Privacy, Security and Safety Concerns of using HMDs in Public and Semi-Public Spaces

Florian Mathis
LMU Munich
Germany
Florian.Mathis@campus.lmu.de

Mohamed Khamis
University of Glasgow
UK
mohamed.khamis@glasgow.ac.uk

ABSTRACT

Head-Mounted Displays (HMDs) are increasingly used in public and semi-public spaces nowadays. However, this development comes with implications on the privacy, security, and safety of the HMD user. Based on prior work on interaction in public space, usable privacy and security, and Head-Mounted Displays, this position paper discusses the implications of HMD usage in public on the user's privacy, security and safety. We provide examples of said threats and present potential solutions that are promising for future work.

KEYWORDS

Head-Mounted Displays; Usable Security; Public HMDs

CHI'19 Extended Abstracts, May 4-9, 2019, Glasgow, Scotland UK

INTRODUCTION

Head-Mounted Displays (HMDs) are becoming increasingly affordable and portable. Today, many high-end HMDs can operate wirelessly, thus alleviating the need for requiring the user to be in a confined space. This has opened doors for HMDs to be used in a myriad of novel contexts. For example, HMDs are now used in public and semi-public spaces [5]. This includes wearing HMDs in public libraries [8], in universities [5], and even in cars [7].

The adoption of HMDs in public spaces also brings novel challenges. Namely, HMD users are often unaware of their surroundings, leading to risks to privacy, security and safety. For example, users might not want to imply that they are using certain HMD applications when observed by others for privacy reasons. The security of users might be compromised if they are trying to authenticate while wearing an HMD in public (e.g., to make purchases or log into an account). HMD users' safety is also at stake as they might bump into surrounding objects that they are not aware of, or if their HMDs are hacked to trick users into dangerous situations (e.g., showing a virtual bridge at a cliff's edge).

In this position paper, we build on previous work to derive potential implications of using HMDs in public on the user's privacy, security and safety. We then propose directions for future research.

IMPLICATIONS ON PRIVACY

Humans might act differently when they know they are being watched. For example, previous work showed repeatedly that users do not like performing mid-air gestures for input while in public space [1, 4]. McGill et al. also highlighted the significance of awareness of the HMD user's surroundings [6]. The fact that public HMD users are not aware of the presence of bystanders means that they are not aware if they are being observed. This might result in HMD users being surprised to find that they were not alone after they take off their HMDs. This raises privacy concerns as users might not want to perform certain movements, or imply that they are using certain HMD applications, while being observed by others.

This can be addressed by designing methods that inform the user of the presence of bystanders. There has been some work in this area (e.g., see [6]), but there is a gap in 1) understanding the full implications of using HMDs in public on privacy, and in 2) designing methods to either inform the user of bystanders or protect their privacy when they are being observed. A potential direction is to use motion sensors and eye trackers to detect the presence of bystanders, and alert the users as done previously on mobile devices [10].

Sidebar 1: The scenario above shows a possible theft where an attacker (red box) reaches out for personal belongings (yellow box) of the HMD user (blue box). In such a scenario HMD users are immersed in a virtual environment, and thus are 1) not in control of their personal belongings, and 2) have no information about the current status of their personal belongings. Therefore, it is necessary to design, develop and evaluate novel approaches to notify the HMD user about theft attacks (e.g., via visual cues) in public and semi-public spaces.

IMPLICATIONS ON SECURITY

Applications of virtual reality already include virtual shopping (e.g., payment transactions, micro transactions within VR games) or social platforms (e.g., AltspaceVR, Facebook Spaces) where it is necessary for users to be able to authenticate within a secure and trusted environment. This can be seen as a challenge because users are not necessarily aware of their external environment. They can be observed by others during the execution of purchases or logging into an account, especially in public and semi-public spaces. Previous work [3, 9] presented the first steps for designing authentication schemes that are suitable for VR environments. Nevertheless, in the work of George et al. [3] 18% of the passwords were successfully guessed by observations. This shows that there is a need for more usable and secure authentication schemes for VR. The improvement of usable and secure authentication schemes can be seen as a further direction for future work. We argue, that novel authentication schemes for VR have the potential to increase the usability and security and thus, reduce the number of successful attacks.

While their work focused on tasks executed within the virtual environment (in this case authentication), there are also implications on personal belongings outside of the virtual environment. Consider a situation where a user puts his bag on the floor while using an HMD (see Sidebar 1). Such a situation would not only decrease the level of control of personal belongings, it also increases the probability for successful theft attacks in public and semi-public spaces.

One promising approach to keep the level of control of personal belongings in VR up could be to overlay the virtual scene with real world information which represent the status of personal belongings (e.g. a bag) in an unobtrusive way. Whereas this method may lead to an information overload and may decrease the level of immersion, another promising approach would be instead of showing the user real world information within the virtual environment, to trigger a notification immediately when such an attack happens (e.g., via haptic, visual or auditory cues). Work by McGill et al. [6] shows that the provision of information from the real world should happen without forcing users to put off their HMDs. While McGill et al. [6] focused on the interaction with objects and the co-presence of others in the real world, it is still unclear to what extent environment awareness must be provided to HMD users. It is necessary to provide users a feeling of being in a secure situation without having an impact on impassiveness.

