown that security indicators can effectively signal secure transitions to users. An established example represents the padlock icon displayed in browsers next to the URL to signal SSL encryption, cf. [48]. So far, research has primarily focused on security indicators in browsers [11, 24, 33] and mobile environments [35, 52]. Here, researchers investigated the effectiveness of using, for example, icons [25, 45], color coding [45], blinking animations [30], or security images that should create a secret between the user and the application [30]. Going from 2D to 3D space offers many novel ways to represent security indicators, such as size and location. Therefore, we argue that the next step will be to extrapolate from 2D indicators and develop indicators suitable for the metaverse.

This paper investigates security indicators for hyperlinking within the metaverse. For this, we first employed a participatory design approach by conducting in-depth interviews with domain experts (N=8) to understand the general design dimensions for security indicators in VR. Based on the expert interviews' findings, we developed and evaluated the five most promising security indicators (one haptic, one audio, and

[1] https://www.microsoft.com/en-us/mesh
[2] https://nianticlabs.com/news/real-world-metaverse
[3] https://www.epicgames.com/site/en-US/news/the-lego-group-and-epic-games-team-up-to-build-a-place-for-kids-to-play-in-the-metaverse

USENIX Symposium on Usable Privacy and Security (SOUPS) 2023.
August 6–8, 2023, Anaheim, CA, United States.

three visual indicators) for their usability and effectiveness in a user study (N=25). We found that while the five indicators performed equally well regarding pragmatic and hedonic quality, there were considerable differences regarding understandability and disturbance. Moreover, the visual blinking indicator significantly improved the accuracy and speed of understanding secure transitions in VR.

Our contribution is twofold. First, this paper is the first to construct a design space for security indicators in VR. This design space will help researchers and developers create security indicators for VR. Second, our study showed that while the visual blinking indicator placed in the periphery performed best regarding the objective measures accuracy and task completion time, participants subjectively preferred the static visual indicator placed above the portal. Moreover, it received high scores for understandability while still being rated low regarding intrusiveness and disturbance. Our findings have implications for designing metaverse environments by ensuring a more secure and enjoyable VR experience.

2 Related Work

We first present definitions of the term metaverse and research trends. Then, we discuss prior research on security indicators on the web, mobile environments, and mixed reality. Finally, we derive our research questions.

2.1 Metaverse

The term metaverse appeared for the first time in a novel by Stephenson [46], where it is described as a parallel universe where people interact through avatars. While the metaverse attracted attention in research, there exists no common definition. While Park and Kim [37] state that the metaverse does not necessarily use VR and AR technologies, Green and Works [19] found that the metaverse is commonly described as a virtual world that uses VR technology by researching the term's definition across social media, the news, and in the ACM. Moreover, Lee et al. [32] define the metaverse as "a virtual environment blending physical and digital," and Ning et al. [36] add the "interaction of humans and a computer-mediated virtual platform" as other key aspects. *Consequently, we define the metaverse as a connected social environment that uses VR technology in this paper's context.*

There is also research on how a widely adopted metaverse might influence the world. Duan et al. [10] outline how the metaverse can be used for social good. They, for example, describe how a metaverse can improve accessibility by hosting social events so that no travel is required, improve diversity as a metaverse would make it easier to cater to individual needs, and how the metaverse can help humanity as historical landmarks can be rebuilt in VR. However, there is also research on the possible threats of the metaverse. Rosenberg [40], for example, outlines three fundamental risks: 1) The current ubiquitous monitoring of users will get even worse in the metaverse, as a multitude of new features can be tracked, such as where users go, looks at, what they grab, or their vital signs; 2) Manipulation of users might also worsen as it will become hard to differ advertisement from real content, as advertisements might be hidden as simulated people or products; and 3) monetization of users in the metaverse will become an issue as people pay with their data. To counteract these possible negative effects, Rosenberg [40] suggest non-regulatory and regulatory approaches, such as restricting the monitoring and emotional analysis of metaverse users or restricting virtual product placements. Especially the first point, the increased monitoring of users, might lead to privacy issues, as massive amounts of personal data are collected and stored. Indeed, a large stack of research solely focuses on the privacy and security implications of the metaverse [5, 8, 12, 50]. In terms of privacy, key concerns include but are not limited to the extensive amounts of personal data collected to build a digital copy of the real world [5, 12, 50], social engineering hacking [5, 8, 50], online harassment [12], and more specifically spying and stalking [8]. In terms of security, Di Pietro and Cresci [8] predict issues regarding authentication as it might become hard to distinguish humans from machines and issues regarding polarization and radicalization as a uniform, massive metaverse replaces the present plurality of the web. In addition, Wang et al. [50] raise concerns about data tempering attacks that might happen during data communication among various sub-metaverses and privacy leakage that might happen as large amounts of data are transferred. *As privacy and security are significant concerns about the metaverse, especially when transmitting large amounts of private data and transitioning between so-called sub-metaverses, we see a need for researching adequate mitigation measures.*

2.2 Security Indicators

Security indicators alert the user of potential risks or validate the identity of a website or application [30, 47]. Prior research has investigated the effectiveness of security indicators on the web. The padlock icon next to the URL is one of the browser's most widely adopted security indicators, demonstrating an authenticated connection [47]. Whalen and Inkpen [51] found while the padlock icon was mostly recognized, users did not use its interaction functions, and von Zezschwitz et al. [49] found that many users still misunderstand the icon. While it only indicates connection security, many people misattribute general privacy, security, and trustworthiness to it [49]. Lee et al. [30] tested the effectiveness of security images during login. A security image is supposed to prevent phishing attacks by displaying a personalized image and caption. Yet, researchers found that most users still log in, even if the image is missing [30, 43]. However, users' attention to security images can be improved by adding a visual effect, such as a blinking animation [30] and making them interactive, such as

requiring the user to find and click the image [21].

Prior research investigated security indicators for mobile devices. For example, Zhang et al. [53] tested the effectiveness of warning notices that alerted users of untrusted certificates. They found that the warnings increased users' perceived threat to their personal information. Another line of research focuses on informing users about possible privacy and security threats before installing an application by providing information in the app store. Choe et al. [6] compared positively and negatively framed visuals and found that they influenced users' app installation decisions. Rajivan and Camp [38] explored the usage of icons in the app store to provide information about applications that access private data. Icons positively influenced the app ratings and increased users' subjective perceptions of the app's privacy and security [38]. However, the most prominent of these indicators is the "privacy nutrition label" [26, 27]. Although such labels are currently deployed in both major app stores[4, 5], they have experienced criticism as they are not prominently placed, use confusing terminology, and are inconsistent with the apps' privacy policies [7].

Previous research on mixed reality security indicators almost solely focuses on indicators for secure authentication by developing techniques to shield users' input from external observers [1, 14, 15, 16, 17]. For this, researchers used randomly color-coded visual cues [1], 3D objects [16, 17], and spatial and virtual targets [14]. In the augmented reality (AR) context, prior research anticipates that future AR systems will run multiple applications simultaneously to share input and output devices, exposing data and APIs to each other [39]. This entails risks like clickjacking attacks that trick users into clicking on malicious interface elements [39]. Moreover, users need to know the origin of content to judge if it is trustworthy, especially when sensitive data is shared across applications [39]. Recognizing these dangers, Hosfelt et al. [22] developed different concepts for security indicators for transitions in the immersive web: A logo, a sigil, and a customizable agent. At the time of this paper, it is the only prior work focusing specifically on security indicators for VR transitions. While most participants preferred the agent, the logo performed best regarding the error rate mainly because participants forgot what their sigil or agent looked like. *While signaling secure origins and transitions have been recognized as important in prior research, security indicators for VR have been scarcely researched so far. Hence, we require more research on how to implement indicators that verify the origin and security status of applications and contents in VR.*

2.3 Summary and Research Questions

Prior research raised significant privacy and security concerns regarding the metaverse [5, 8, 12, 50]. Especially as large amounts of data will be transmitted between sub-metaverses [50], users need indicators to verify the origins of content [39]. Yet, before implementing indicators, we first need to know what they can look like. Therefore, we pose our first research question (**RQ1**): *What are the general design dimensions for security indicators in the metaverse?* Researchers found that while security indicators can be effective measures to indicate a secure connection or origin, several have shortcomings preventing them from fulfilling their goals [7, 30, 43]. Hence, we ask our second research question (**RQ2**): *Which security indicators are the most effective?* Yet, for users to willingly use indicators, they must be usable. Thus, our third research question (**RQ3**) is: *Which security indicators are the most usable?* Security indicators must be noticeable and understandable to fulfill their goal while not being intrusive or disturbing. Hence, our fourth research question (**RQ4**) is: *Which security indicators have the best notification qualities?* Lastly, weighing all these qualities against each other, we investigate the best tradeoff with our last research question (**RQ5**): *Which security indicators would participants like to use in their daily VR experience?*

3 A Design Space for VR Security Indicators

As research on security indicators in the metaverse is scarce, we conducted eight semi-structured expert interviews from industry and academia to understand their general design dimensions (**RQ1**). Interviews allowed us to follow up on the experts' ideas and start an in-depth discussion on them.

