Perceptions of the Privacy and Security of Virtual Reality

Abstract. Virtual Reality (VR) is an emerging technology, projected to grow into a $100B industry in the next five years. While a preliminary body of research has begun to explore security vulnerabilities and privacy threats in VR, little prior work has explored how users perceive these threats. By understanding users' perceptions early in the VR adoption lifecycle, we have a unique opportunity to inform the development of policies, educational materials, and corporate best-practices to help ensure the protection of VR users. In this poster, we present preliminary findings from a series of semi-structured interviews with VR users to understand their use of VR, their awareness of the data collected by these systems, and their privacy and security concerns.

1 Introduction & Background

Virtual Reality (VR) uses a multitude of sensors to generate "immersive, interactive, and imaginative" simulations for the user [1]. Projected to become a $100B market in the next five years, VR can be used for great good: PTSD treatment, innovative education – but can also pose significant privacy and security risks given the breadth and type of data collected by VR systems [2] to enhance simulations and drive profits.

VR risks to users fall broadly into three categories: data collection and inferences; physical harms [3,4]; and manipulation and violation of immersive experiences. Prior work has found that VR systems collect new information about users such as body and facial muscle movements, which can be used to discern users emotions [2]. Additionally, such information may be collected even when the user believes the system is off, as many headsets are "always on", enabling developers to gain data without users knowledge [5]. This data may then be sold to third parties [2] or may be leaked through known vulnerabilities [6]. VR also enables virtual crimes, which prior work has found generate strong emotional reactions similar to real-world crimes [7,8]. To protect against such threats, early work has explored defenses for VR, including authentication systems [9,10].

Despite this prior work beginning to evaluate VR threats, little prior work has explored users' perceptions of these threats. Most closely related, Motti et al. collected online comments about digital glasses and other head-mounted devices (which included a small number of VR headsets) from forums, social media, and varying websites [11]. In the work presented in this poster, we expand on their prior findings, focusing exclusively on VR and collecting more in-depth data than is available through online comments.

Similar to other, somewhat more studied IoT devices such as drones [12] little legislation or policy yet exists to protect users or guide developers of VR

systems. To establish effective protections, we must understand both the technological vulnerabilities of VR as well as users' concerns and perceptions. This understanding of perceptions can also help us to develop education and awareness materials to help users more accurately assess risk and make informed purchasing decisions. Our work takes an initial step toward providing a foundation for reasoning about privacy and security in VR by exploring users' perceptions through a series of semi-structured interviews. We are conducting these interviews with VR users, querying their motivations for using VR, awareness of data collection in VR, and privacy and security concerns. In this poster, we present the results of the first of these interviews (n=5) and outline our plans for future work.

2 Methods

Thus far, we have conducted five semi-structured interviews with VR users [1].We recruited these participants by posting advertisements in VR-related Reddit communities, Facebook groups, and online forums. Participants completed a short screening questionnaire containing demographic questions and requiring them to upload an image of themselves wearing or using a VR headset, to ensure that they were actually VR users. Eligible participants were invited to participate in a 20 minute semi-structured interview via phone, Skype, or Google hangouts, and were compensated with a $15 Amazon gift card for their participation.

Three different researchers conducted the interviews according to a semi-structured interview protocol. Participants were asked about their motivations for purchasing or using their VR system, what they do with VR, and what benefits they perceive with their current VR system. Next, participants were asked what, if any, data they think their VR system collects, how they think that data might be used and if they had any concerns about that use. Finally, participants were asked if they have privacy or security concerns with their VR system and how those concerns compare to their concerns about other technologies they use. Each interview was transcribed and the interview data was then analyzed via thematic analysis [13].

Limitations. In qualitative studies, sufficient sample size and participant diversity are necessary to decrease bias and increase the generalizability of findings. In the preliminary work presented in this poster, we interview only five participants, and our sample has an over-representation of some demographic groups. In our ongoing and future work, we plan to continue conducting interviews until new themes stop emerging [14] and will continue to recruit from a variety of sources in an effort to ensure diversity.

3 Results

Below we describe our participants and detail our preliminary findings.

[1] This study was approved by our institutional review boards.

Participants. Four out of the five participants are male; and two of the five participants identify as Asian, Native Hawaiian, or Pacific Islander, while the other three participants identify as White. The ages of the five participants varied, two of the participants are between the age of 18-29 and the other three are 30-39, 40-49, and 50-59, respectively.