IMPLICATIONS ON SAFETY

The use of HMDs in crowded or alternating spaces can be risky. By taking the two following situations into account: 1) A public space (e.g. a huge shopping centre), and 2) A semi-public space (e.g. living room in a shared flat), HMD users might not see what's around them and might bump into real world objects (e.g., chairs, tables) or into other present humans. A Mixed Reality (MR) approach could be

used to tackle safety concerns of users by displaying parts of the real world in the virtual scene. This can be done by scanning real world objects and embed them in the VR scene directly or by sampling and creating a 3D replica of a real world object. In such a case it is important to distinguish between virtual and real objects to avoid misinterpretations which have the potential to lead into an unsafe situation. Looking through the lens of HCI, users should be trained to distinguish real objects from virtual 3D generated objects. A challenge is how to balance this with immersiveness.

The possibility to embed real and virtual objects into such a scene provides an opportunity for attackers to manipulate virtual scenes from an external point of view. This can be abused by displaying non-existent objects within the scene. Consider a case where an attacker displays a virtual bridge over a cliff. In such a case, a user's life might be subject to danger. Therefore, it is necessary to secure HMDs against "man-in-the-middle attacks" where external unauthorised attackers change the virtual scene in a way that could cause harm to the user.

CONCLUSION

HMDs are already in their early stage to find use in public spaces such as libraries, universities and cars [5, 7, 8]. There is still a gap in understanding the full implications of using HMDs in public and semi-public spaces regarding privacy, security, and safety. Future works have to address these challenges and consider to what extent methods to inform and protect users from external potential risks (e.g. obervations from other present humans) affect user's usability and immersiveness. Upcoming approaches have to be evaluated in terms of privacy, security and safety protection, and also in terms of usability, presence and immersiveness. Further upcoming challenges include the distinction between different intentions of observating HMD users (e.g. shoulder surfing). While friends of an HMD user may observe the interaction to provide cues about obstacles in the real world and thus, their intention is to support the user, some others may observe mid-air gestures to infer personal data such as password inputs. We argue that the distinction of the two mentioned scenarios 1) shoulder surfing to support the current user, and 2) shoulder surfing as a social engineering technique used to obtain information is a novel upcoming challenge within HMDs and differs from shoulder surfing in the context of other applications such as mobile devices (e.g. in [2]). Thus, an HMD in public and semi-public spaces which considers privacy, security, and safety aspects has to distinguish between different secondary characters and has to alternate unobtrusive between different states in a way that doesn't impact the actual HMD user.

The ideal system would consider both the protection of the user in terms of privacy, security, and safety as well as securing high usability, presence and immersiveness.

REFERENCES

[1] Harry Brignull and Yvonne Rogers. 2003. Enticing people to interact with large public displays in public spaces. In *Proceedings of INTERACT*, Vol. 3. 17–24.

[2] Malin Eiband, Mohamed Khamis, Emanuel Von Zezschwitz, Heinrich Hussmann, and Florian Alt. 2017. Understanding shoulder surfing in the wild: Stories from users and observers. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, 4254–4265. https://doi.org/10.1145/3025453.3025636

[3] Ceenu Goerge, Mohamed Khamis, Emanuel von Zezschwitz, Marinus Burger, Henri Schmidt, Florian Alt, and Heinrich Hussmann. 2017. Seamless and Secure VR: Adapting and Evaluating Established Authentication Systems for Virtual Reality. In *Proceedings of the Network and Distributed System Security Symposium (NDSS 2017) (USEC '17)*. NDSS. https://doi.org/10.14722/usec.2017.23028

[4] Mohamed Khamis, Ludwig Trotter, Ville Mäkelä, Emanuel von Zezschwitz, Jens Le, Andreas Bulling, and Florian Alt. 2018. CueAuth: Comparing Touch, Mid-Air Gestures, and Gaze for Cue-based Authentication on Situated Displays. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 4, Article 174 (Dec. 2018), 21 pages. https://doi.org/10.1145/3287052

[5] Christian Mai and Mohamed Khamis. 2018. Public HMDs: Modeling and Understanding User Behavior Around Public Head-Mounted Displays. In *Proceedings of the 7th ACM International Symposium on Pervasive Displays (PerDis '18)*. ACM, New York, NY, USA, Article 21, 9 pages. https://doi.org/10.1145/3205873.3205879

[6] Mark McGill, Daniel Boland, Roderick Murray-Smith, and Stephen Brewster. 2015. A Dose of Reality: Overcoming Usability Challenges in VR Head-Mounted Displays. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 2143–2152. https://doi.org/10.1145/2702123.2702382

[7] Mark McGill, Alexander Ng, and Stephen Brewster. 2017. I Am The Passenger: How Visual Motion Cues Can Influence Sickness For In-Car VR. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 5655–5668. https://doi.org/10.1145/3025453.3026046

[8] Ilya Minyaev, Matti Pouke, Johanna Ylipulli, and Timo Ojala. 2018. Implementation of a Virtual Reality Interface for a Public Library. In *Proceedings of the 17th International Conference on Mobile and Ubiquitous Multimedia (MUM 2018)*. ACM, New York, NY, USA, 513–519. https://doi.org/10.1145/3282894.3289718

[9] Zhen Yu, Hai-Ning Liang, Charles Fleming, and Ka Lok Man. 2016. An exploration of usable authentication mechanisms for virtual reality systems. In *Circuits and Systems (APCCAS), 2016 IEEE Asia Pacific Conference on*. IEEE, 458–460. https://doi.org/10.1109/APCCAS.2016.7804002

[10] Huiyuan Zhou, Khalid Tearo, Aniruddha Waje, Elham Alghamdi, Thamara Alves, Vinicius Ferreira, Kirstie Hawkey, and Derek Reilly. 2016. Enhancing Mobile Content Privacy with Proxemics Aware Notifications and Protection. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, NY, USA, 1362–1373. https://doi.org/10.1145/2858036.2858232