3.1 Procedure

Before we started the interview, we provided experts with an informed consent form and practical information, such as the session duration and confidentiality. We then started with introductory questions about our experts' general familiarity and experience with security indicators, followed by their familiarity with VR. After that, we introduced the security issues that might arise in the metaverse when transitioning between applications and the interviews' goal of understanding the general design dimensions of security indicators for usage in VR. To spark our experts' creativity, we presented approaches that prior work had found to be effective for security indicators and to attract users' attention in VR. This included different placements, i.e., in the periphery [20, 33] or the user's focus area [20], the different forms of representation and customization, such as 2D or 3D objects or customized avatars, and the different ways to draw user attention, such as using a pulsating [31] or blinking [20] effect. We then asked our experts to envision security indicators they consider suitable to signal secure transitions in VR, whereby we advised them to describe the different parameters, form factors, and functionalities in detail.

[4] https://www.apple.com/privacy/labels/
[5] https://blog.google/products/google-play/data-safety/

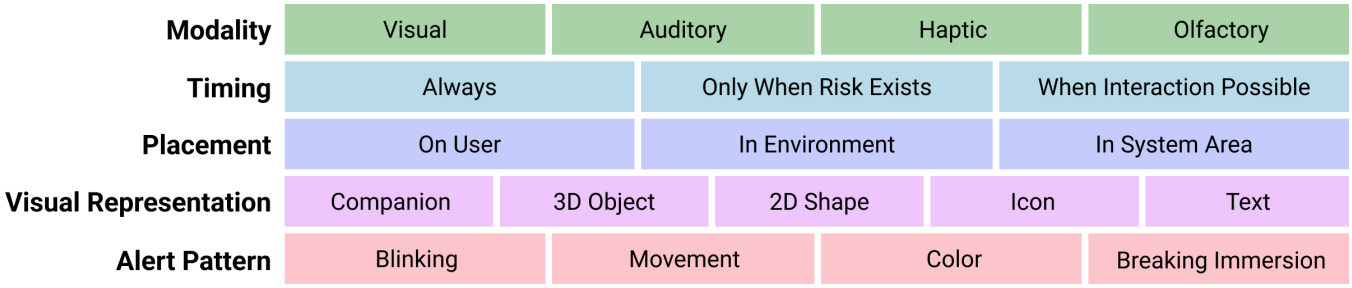


Figure 1: A design space for security indicators in VR based on expert interviews.

3.2 Participants

Eight experts took part in the interviews. We recruited our experts through our personal network, followed by snowball sampling. To qualify as an expert, the participant had to have at least 3 years of experience with VR, usable security, and/or privacy, see Table 1. All participants had either an IT or usability background. In addition, all experts stated that they have experience with security indicators in their daily life or work, and three experts already had experience with security indicators in VR. We did not compensate the experts.

3.3 Results

We transcribed 257.25 minutes ($M = 32.16$, $SD = 6.64$) of audio material, which we recorded during the eight interviews and analyzed the data using thematic analysis [4] and Atlas.ti. More precisely, we followed the *theoretical approach* as outlined in Braun and Clarke [4], where one "code[s] for a specific research question." For that, two researchers first coded all transcribed interviews, after which a third researcher joined to create the code groups and themes in multiple hour-long sessions. This process resulted in two themes: DESIGN SPACE and CONTEXT SPACE.

3.3.1 Design Space

We extracted five themes that describe the dimensions of security indicators in VR, which we used to create a design space, see Figure 1. These five themes are MODALITY, TIMING, PLACEMENT, VISUAL REPRESENTATION, and ALERT PATTERN.

Modality. Our experts discussed four general modalities that can be used to deliver the security indicator. All experts suggested at least one visual security indicator, especially because of its simplicity: *"I would probably go for something simple. For this, a visual cue is actually quite good."* Next to this, our experts also suggested *Auditory* (E1, E3, E6, E8), *Haptic* (E1, E3, E4, E6, E8), and *Olfactory* (E3) indicators.

Table 1: Demographics of our interviewed experts: Their experience, and whether they work in industry or academia.

ID	Experience	Sector
1	Usable Security, Collaborative VR, Presence	Academia
2	Software Engineering, Mobile, XR	Industry
3	Usable Security, Authentication, XR	Academia
4	Software Engineering, XR	Industry
5	Mobile Security and Privacy	Industry
6	Software Engineering, XR	Industry
7	Usable Security and Privacy, Gaze-based Systems	Academia
8	Usable Security and Eye Tracking	Academia

Timing. Our experts named three different timings suitable to display security indicators. One suggestion was to show the indicator *Always*. While E7 opposed this as they feared it might be *"distracting"* and *"annoying,"* E4 suggested implementing such an indicator subtle but still obtrusive, comparing it to the green light indicating an active camera in laptops (E4). Another suggestion was to display the indicator *Only When Risk Exists* (E3, E4), i.e., when it becomes *"relevant (E4)."* The suggestion made by most experts was to display the indicator *When Interaction [is] Possible* (E2, E3, E6, E8), so only displaying the security indicator when a user is *"close enough to interact (E6)"* with a portal or when users have the *"option to change to another environment (E3)."*

Placement. Our experts discussed three general placements for the security indicators. The option most frequently mentioned was placing the indicator *On [the] User* (E1, E2, E4, E5, E6, E8), for example, directly in the user's field of view: *"Perhaps directly centered in the middle (E5),"* or in the periphery around the user (E6). Apart from that, our experts also suggested placing the indicator *In [the] Environment* near the transition or portal (E2, E5, E6, E7, E8) or in the *System Area* (E4, E5, E7), such as it is done in browsers for the padlock.

Visual Representation. Our experts also discussed five different visual representations. They extensively discussed a more playful variant in the form of a *Companion* that actively

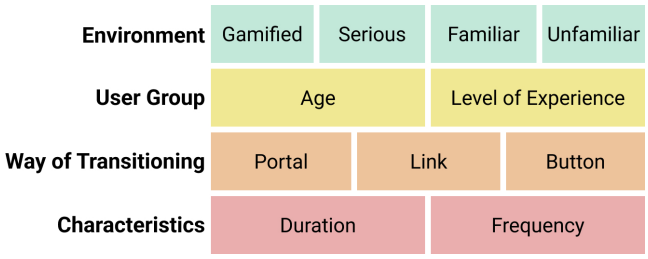


Figure 2: A context space influencing the suitability of different characteristics of security indicators in VR based on expert interviews.

warns the user whenever security issues occur. Such a *Companion* could take different forms, such as an animal (E2), avatar (E5), or even a small robot (E7). However, half of our experts considered *Companions* unsuitable for the security context since they found them either too playful or complex or only understandable with the help of onboarding (E1, E2, E3, E5). While two experts suggested using *3D Objects* (E2, E6), most experts favored simple *2D Shapes* (E3, E4, E5, E6, E8), for example, in the form of a red dot (E4, E3, E7). Other suggestions included porting the padlock *Icon* to VR (E3) or using *Text* (E6). Yet, E6 also discussed the challenges of using *Text* as a security indicator: *"People always click it away and reading in VR is no fun anyway (E6)."*

Alert Pattern. The experts discussed four different alert patterns to draw users' attention to the security indicator. The experts most often suggested to *Break Immersion*, by, for example, either playing an unpleasant sound (E6) or more subtle sounds like a beeping noise (E3) or a whisper (E8). Other suggestions to break immersion included displaying the indicator directly in the user's field of view (E2, E3, E4), dispensing an unpleasant smell (E3), using thermal feedback (E3), or letting the controller vibrate using an obtrusive pattern, such as an elevated heartbeat (E6). Here, a secure transition would be indicated using a calm pattern, and an insecure transition by an elevated heart rate pattern (E6): *"Something exciting that feels somewhat stressful."* Next to this, experts suggested alerting users by changing the *Color* (E3, E4, E5, E6, E8) of the security indicator, using a *Blinking* effect (E2, E4, E5, E6), or using *Movement*, for example, increasing the rotation speed (E2) or changing the size of the indicator (E3).