Two of our participants use the Vive, three use the Oculus Rift, and two use the Gear VR (two participants use multiple systems). All five reported using VR to play games; one uses VR for education; and one uses VR to view videos and other media. Two participants also reported using VR with "real-world" friends, noting that doing so significantly enhanced their VR experience: "the social aspect completely turns VR into a different animal...it's kinda a teleportation device, even."

Findings. All participants thought that their VR systems collected some type of data about them. However, only two participants mentioned data being collected by sensors (one mentioned microphones and one mentioned cameras). The other three reported believing either that the only data collected was the data they provided when creating an account on the system (two participants), usage data (one participant), or were unsure exactly what data was collected (one participant). Additionally, one of these three participants explicitly stated that their VR system, an Oculus Rift, could not collect audio data.

We observe a preliminary trend that awareness of data collection seems to relate to level of concern about privacy and security in VR. The two participants who were aware of sensor data collection in VR expressed more or equal concern about their VR system compared to other devices they used, while the other three participants expressed less (two participants) or equal (one participant) concern about VR vs. their other devices. For example, the participant who thought their VR system collected only account and usage data said, "I'm sure it's collecting data, but it's not very personal...just usage statistics like how frequently I've been using an application and I don't really care." Similarly, the participant who was unsure what information their VR system collected stated, "If you're worried about something then you're up to something you shouldn't be doing...I know they could be collecting something...but I'm not concerned."

Participants also express different levels of concern regarding applications from different companies. Three participants explicitly expressed concern with using a Facebook application (e.g., Facebook Spaces) or device (e.g., Oculus Rift): "Considering that Oculus Rift is owned by Facebook, I was concerned [because] Facebook has been in the news recently about how much information they pick up from your habits and posting activities."

On the other hand, a fourth participant felt more secure when using the Facebook-owned Oculus product: "the old [Google] Cardboard glasses let third parties produce content...[I had] concerns with vulnerabilities in those applications...now with the Oculus store, Facebook vets it." This fourth participant was one of only two participants who expressed security-related concerns, the other participant worried about identity theft in virutal reality. This participant

thought their concern was not yet relevant, but said, "imagine if somebody can put on a VR head unit and go into a virtual world assuming your identity...I think if VR becomes mainstream [identity theft] will be rampant."

Finally, four of the five participants expressed concerns about their health or the health of others they invited to use their VR system. These concerns primarily focused on nausea, but two participants expressed concern about mental health, referencing the intensive nature of immersive VR experiences.

4 Next Steps

The results presented in this poster provide a preview of our findings regarding users' perceptions of privacy and security in VR. In future work, we plan to continue conducting interviews with VR users until new themes stop emerging. Additionally, we plan to interview VR developers in order to better understand whether they are aware of users' concerns, what concerns they have around security and privacy in VR, and how they are tailoring their development to address those concerns. By analyzing and comparing developer and user' perceptions we hope to provide a foundation for future work on privacy and security in VR and inform the development of guidelines and educational materials that can ensure a safe and enjoyable VR user experience.

References

1. LT De Paolis and A Mongelli. *Augmented and Virtual Reality*. AVR, 2015.
2. F O'Brolcháin and et al. The convergence of virtual reality and social networks: threats to privacy and autonomy. *Science and engineering ethics*, 2016.
3. SVG Cobb and et al. Virtual reality-induced symptoms and effects (vrise). *Presence: teleoperators and virtual environments*, 1999.
4. R Yao and et al. Oculus vr best practices guide. *Oculus VR*, 2014.
5. F Roesner, T Kohno, and D Molnar. Security and privacy for augmented reality systems. *Communications of the ACM*, 2014.
6. G Maganis and et al. Sensor tricorder. In *ACM MCSA*.
7. J W Nelson. A virtual property solution: How privacy law can protect the citizens of virtual worlds. *Okla. City UL Rev.*, 2011.
8. I Warren and D Palmer. *Crime risks of three-dimensional virtual environments*. PhD thesis, Australian Institute of Criminology, 2010.
9. Z Yu, HN Liang, C Fleming, and KL Man. An exploration of usable authentication mechanisms for virtual reality systems. In *IEEE APCCAS*.
10. C Goerge and et al. Seamless and secure vr: Adapting and evaluating established authentication systems for virtual reality. In *NDSS*.
11. VG Motti and K Caine. *Users' Privacy Concerns About Wearables*. 2015.
12. WG Voss. Privacy law implications of the use of drones for security and justice purposes. *International Journal of Liability and Scientific Enquiry*, 2013.
13. V Braun and V Clarke. Using thematic analysis in psychology. 2006.
14. JJ Francis and et al. What is an adequate sample size? Operationalising data saturation for theory-based interview studies. *Psychology and Health*, 2010.