Communicating Security & Privacy Information in Virtual Reality

Melvin Abraham
University of Dundee / University of Glasgow

Mohamed Khamis
University of Glasgow

1. Research Statement

Virtual Reality is becoming more affordable and will soon become ubiquitous within society. However, currently the technology is not there yet, as virtual reality can pose security and privacy risks to a user which they may not be aware of.

In Virtual Reality, information is always being collected, even when the user may believe the headset is turned off [1, 2]. Modern day headsets, are "*always on*" [1, 2]. This allows for companies to gain access to data without proper consent from the users or bystanders around the headset [2]. This data can be sold to third parties [2, 3], used for internal data analytics [5] or even stolen through a man in the middle attack. With the sheer quantity of data being collected, it is very plausible that the collection of virtual reality data may even lead to adjustments of quality, pricing of items and targeted advertisements [2, 5].

The attacks and misuse of infrared sensors data on the Head Mount Display (HMD) also pose a real threat to a user's security and privacy [2]. An individual could become a victim to blackmail, due to the clarity of the infrared image. For example, the appearance, facial expressions [4] and the surroundings [2], can be seen with sufficient detail which could lead to non-consensual data collection of both the user and their environment.

2. Future Work

Clear research exists into effectively communicating security issues using a digital medium [6, 7, 8] but none of the methods were formulated with the considerations of virtual reality in mind. For example, the immersion of the user when in a virtual environment, eye movement hotspots, the need to physically move around to interact or how to account for and protect bystanders. The methods and guidelines fail to explore and take full advantage of the capabilities available within a virtual environment.

We have yet to provide methods to communicate to a user within virtual reality, when their data is being collected or if a security vulnerability is present. This project aims to preserve a users' cyber security and privacy when using virtual reality. This will be achieved by taking advantage of the capabilities seen within virtual reality to develop novel methods of identifying threats and communicating security and privacy information to a user. This work will contribute to creating an environment that supports virtual reality users to inform and more importantly, provide knowledge to protect them-selves from security vulnerabilities and data that is being collected potentially without the users' prior knowledge or consent.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2021. August 8 -- 10, 2021, Vancouver, B.C., Canada.

2. References

[1] Franziska Roesner, Tadayoshi Kohno, and David Molnar. 2014. Security and privacy for augmented reality systems. Communications of the ACM, 57(4), pp.88-96.

[2] Devon Adams, Alseny Bah, Catherine Barwulor, Nureli Musaby, Kadeem Pitkin,and Elissa M Redmiles. 2018. Ethics emerging: the story of privacy and security perceptions in virtual reality. In Fourteenth Symposium on Usable Privacy and Security ({SOUPS}2018). pp.427– 442.

[3] Fiachra O'Brolcháin, Tim Jacquemard, David Monaghan, Noel O'Connor, Peter Novitzky, and Bert Gordijn. 2016. The convergence of virtual reality and social networks: threats to privacy and autonomy. Science and engineering ethics 22(1), pp.1–29.

[4] Steven Hickson, Nick Dufour, Avneesh Sud, Vivek Kwatra, and Irfan Essa. 2019. Eyemotion: Classifying facial expressions in VR using eye-tracking cameras. IEEE Winter Conference on Applications of Computer Vision (WACV). pp. 1626–1635.

[5] Ian Hamilton. 2019. If Logged Into Facebook, Oculus VR Data Will Now Be Used For Ads. https://uploadvr.com/facebook-ads-vr/ (Last Accessed 20 May 2021)

[6] Serge Egelman, Lorrie Faith Cranor, and Jason Hong. 2008. 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. pp.1065–1074.

[7] Elissa M Redmiles, Everest Liu, and Michelle L Mazurek. 2017. You Want Me To Do What? A Design Study of Two-Factor Authentication Messages. In SOUPS.

[8] Marian Harbach, Sascha Fahl, Polina Yakovleva, and Matthew Smith. 2013. Sorry, I don't get it: An analysis of warning message texts. In International Conference on Financial Cryptography and Data Security. Springer. pp. 94–111.