3.3.2 Context Space

Next to the general design dimensions, our experts also discussed different contextual factors influencing the suitability of the different indicators. We used these insights to create a context space, depicted in Figure 2. It has four levels: ENVIRONMENT, USER GROUP, TYPE OF TRANSITION, and CHARACTERISTICS OF TRANSITION.

Environment. Our experts discussed how the type of environment influences the suitability of the different security indicators. Here, our experts emphasized that the indicator as a companion only fits *Gamified* environments or applications specifically designed for children (E5): *"If it's a game [...] and weird creatures are running around all the time anyway, suddenly some thing jumps around the corner and says: Here, you're going into the wrong world or something. That would be okay."* In contrast, neutral indicators might fit more in *Serious* environments, such as meeting rooms (E5, E6). Additionally, our experts differed between *Familiar* and *Unfamiliar* environments. While unfamiliar environments call for stricter standardization since it might otherwise be hard or impossible for users to differentiate security indicators from other elements, familiar environments allow for more experimental indicators (E8).

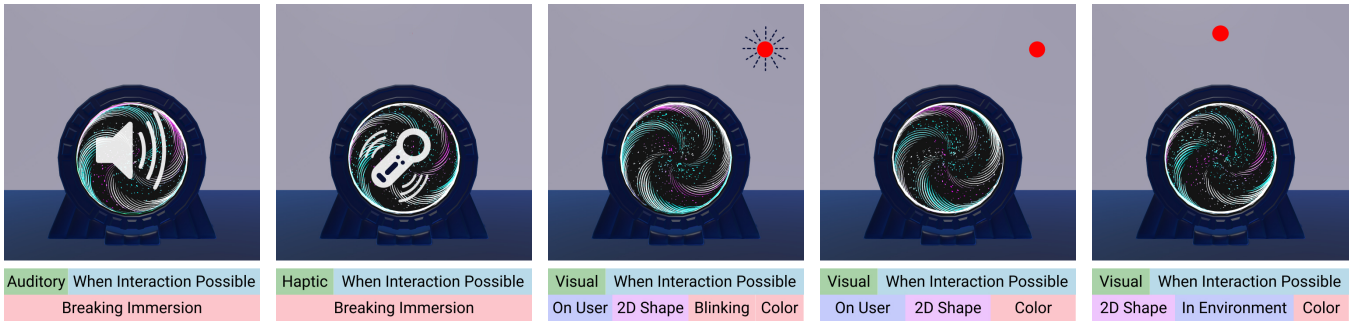
User Group. One factor related to the type of environment mentioned previously is the *Age* of the user. While more serious and neutral indicators are suitable for adults, playful indicators might be used for children: *"I think a stuffed animal [...] would be quite suitable for children (E5)."* The other differentiating factor is the *Level of Experience*. While warning notifications containing text might be suitable to teach inexperienced users the meaning of the indicator, more experienced users might be annoyed by extensive explanations and, thus, prefer more concise indicators (E6).

Way of Transitioning. Transitioning between applications might happen in different ways. While some transitions happen through *Portals*, others, for example, happen through an invitation that includes a *Link* or confirmation *Button* (E2), which in turn determines where a security indicator should and could be placed, as E2 explained: *"The information about whether the transition is safe is not so relevant if I stand ten meters away from the portal. But if I am really close to the portal, it is because only then can I start the transition."*

Characteristics of Transitions. Here, the *Duration* and *Frequency* of a transition matter (E3, E8). Quick transitions call for simple indicators that can be understood quickly, as E3 explains: *"Often, transitions happen very quickly. And then you also have to react very quickly (E3)."* Moreover, while transitions that happen very rarely need to be more obtrusive and contain additional information so that the user understands them, security indicators for frequent transitions can be reduced to simpler versions as the user is already familiar with them (E8).

3.3.3 Indicator Selection

We selected five different indicators to test in our user study, considering our experts' feedback and taking additional design constraints into account. The indicators can be seen in



(a) Audio (b) Haptic (c) Blinking (d) Peripheral (e) Static

Figure 3: The five indicators evaluated in our user study and the design dimensions used to create them.

Figure 3. Our most vital consideration was not restricting the metaverse designers' freedom by placing the indicators directly in the 3D environment. Here, we ensured that the indicator does not occupy more than one sense at a time (e.g., visual and auditory), as this would drastically reduce the expressive freedom of designers and developers of VR environments. Thus, we only use one modality (i.e., one sense) at a time. Moreover, we also wanted to investigate all MODALITIES (see Figure 1) the experts suggested at least once to explore the full design potential (except for olfactory indicators, as dispensing smells is not technically feasible at the moment). In addition, we designed two more visual indicators that, however, in contrast to the other indicators, do not interfere with the 3D environment design as they are not placed in the environment (see Figure 1, *In [the] Environment*) but anchored in the user's field of view (see Figure 1, *On [the] User*). These considerations led to the following five indicators: (1) An *audio* indicator in the form of an unpleasant warning sound (constant 1000Hz beep) as suggested by E3, whereby a secure transition is indicated by no sound similar to a fire or ambulance siren that only sounds when there is danger. (2) A *haptic* indicator using the heart rate pattern suggested by E6, whereby a calm heart rate pattern indicates a secure transition, and an elevated pattern an insecure transition. The following three indicators were color-coded 2D shapes, whereby secure transitions are colored green and have square shapes, and insecure transitions are red and round (we added the shapes to support acceptability needs). These indicators differ in their placement and whether they used a blinking effect: (3) a *visual peripheral blinking* indicator, (4) A *visual peripheral static* indicator, and (5) a *visual static* indicator above the portal.

4 Indicator Evaluation

We conducted a lab study with 25 participants to evaluate the security indicators for their effectiveness (**RQ2**), usability (**RQ3**), notification qualities (**RQ4**), and overall user preference (**RQ5**). We developed a maze VR game containing several portals which participants could use to teleport themselves closer to the exit. We used a maze to (1) simulate the interconnectivity of the metaverse and (2) force the participants to make several decisions without having them focus too intensely on the security indicators as they also would not in real life. We used a within-subject study design. Thus, all five security indicators were tested by all participants in a randomized order to prevent order effects. The goal for participants was to distinguish the secure portals from the insecure ones with the help of the security indicators while finding the maze's exit as quickly and gaining as many points as possible.

4.1 Apparatus

Our environment and task design were motivated by the need to enable frequent hyperlinking: The primary focus was to test whether participants could make split-second decisions when transitioning between portals. We aimed at replicating situations where these decisions are made, such as when users move between pages through hyperlinking in the browser, and evaluate the security of their transition based on security indicators and related web elements. As such, we aimed to provide a context where the primary task is engaging while the secondary task mimics how these split-second decisions are made. These design considerations resulted in the following maze VR environment, where the primary task was to find a path through it by making quick decisions based on security indicator evaluations.

We developed five slightly different VR mazes, see Figure 4. The VR mazes had a single path from which several dead ends branched off. We placed the portals along the path embedded into walls so participants could walk past them without using them. Each maze had eight portals (four secure and four insecure ones), with the indicator always appearing near the portal. As we found through pilot testing that several participants got lost in the maze, we designed different portals and added simple 3D objects at crossroads for orientation purposes. We added arrows near the teleportation target pointing toward the exit. Here, we ensured that participants did not go

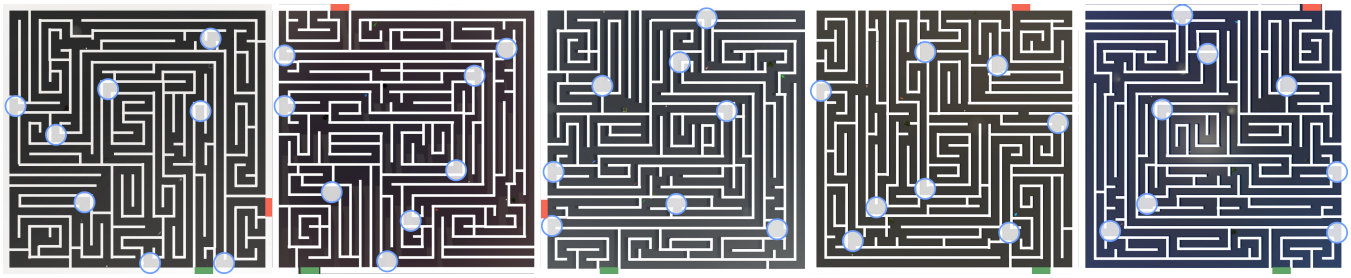


Figure 4: The five mazes with their eight portals. The entrances are marked green and the exits are marked red.

in the wrong direction after using a portal.

Even though we paid attention to making the mazes similar in difficulty, we randomly paired indicators and mazes for each participant to prevent biases. In addition, we also randomized the assignment of secure and insecure portals within each maze. In Figure 4, we depict the location of each portal.

The participants started the game with 100 points on the scoreboard. When going through a secure portal, participants received 10 points and lost 10 points for an insecure portal. Additionally, we presented them with a timer for each maze. The points serve as a gamification element and should motivate the participants to deal with the portals actively and to choose secure connections, mimicking real-world behavior. Even though users do not get actively rewarded for choosing secure connections in real life, most intrinsically do so to protect their data. As our participants knew they were in a study setting without real danger, we needed a well-enough simulation of negative consequences for choosing an insecure connection. Thus, we deducted points when participants chose an insecure portal. The timer is a constant reminder not to lose too much time at the portals – similar to how security decisions are usually not given too much time in real life.

Participants moved though the maze using point&teleport [3]. When a participant went through a portal, whether secure or insecure, they were teleported closer to the maze's exit. Here, we ensured that participants still saw all remaining portal on the way to the exit; so, no portal was ever skipped. This allows us to compare the final time while the use of a wrong portal is penalized by point reduction only.

4.2 Procedure

After we welcomed our participants and answered any open questions, we asked them to sign a consent form. Next, we asked them to provide demographic data. Before starting with the first maze, we introduced the VR environment and explained the controllers. Afterward, the participants could test the movement within the environment by teleporting in place and by testing teleportation through portals. Before the first maze, each participant received a short onboarding, which explained how to move around within the maze, what the portals looked like, and how to use them. We prepared an instructions sheet which we read out to our participants to ensure we conveyed all information consistently. In this sheet, we explained that our participants would be confronted with 5 different mazes, that each maze would contain "good" and "bad" portals, and that "good" portals would gain 10 points, while "bad" portals would deduct 10 points. We informed our participants that they would have 100 points available at the beginning and that a timer would run along. Moreover, we told our participants that, while they are not forced to use the portals, the portals would teleport them closer to the maze's exit. Finally, we told our participants to complete the maze with as many points and as quickly as possible.

Afterward, participants made their way through the maze. After completing each maze, we monitored cybersickness using the scale by Keshavarz and Hecht [28]. Additionally, we asked them to fill in the User Experience Questionnaire (UEQ) [44] and four notification-related questions by Rzayev et al. [41] that asked about intrusiveness, disturbance, noticeability, and understandability. After completion, they put on the headset and continued with the next maze.

We finished the study by rating indicators on a scale from 0-100 using the item *"I would like to use the security indicator in my daily VR experience."* Additionally, we conducted a short interview asking which indicator they liked the best and least and exploring possible design alternatives. Depending on the participants' feedback, the conversation was deepened.

4.3 Participants

We recruited 25 participants (14 female and 11 male) aged 18 to 62 years (M = 26.2, SD = 8.7). None of the participants reported having a color vision deficiency. Most participants (17) were students, while 3 were Ph.D. students, 3 were unemployed, and 2 worked as IT consultants. Four participants reported no experience with VR, 13 had used VR about 1-3 times, 5 said they had used VR 4-7 times, and 3 said they had used VR more than 7 times. Two participants owned a head-mounted display. We compensated the participants with either 10 EUR or one participant hour[6].

[6]The students at our institution have to earn a certain amount of study credits towards completing their degree, where one hour equals one course credit. Participation is anonymous, and the students receive the same com-

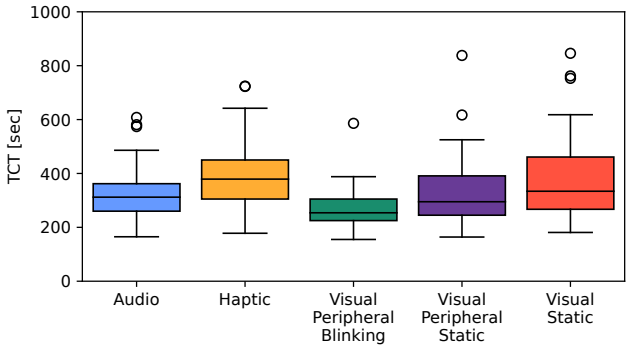


Figure 5: The task completion time of the maze VR game.

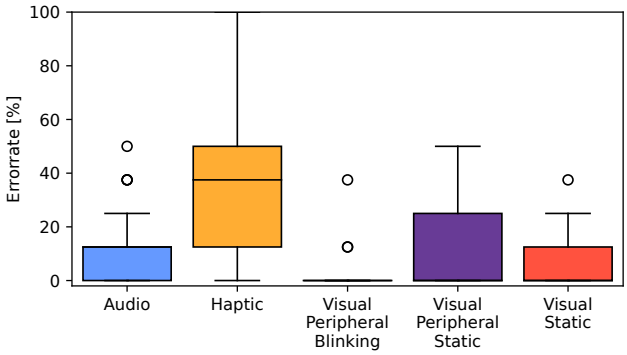


Figure 6: The average error rate for entering the portals.

5 Indicator Evaluation Results

We first describe our quantitative results, followed by the qualitative results we collected after the study through interviews.

5.1 Quantitative Results

We used Python and R to analyze the data. We report task completion time (**RQ2**), accuracy (**RQ2**), usability (**RQ3**), notification quality (**RQ4**), and overall user preference results (**RQ5**).

Task Completion Time (RQ2). First, we analyzed the time participants needed to complete the maze, namely, task completion time (TCT), see Figure 5. As a Shapiro-Wilk normality test showed that the data is significantly different from a normal distribution ($W = .971$, $p = .009$), we performed a Friedman test which revealed a significant difference for TCT ($\chi^2(4) = 18.336$, $p < .001$, *Kendall's* $W = 0.183$). We used pairwise Wilcoxon signed rank test as post hoc tests with Bonferroni correction applied that revealed that participants were significantly slower using the *Haptic* than the *Visual Peripheral Blinking* indicator ($p = .031$) and significantly faster with the *Visual Peripheral Blinking* than the *Visual Static* indicator ($p < .007$), all others $p > .05$.

Error Rate (RQ2). Next, we analyzed participants' accuracy using the portals in the maze, see Figure 6. Here, getting all 8 portals correct counts as 0% error rate. When a player misses or takes an insecure portal, we added 1/8 of the total error (12.5%). As a Shapiro-Wilk normality test showed that the data is significantly different from a normal distribution ($W = .702$, $p < .001$), we performed a Friedman test which revealed a significant difference for error rate ($\chi^2(4) = 31.047$, $p < .001$, *Kendall's* $W = 0.310$). Pairwise Wilcoxon signed rank test as post hoc tests with Bonferroni correction applied revealed that participants made significantly more errors using the *Haptic* indicator than the *Audio* ($p < .017$), *Visual Peripheral Blinking* ($p < .002$), *Visual Peripheral Static* ($p < .012$), and *Visual Static* ($p < .007$) indicator. In addition, participants made significantly more errors using the *Audio* than the *Visual Peripheral Blinking* ($p < .007$) indicator, all others $p > .05$.

pensation, no matter their responses.

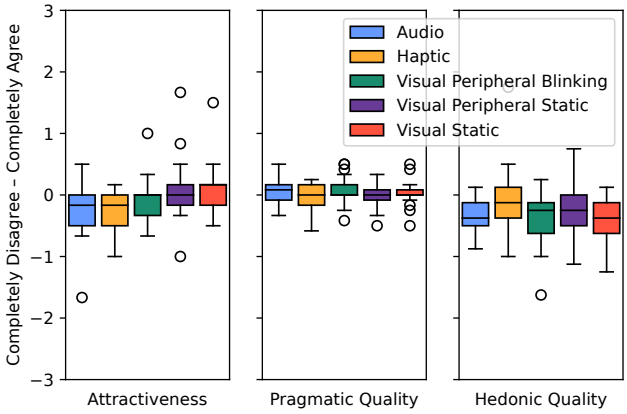


Figure 7: The results of the UEQ [44].

User Experience Questionnaire (RQ3). Next, we analyzed the User Experience Questionnaire (UEQ) [44] with its three sub-scales: *Attractiveness*, *Pragmatic Quality*, and *Hedonic Quality*, see Figure 7. As a Shapiro-Wilk normality test showed that the data of the three scales is significantly different from a normal distribution ($W = .903$, $p < .001$; $W = .969$, $p < .007$; $W = .945$, $p < .001$; respectively), we again performed Friedman tests.

For *Attractiveness*, the Friedman test revealed a significant difference ($\chi^2(4) = 20.21$, $p < .001$, *Kendall's* $W = 0.202$). We applied pairwise Wilcoxon signed rank tests with Bonferroni correction applied that revealed that the *Visual Static* indicator was perceived significantly more attractive than the *Haptic* indicator ($p < .001$), all others $p > .05$.

For *Pragmatic Quality*, the Friedman test revealed no sig-

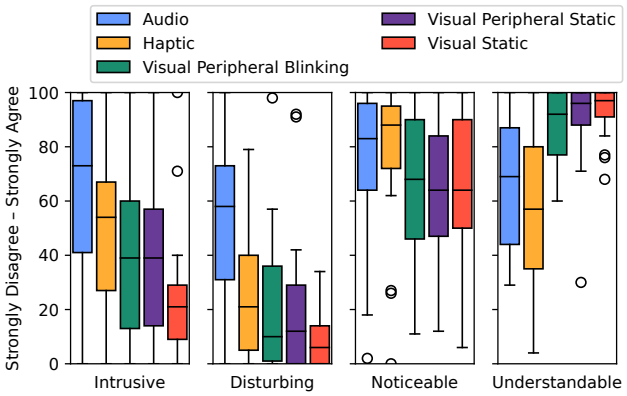


Figure 8: The four measures for a good user experience of notification by Rzayev et al. [41].

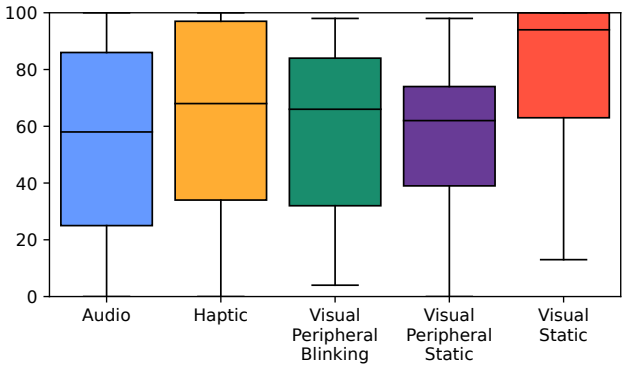


Figure 9: The results of how the participants rated if they would like to use the security indicator in their daily VR experience.

nificant differences ($\chi^2(4) = 7.145$, $p = .128$, *Kendall's* $W = 0.071$).

For *Hedonic Quality*, the Friedman test revealed a significant difference ($\chi^2(4) = 12.511$, $p < .014$, *Kendall's* $W = 0.125$). However, Pairwise Wilcoxon signed rank test post hoc tests with Bonferroni correction applied did not reveal significant differences, all $p > .05$.

Notification Quality (RQ4). We investigated the indicators' notification quality using the factors *Intrusive*, *Disturbing*, *Noticeable*, and *Understandable* by Rzayev et al. [41], see Figure 8. Again all four measures are not normally distributed, ($W = .927$, $p < .001$; $W = .852$, $p < .007$; $W = .905$, $p < .001$; $W = .823$, $p < .001$; respectively).

For *Intrusive*, the Friedman test revealed significant differences ($\chi^2(4) = 34.358$, $p < .001$, *Kendall's* $W = 0.344$). Pairwise Wilcoxon signed rank test as post hoc tests with Bonferroni correction applied revealed that participants perceived the *Visual Static* indicator significantly less intrusive than the *Audio* ($p < .003$) and *Haptic* ($p < .040$) indicator, all others $p > .05$.

For *Disturbing*, the Friedman test revealed significant differences ($\chi^2(4) = 40.57$, $p < .001$, *Kendall's* $W = 0.406$). Pairwise Wilcoxon signed rank test as post hoc tests with Bonferroni correction applied revealed that participants perceived the *Audio* indicator significantly more disturbing than the *Haptic* ($p < .047$), *Visual Peripheral Blinking* ($p < .004$), *Visual Peripheral Static* ($p < .002$), and *Visual Static* ($p < .001$) indicator, respectively. In addition, participants perceived the *Haptic* indicator significantly more disturbing than the *Visual Static* ($p < .008$) indicator, all others $p > .05$.

For *Noticeable*, the Friedman test showed no significant differences ($\chi^2(4) = 9.205$, $p < .056$, *Kendall's* $W = 0.092$).

For *Understandable*, the Friedman test revealed a significant difference ($\chi^2(4) = 31.686$, $p < .001$, *Kendall's* $W = 0.317$). Pairwise Wilcoxon signed rank test post hoc tests with Bonferroni correction applied revealed that participants perceived the *Audio* indicator significantly less understandable than the *Visual Peripheral Blinking* ($p < .049$), *Visual Peripheral Static* ($p < .010$), and *Visual Static* ($p < .002$) indicator, respectively. Moreover, participants perceived the *Haptic* indicator significantly less understandable than the *Visual Peripheral Static* ($p < .003$), *Visual Static* ($p < .001$), and *Audio* ($p < .047$) indicator.

Overall User Preference (RQ5). Finally, we analyzed the question *"I would like to use the security indicator in my daily VR experience."* A Shapiro-Wilk normality test showed that the data is significantly different from a normal distribution ($W = .925$, $p < .001$), see Figure 9. As the Friedman test revealed significant differences ($\chi^2(4) = 11.728$, $p < .019$, *Kendall's* $W = 0.117$), we again used pairwise Wilcoxon signed rank test as post hoc tests with Bonferroni correction applied that revealed that participants liked the *Visual Static* indicator significantly more than the *Visual Peripheral Blinking* indicator ($p < .019$), all others $p > .05$.

5.2 Qualitative Results (RQ3-5)

We recorded and transcribed all interviews and used thematic analysis to analyze our data [2]. Two authors independently coded the interviews using Atlas.ti. Finally, a third author joined the group to form code groups and overarching themes. We reworked and refined these themes through multiple hour-long sessions. This process resulted in two themes: *Feedback on Indicators* and *Indicator Design Suggestions*.

5.2.1 Feedback on Indicators

Ten participants named the *visual static* indicator above the portal as the best indicator (P7, P8, P11, P15, P16, P17, P20, P21, P24, P25), as they found it very understandable and not

disturbing. Moreover, three participants (P8, P20, P24) explained that the placement made it easier to understand that the indicator belonged to the portal: *"It's also extremely clear where it belongs and what it's supposed to say (P8)."* On the contrary, four participants liked this indicator the least (P5, P12, P18, P19). P18, for example, found that the indicator provided too little feedback. In addition, all participants criticized that the indicator on top of the portal had not been noticeable enough, as you had to look up to see it.

In contrast, nine participants liked the *haptic* indicator best (P1, P4, P5, P10, P12, P14, P21, P22, P23) since they considered it very noticeable and understandable while not being intrusive. Participants also found the *haptic* indicator fun to use and liked that it did not block the visual sense and, thus, did not take the focus off the main task (P14, P23): *"You just notice in your hand: okay, right, something's happening (P23)."* In contrast, seven participants liked the *haptic* indicator the least (P2, P3, P6, P8, P9, P20, P24). Reasons included that they found the feedback very intrusive (P6) and criticized that the difference between the indicator and a possible hardware problem of the controllers was unclear. Moreover, seven participants could not tell the difference between the different vibration patterns (P2, P3, P6, P8, P9, P20, P24).

Three participants named the *visual peripheral blinking* indicator as the best (P2, P6, P9). Reasons included that it was easy to understand (P18, P19), not distracting (P3, P18), and did not interfere with the main task (P18). In contrast, four participants rated this indicator as the worst (P1, P7, P22, P23). Here, one participant stated that it was intrusive and took the focus away from the main task by flashing (P23). Additionally, P22 and P23 found this indicator very annoying and distracting, and two participants criticized that they had to actively wait for the indicator's first flashing before knowing whether the portal was secure (P22, P23).

Three participants liked the *visual peripheral static* indicator the best (P2, P6, P9), while five liked it the least (P1, P4, P7, P13, P15). Here, two participants stated that they did not immediately recognize the indicator (P1, P4). Another participant did not find the indicator clearly understandable (P15), and another criticized that the indicator was placed far outside the field of view and moved along with the movement of the head (P7).

The *audio* indicator was mentioned least frequently as the best one, with only two participants naming it (P7, P13). In contrast, it was named the worst by ten participants (P6, P8, P10, P11, P16, P17, P20, P21, P24, P25). Four of the participants stated that the *audio* feedback was not intuitive since it only sounded when there was a risk (P8, P17, P24, P25). Moreover, nine participants found the audio signal very annoying, and P20 confused the security indicator with a siren from real life: *"At the beginning, I thought: okay, that's now an alarm from the real world (P20)."*

5.2.2 Indicator Design Suggestions

We also asked participants for additional design ideas for security indicators. Our participants suggested single modality and combined modalities security indicators. The single modality indicators included auditory, haptic, and visual indicators, and the combined indicators included audio/visual and haptic/visual combinations.

Single Modality Indicators. Three participants suggested audio indicators (P1, P11, P18) as they considered them the most noticeable: *"I find audio the easiest. Because for the others, you have to pay more attention to find the signal or see where's coming from (P1)."* P18 suggested an auditory indicator where the sound volume is linked to the distance to the portal and where the sound only appears if there is a risk. Two participants additionally suggested an audio indicator with two different types of sound instead of only playing sound when a risk exists (P21, P23): *"I would work with a tone that is rather soft and one that is deep, which is then negative (P23)."*

Three participants designed haptic feedback (P4, P10, P23). P4 suggested haptic feedback that only appears during an impending risk. Similar to the audio indicator used in the study, which played a sound only during a risk. P23 suggested adjusting the heartbeat pattern to be more clearly recognizable by increasing the pause between the pulses.

Eleven participants suggested a visual indicator (P3, P6, P7, P8, P9, P11, P12, P15, P17, P20, P24). P20, for example, imagined an indicator where the behavior and design of the portal indicate possible security issues by, for example, adding animated sparks. Three participants (P15, P24) suggested a visual indicator that used an X symbol for bad transitions and a tick symbol for good ones: *"I think I would just do it with X and a checkmark. [...] Because that is understandable for people who perhaps have a red-green visual impairment, or in other cultures where colors mean something else (P15)."*

Combined Modalities Eight participants proposed security indicators that combined two modalities. P2 suggested a combination of auditory and visual feedback in the periphery, and P13 suggested combining audio with a visual indicator above the portal. Five participants suggested combining haptic and visual feedback. P6 suggested a combination of a peripherally placed indicator and haptic feedback. In contrast to the haptic patterns used for this study, the controllers should only vibrate shortly in the case of a risk. If there is no risk, no haptic feedback should be given. Two participants suggested combining haptic with visual blinking feedback, whereby the blinking should only appear in case of a risk. P22 suggested a visual indicator displayed both when there is risk and when there is no risk, but that vibrates only on insecure transitions.

6 Discussion

Our study (N=25) shows that the visual blinking indicator in the periphery performed best regarding accuracy and task completion time (**RQ2**) as an indicator for hyperlinking in the metaverse. On the other hand, our participants preferred the static visual indicator above the transition portal (**RQ5**). Participants voiced that searching for the visual blinking indicator was seen as a challenge, and the blinking seemed distracting (**RQ3**, **RQ4**). This is in line with Ghosh et al. [18], who also found visual search distracting too much from the primary task in their study on VR interruption design.

While there is no prior research on security indicators in VR, we see parallels to the privacy notice design spaces by Feng et al. [13] and Schaub et al. [42]. As our primary focus is alerting the user about security considerations, our design space focuses on mechanisms to grab the user's attention and not to offer interaction possibilities. Thus, we found very similar design dimensions, such as modality and timing, but also clear differences, as, for example, a choice and functionalities do not exist for security. This sets our new security indicator design dimensions apart from prior research on privacy. Concurrently, we argue that our additional design dimensions have the potential to enrich the design spaces of prior work, allowing them to design with more dimensions.

6.1 The Dominance of Visual Indicators

Overall, visual indicators outperformed haptic and audio ones across most of our measures. The auditory and haptic indicators were only rated higher regarding noticeability. This confirms findings from prior work on VR interruptions, which also found haptic notifications more noticeable [18]. However, contrary to our results, Ghosh et al.'s [18] results overall lean towards audio and haptic as a favored modality. Ghosh et al. [18] showed that visual indicators, independent of their placement, performed worse concerning reaction time and task completion time than haptic and audio. Of course, the differences in the type of task participants had to complete in the studies influenced these results, and they cannot be directly compared. However, the combined results strongly indicate the need to use haptic indicators sparingly.

We argue that the lack of familiarity with the VR environment is another reason users preferred the static visual indicator. However, the blinking indicator in the periphery performed best regarding accuracy and task completion time. In our study, users were unfamiliar with the VR environment, and the static indicators might have given a sense of user agency, whereby users perceived to be in control when knowing where to locate the static indicator. Moreover, the static indicator is directly coupled with a portal; and, thus, is less likely to be confused with another transition that might happen nearby. This discrepancy needs to be reviewed in future work, for example, in the form of a longitudinal study that allows participants to familiarize themselves with the environment and indicators over a longer period of time.

Design Recommendation 1: Visual indicators, independent of placement in the VR scene, may be used for frequent messages/interactions, such as requesting permissions. They were perceived to be non-intrusive and understandable and, on average, scored highest with regard to performance. This will allow users to quickly engage with them, reducing the cognitive load needed to return to the main task.

6.2 The Potential of Haptic Indicators

The polarizing qualitative feedback indicates the need to use haptics sparingly. While some participants liked that it did not overlay the visual sense already in use for the main task, others were irritated by their lack of understanding of the vibration patterns. Based on prior work Mäkelä et al. [34], we argue that learning effects may overcome this over time. Mäkelä et al. [34] also highlight the value of hidden modalities, such as being out of sight of the primary task and the user's field of view. Thus, haptic and auditory indicators can support users to focus on the primary task while delivering additional security information. However, when combining these statements with the quantitative results, we found that the haptic indicator lacked understandability, was intrusive, and negatively affected task performance. Thus, we recommend leveraging this modality's noticeability and hidden aspect while being wary of its lack of understandability and high intrusion.

Yet, from a VR designer's perspective, an argument favoring the haptic indicator is using a sense that is usually not already occupied. In contrast, the visual indicators might strongly interfere with the environment's design, and auditory feedback is frequently already used for other purposes. Thus, occupying visual or audio for security indicators would significantly reduce the designers' degrees of freedom. An important consideration when designing haptic indicators will be the limited information throughput of vibration feedback. Thus, clearly distinguishable patterns will be important and might even reduce the error rate and task completion time.

Design Recommendation 2: Haptic security indicators may be used to communicate a warning or security breach that needs immediate attention. This will effectively remove the users' attention from the main task while not limiting the designers' freedom to design the VR environment.

6.3 Balancing User Attention

A known challenge when designing security elements for hyperlinking between sites is balancing user attention between the primary task (e.g., viewing the main content of the site) and the secondary task (e.g., viewing the security elements, such as security indicators and messages) [29]. Due to the form factor in which 2D environments are presented (e.g., desktop and mobile screens), designers are limited to

a smaller, mostly visual space to communicate security elements. Our results highlight the opportunities for designers to explore the placement of visual indicators across three dimensions (static vs. peripheral, see Figure 1, PLACEMENT).

The preference for static indicators may be leveraged in tasks where performance is not the primary goal, such as visiting a museum. On the other hand, in tasks where measures such as task completion time are vital, a blinking visual indicator in the periphery may be a better design direction. Such design explorations could contribute to reducing the effect on task resumption lag, which quantifies how quickly users can return to the main task after being interrupted by the secondary one [29]. We plan to investigate this type of task versus placement effect on resumption lag in future studies.

Design Recommendation 3: The characteristics of the 3D environment may be leveraged to optimize the placement of security indicators with the type of task.

6.4 Audio as a Complementing Modality

The audio indicator performed poorly in both the quantitative and qualitative results. We ascribe this to the way it was implemented in our apparatus. As this was an exploratory study, the implementation was a constant audio tune when coming close to the portal. In the qualitative feedback, participants found this tune to be annoying and distracting from the virtual environment. Similar results were reported in Ghosh et al.'s study [18], whereby participants also found it difficult to ascribe the audio tune to the appropriate environment, virtual versus real. In a fully immersive VR experience, audio feedback is given through headphones, which theoretically makes it difficult to hear real-world sound. Based on these combined results, there seems to be an intrinsic need to be able to hear the real world and want to be part of it through the auditory sense – possibly elevated by the visual attention being solely focused on the virtual environment. Considering the above results and the qualitative feedback on combining modalities, including audio, is preferred in a multi-modal approach. Audio may be coupled with other modalities and timed in such a way that it complements visual and haptic indicators to foster engagement with the latter.

Design Recommendation 4: Audio may be used as a complementary modality in combination with visual and/or haptic security indicators. This will help users in ascribing the audio tune to the virtual environment.

6.5 Limitations

We acknowledge that the setup of the modalities is broad. This was necessary for this exploratory study, as we purposely wanted to test the extreme ends of the modalities. However, this could have affected how our haptic patterns and audio feedback were perceived, i.e., participants found the haptic pattern difficult to interpret and the audio feedback annoying.

By choosing a participatory approach for creating the design space, our first study resulted in a trend toward visual indicators. Our experts mostly shared their knowledge from existing settings, such as the browser. In such a setting, the implementation heavily relies on visual indicators. However, we argue that this focus will shift in the VR environment, where all modalities that we are using in our study are part of the immersive experience.

As we did not include a baseline condition without indicators, we can not exclude that similar task completion times might have been achieved without security indicators. Regardless, fast task completion times are only relevant when participants select secure portals in the first place. However, a baseline condition without indicators will have an average error rate of 50% (chance level accuracy). Yet, we showed that, on average, all indicators outperformed chance level accuracy. Thus, we argue a baseline condition does not help understand the security indicators.

Above, we stated that we used the points as a replacement for the users' intrinsic motivation to choose secure portals when transitioning on the web. We know that security may not be the most impactful factor compared to other factors, such as perceived usefulness [9] when transitioning on the web. However, based on learnings from the web, e.g., certificate warnings, we argue that our study design is well suited to retrieve and understand security indicators in the metaverse. Nevertheless, future work should investigate how such indicators perform in more naturalistic settings.

Finally, the contextual integrity of our results might be affected by the maze setting. Although not evident in our results, the gamified task design might have reduced the perception of personal security when evaluating the security indicators. In this study, we consciously chose to trade-off in favor of increased transition frequency.

7 Conclusion

Inspired by the rise of the metaverse, we created an initial design space for security indicators in the metaverse. We then used this design space to implement and test the five most promising indicators for their effectiveness, usability, notification qualities, and overall user preference. For that, we first conducted eight in-depth interviews with domain experts to create an initial design space for security indicators in VR. We then used these insights to implement the five most promising indicators, which we tested through a lab study with 25 participants. We found while the visual blinking indicator in the periphery performed best regarding the accuracy and task completion time, our participants preferred the static visual indicator placed above the transition portal. Furthermore, it received high scores regarding understandability while still being rated low regarding intrusiveness and disturbance. Our findings contribute to making hyperlinking within the metaverse more secure and enjoyable.

References

[1] Yomna Abdelrahman, Florian Mathis, Pascal Knierim, Axel Kettler, Florian Alt, and Mohamed Khamis. Cuevr: Studying the usability of cue-based authentication for virtual reality. In *Proceedings of the 2022 International Conference on Advanced Visual Interfaces*, AVI 2022, New York, NY, USA, 2022. Association for Computing Machinery. doi: 10.1145/3531073.3531092.

[2] Ann Blandford, Dominic Furniss, and Stephann Makri. *Qualitative HCI Research: Going Behind the Scenes*. Synthesis Lectures on Human-Centered Informatics. Springer Cham, Cham, Switzerland, 2016. doi: 10.2200/S00706ED1V01Y201602HCI034.

[3] Doug A Bowman, David Koller, and Larry F Hodges. Travel in immersive virtual environments: An evaluation of viewpoint motion control techniques. In *Proceedings of IEEE 1997 Annual International Symposium on Virtual Reality*, pages 45–52. IEEE, 1997. doi: 10.1109/VRAIS.1997.583043.

[4] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3:77–101, 01 2006. doi: 10.1191/1478088706qp063oa.

[5] Zefeng Chen, Jiayang Wu, Wensheng Gan, and Zhenlian Qi. Metaverse security and privacy: An overview. *arXiv preprint arXiv:2211.14948*, 2022. doi: 10.48550/arXiv.2211.14948.

[6] Eun Kyoung Choe, Jaeyeon Jung, Bongshin Lee, and Kristie Fisher. Nudging people away from privacy-invasive mobile apps through visual framing. In *IFIP Conference on Human-Computer Interaction*, pages 74–91. Springer, 2013. doi: 10.1007/978-3-642-40477-1_5.

[7] Lorrie Faith Cranor. Mobile-app privacy nutrition labels missing key ingredients for success. *Commun. ACM*, 65 (11):26–28, oct 2022. doi: 10.1145/3563967.

[8] Roberto Di Pietro and Stefano Cresci. Metaverse: Security and privacy issues. In *2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, pages 281–288, 2021. doi: 10.1109/TPSISA52974.2021.00032.

[9] Tamara Dinev and Paul Hart. An extended privacy calculus model for e-commerce transactions. *Information systems research*, 17(1):61–80, 2006.

[10] Haihan Duan, Jiaye Li, Sizheng Fan, Zhonghao Lin, Xiao Wu, and Wei Cai. Metaverse for social good: A university campus prototype. In *Proceedings of the 29th ACM International Conference on Multimedia*, MM '21, page 153–161, New York, NY, USA, 2021. Association for Computing Machinery. doi: 10.1145/3474085.3479238.

[11] Serge Egelman, Lorrie Faith Cranor, and Jason Hong. You've been warned: An empirical study of the effectiveness of web browser phishing warnings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '08, page 1065–1074, New York, NY, USA, 2008. Association for Computing Machinery. doi: 10.1145/1357054.1357219.

[12] Ben Falchuk, Shoshana Loeb, and Ralph Neff. The social metaverse: Battle for privacy. *IEEE Technology and Society Magazine*, 37(2):52–61, 2018. doi: 10.1109/MTS.2018.2826060.

[13] Yuanyuan Feng, Yaxing Yao, and Norman Sadeh. A design space for privacy choices: Towards meaningful privacy control in the internet of things. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21, New York, NY, USA, 2021. Association for Computing Machinery. ISBN 9781450380966. doi: 10.1145/3411764.3445148.

[14] Markus Funk, Karola Marky, Iori Mizutani, Mareike Kritzler, Simon Mayer, and Florian Michahelles. Lookunlock: Using spatial-targets for user-authentication on hmds. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI EA '19, page 1–6, New York, NY, USA, 2019. Association for Computing Machinery. doi: 10.1145/3290607.3312959.

[15] 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. In *USEC*, USEC '17. NDSS, 2017. doi: 10.14722/usec.2017.23028.

[16] Ceenu George, Mohamed Khamis, Daniel Buschek, and Heinrich Hussmann. Investigating the third dimension for authentication in immersive virtual reality and in the real world. In *2019 ieee conference on virtual reality and 3d user interfaces (vr)*, pages 277–285. IEEE, 2019. doi: 10.1109/VR.2019.8797862.

[17] Ceenu George, Daniel Buschek, Andrea Ngao, and Mohamed Khamis. Gazeroomlock: Using gaze and head-pose to improve the usability and observation resistance of 3d passwords in virtual reality. In *International Conference on Augmented Reality, Virtual Reality and Computer Graphics*, pages 61–81. Springer, 2020. doi: 10.1007/978-3-030-58465-8_5.

[18] Sarthak Ghosh, Lauren Winston, Nishant Panchal, Philippe Kimura-Thollander, Jeff Hotnog, Douglas

Cheong, Gabriel Reyes, and Gregory D. Abowd. Notifivr: Exploring interruptions and notifications in virtual reality. *IEEE Transactions on Visualization and Computer Graphics*, 24(4):1447–1456, 2018. doi: 10.1109/TVCG.2018.2793698.

[19] Nathan Green and Karen Works. Defining the metaverse through the lens of academic scholarship, news articles, and social media. In *Proceedings of the 27th International Conference on 3D Web Technology*, Web3D '22, New York, NY, USA, 2022. Association for Computing Machinery. doi: 10.1145/3564533.3564571.

[20] Uwe Gruenefeld, Andreas Löcken, Yvonne Brueck, Susanne Boll, and Wilko Heuten. Where to look: Exploring peripheral cues for shifting attention to spatially distributed out-of-view objects. In *Proceedings of the 10th International Conference on Automotive User Interfaces and Interactive Vehicular Applications*, AutomotiveUI '18, page 221–228, New York, NY, USA, 2018. Association for Computing Machinery. doi: 10.1145/3239060.3239080.

[21] Amir Herzberg and Ronen Margulies. Forcing johnny to login safely. In Vijay Atluri and Claudia Diaz, editors, *Computer Security – ESORICS 2011*, pages 452–471, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg. doi: 10.1007/978-3-642-23822-2_25.

[22] Diane Hosfelt, Jessica Outlaw, Tyesha Snow, and Sara Carbonneau. Look before you leap: Trusted user interfaces for the immersive web. *arXiv preprint arXiv:2011.03570*, 2020. doi: 10.48550/arXiv.2011.03570.

[23] Yan Huang, Yi Joy Li, and Zhipeng Cai. Security and privacy in metaverse: A comprehensive survey. *Big Data Mining and Analytics*, 6(2):234–247, 2023. doi: 10.26599/BDMA.2022.9020047.

[24] Collin Jackson, Daniel R. Simon, Desney S. Tan, and Adam Barth. An evaluation of extended validation and picture-in-picture phishing attacks. In *Financial Cryptography and Data Security*, pages 281–293, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg. doi: 10.1007/978-3-540-77366-5_27.

[25] Markus Jakobsson, Alex Tsow, Ankur Shah, Eli Blevis, and Youn-Kyung Lim. What instills trust? a qualitative study of phishing. In *Financial Cryptography and Data Security*, pages 356–361, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg. doi: 10.1007/978-3-540-77366-5_32.

[26] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder. A "nutrition label" for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, SOUPS '09, New York, NY, USA, 2009. Association for Computing Machinery. doi: 10.1145/1572532.1572538.

[27] Patrick Gage Kelley, Lucian Cesca, Joanna Bresee, and Lorrie Faith Cranor. Standardizing privacy notices: An online study of the nutrition label approach. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '10, page 1573–1582, New York, NY, USA, 2010. Association for Computing Machinery. doi: 10.1145/1753326.1753561.

[28] Behrang Keshavarz and Heiko Hecht. Validating an efficient method to quantify motion sickness. *Human factors*, 53:415–26, 08 2011. doi: 10.1177/0018720811403736.

[29] Byung Cheol Lee, Kwanghun Chung, and Sung-Hee Kim. Interruption cost evaluation by cognitive workload and task performance in interruption coordination modes for human–computer interaction tasks. *Applied Sciences*, 8(10), 2018. doi: 10.3390/app8101780.

[30] Joel Lee, Lujo Bauer, and Michelle L Mazurek. The effectiveness of security images in internet banking. *IEEE Internet Computing*, 19(1):54–62, 2014. doi: 10.1109/MIC.2014.108.

[31] Joel Lee, Lujo Bauer, and Michelle Mazurek. Studying the effectiveness of security images in internet banking. *IEEE Internet Computing*, 13, 01 2015. doi: 10.1109/MIC.2014.108.

[32] Lik-Hang Lee, Tristan Braud, Pengyuan Zhou, Lin Wang, Dianlei Xu, Zijun Lin, Abhishek Kumar, Carlos Bermejo, and Pan Hui. All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda. *arXiv preprint arXiv:2110.05352*, 2021. doi: 10.48550/arXiv.2110.05352.

[33] Eric Lin, Saul Greenberg, Eileah Trotter, David Ma, and John Aycock. Does domain highlighting help people identify phishing sites? In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '11, page 2075–2084, New York, NY, USA, 2011. Association for Computing Machinery. doi: 10.1145/1978942.1979244.

[34] Ville Mäkelä, Johannes Kleine, Maxine Hood, Florian Alt, and Albrecht Schmidt. Hidden interaction techniques: Concealed information acquisition and texting on smartphones and wearables. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21, New York, NY, USA, 2021. Association for Computing Machinery. doi: 10.1145/3411764.3445504.

[35] Lukas Mecke, Sarah Prange, Daniel Buschek, and Florian Alt. A design space for security indicators for behavioural biometrics on mobile touchscreen devices. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI EA '18, page 1–6, New York, NY, USA, 2018. Association for Computing Machinery. doi: 10.1145/3170427.3188633.

[36] Huansheng Ning, Hang Wang, Yujia Lin, Wenxi Wang, Sahraoui Dhelim, Fadi Farha, Jianguo Ding, and Mahmoud Daneshmand. A survey on metaverse: the state-of-the-art, technologies, applications, and challenges. *arXiv preprint arXiv:2111.09673*, 2021. doi: 10.48550/arXiv.2111.09673.

[37] Sang-Min Park and Young-Gab Kim. A metaverse: Taxonomy, components, applications, and open challenges. *IEEE Access*, 10:4209–4251, 2022. doi: 10.1109/ACCESS.2021.3140175.

[38] Prashanth Rajivan and Jean Camp. Influence of privacy attitude and privacy cue framing on android app {Choices}. In *Twelfth Symposium on Usable Privacy and Security*, SOUPS 2016, 2016. URL https://www.usenix.org/system/files/conference/soups2016/wpi16_paper-rajivan.pdf.

[39] Franziska Roesner, Tadayoshi Kohno, and David Molnar. Security and privacy for augmented reality systems. *Commun. ACM*, 57(4):88–96, apr 2014. doi: 10.1145/2580723.2580730.

[40] Louis Rosenberg. Regulation of the metaverse: A roadmap: The risks and regulatory solutions for largescale consumer platforms. In *Proceedings of the 6th International Conference on Virtual and Augmented Reality Simulations*, ICVARS '22, page 21–26, New York, NY, USA, 2022. Association for Computing Machinery. doi: 10.1145/3546607.3546611.

[41] Rufat Rzayev, Sven Mayer, Christian Krauter, and Niels Henze. Notification in vr: The effect of notification placement, task and environment. In *Proceedings of the Annual Symposium on Computer-Human Interaction in Play*, CHI PLAY '19, page 199–211, New York, NY, USA, 2019. Association for Computing Machinery. doi: 10.1145/3311350.3347190.

[42] Florian Schaub, Rebecca Balebako, Adam L. Durity, and Lorrie Faith Cranor. A design space for effective privacy notices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 1–17, Ottawa, July 2015. USENIX Association. ISBN 978-1-931971-249. URL https://www.usenix.org/conference/soups2015/proceedings/presentation/schaub.

[43] Stuart E. Schechter, Rachna Dhamija, Andy Ozment, and Ian Fischer. The emperor's new security indicators. In *2007 IEEE Symposium on Security and Privacy*, SP '07, pages 51–65. IEEE, 2007. doi: 10.1109/SP.2007.35.

[44] Martin Schrepp. *User experience questionnaire handbook*. Online, 2015. URL https://www.ueq-online.org/Material/Handbook.pdf.

[45] Dongwan Shin, Huiping Yao, and Une Rosi. Supporting visual security cues for webview-based android apps. In *Proceedings of the 28th Annual ACM Symposium on Applied Computing*, SAC '13, page 1867–1876, New York, NY, USA, 2013. Association for Computing Machinery. doi: 10.1145/2480362.2480709.

[46] Neal Stephenson. *Snow crash: A novel*. Spectra, 2003.

[47] Christopher Thompson, Martin Shelton, Emily Stark, Maximilian Walker, Emily Schechter, and Adrienne Porter Felt. The web's identity crisis: understanding the effectiveness of website identity indicators. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 1715–1732, Santa Clara, CA, August 2019. USENIX Association. URL https://www.usenix.org/conference/usenixsecurity19/presentation/thompson.

[48] Emanuel von Zezschwitz, Serena Chen, and Emily Stark. "it builds trust with the customers" - exploring user perceptions of the padlock icon in browser ui. In *2022 IEEE Security and Privacy Workshops (SPW)*, pages 44–50, 2022. doi: 10.1109/SPW54247.2022.9833869.

[49] Emanuel von Zezschwitz, Serena Chen, and Emily Stark. "it builds trust with the customers" - exploring user perceptions of the padlock icon in browser ui. In *2022 IEEE Security and Privacy Workshops (SPW)*, pages 44–50, 2022. doi: 10.1109/SPW54247.2022.9833869.

[50] Yuntao Wang, Zhou Su, Ning Zhang, Rui Xing, Dongxiao Liu, Tom H. Luan, and Xuemin Shen. A survey on metaverse: Fundamentals, security, and privacy. *IEEE Communications Surveys & Tutorials*, pages 1–1, 2022. doi: 10.1109/COMST.2022.3202047.

[51] Tara Whalen and Kori M. Inkpen. Gathering evidence: Use of visual security cues in web browsers. In *Proceedings of Graphics Interface 2005*, GI '05, page 137–144, Waterloo, CAN, 2005. Canadian Human-Computer Communications Society. URL https://dl.acm.org/doi/abs/10.5555/1089508.1089532.

[52] Zhi Xu and Sencun Zhu. Abusing notification services on smartphones for phishing and spamming. In *6th USENIX Workshop on Offensive Technologies*, WOOT

'12, Bellevue, WA, August 2012. USENIX Association. URL https://www.usenix.org/conference/woot12/workshop-program/presentation/Xu.

[53] Bo Zhang, Mu Wu, Hyunjin Kang, Eun Go, and S. Shyam Sundar. Effects of security warnings and instant gratification cues on attitudes toward mobile websites. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '14, page 111–114, New York, NY, USA, 2014. Association for Computing Machinery. doi: 10.1145/2556288.2557347.