Vulnerabilities of Mediated Embodiment: Towards Unmasking Security and Privacy Risks of Ability-Mediating Wearables

Radu-Daniel Vatavu

MintViz Lab, MANSiD Research Center, Ştefan cel Mare University of Suceava

Abstract

Wearables designed to mediate user perception and/or action present specific challenges regarding the security and privacy of their users. The objective of this position paper is to raise awareness about the potential threats that arise when mediating user perception and action through technology that draws from wearable computing, ambient intelligence, and virtual and augmented reality environments. As the boundaries between these areas of computing become increasingly blurred, security and privacy threats escalate. Consequently, it is crucial to start examining the potential risks associated with wearable systems that provide highly personal, embodied, and intimate experiences taking place on the user's body or experiences that are integrated with the body.

Keywords

Wearable computing, mediated embodiment, mixed reality, augmented reality, ambient intelligence, mediated reality, security, privacy, threats, sensorimotor realities

1. Introduction

As wearable devices, such as smart watches, glasses, and jewelry, become more complex in terms of sensing and processing capabilities due to manufacturers striving to deliver more features at lower costs, uninformed users can easily become exposed to various security and privacy attacks [1]. At the same time, a diversity of ambient devices, from personal assistants to smart home entertainment systems, can sense, process, and share increasingly more data about their users and environments [2]. Furthermore, the increasing accessibility of virtual and augmented reality (VR/AR) systems introduces specific risks for consumers of virtual content [3].

Although the scientific community has systematically uncovered and documented security and privacy threats *within* these individual areas of computing, recent advancements *at the intersection* of these areas present new challenges and give rise to new concerns. One example is the emergence of on-body interaction [6], on-body companion robots [7], and the integration between personal computing devices and the user's body [8], which enable the new experience of mediated embodiment [9], but also open up new possibilities for malicious actors to compromise

Workshop on Advances of Mobile and Wearable Biometrics at MobileHCI '23, the ACM International Conference on Mobile Human-Computer Interaction, Athens, Greece

radu.vatavu@usm.ro (R. Vatavu)

http://www.eed.usv.ro/~vatavu (R. Vatavu)

0000-0002-7631-6445 (R. Vatavu)

CEUR Workshop Proceedings (CEUR-WS.org)

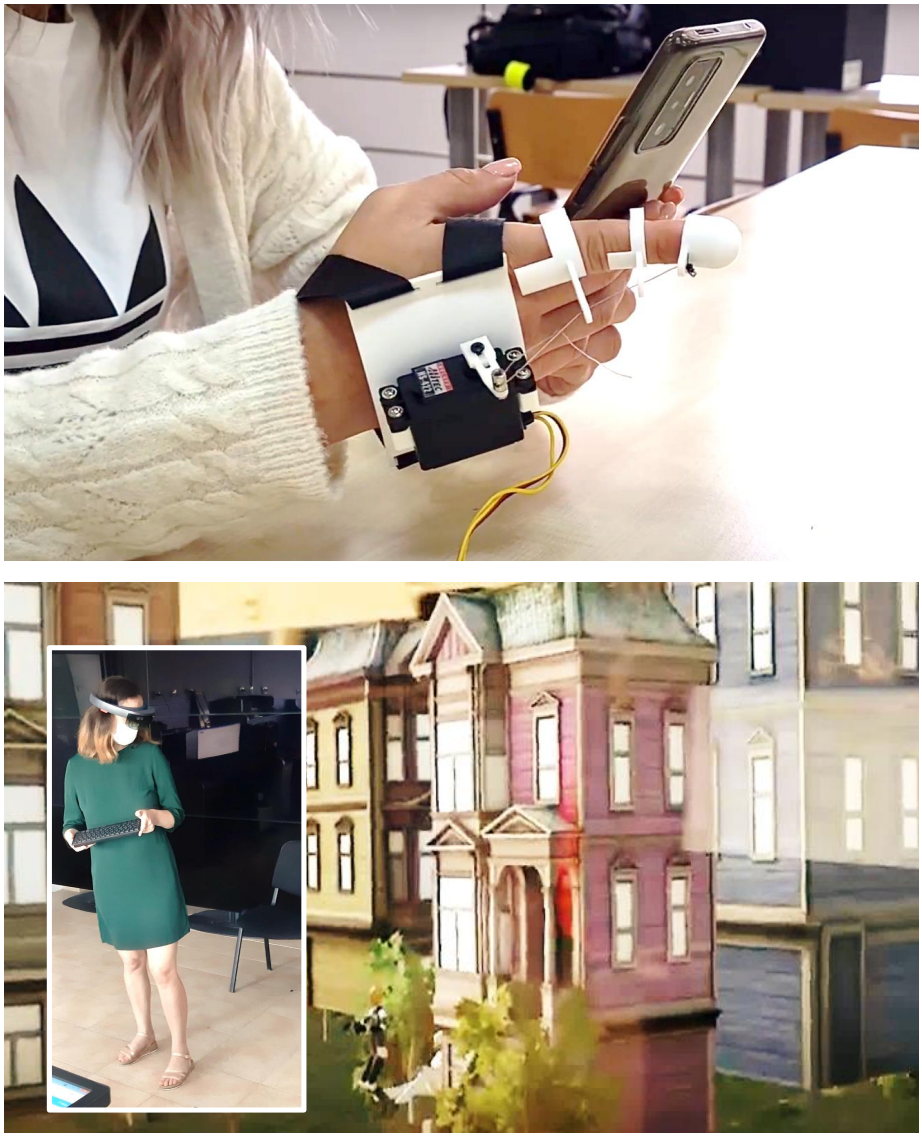

Figure 1: Fingerhinter [4] (top), a finger-augmentation wearable device designed for kinesthetic feedback, and ARTV journeys [5] (bottom), a HoloLens application for multi-perspective television watching in augmented reality. Wearable systems such as these, which are specifically designed to mediate user perception and action for new technology-mediated embodiment experiences, give raise to specific security and privacy risks that malicious actors could exploit.

users' security and privacy. For instance, Figure 1, top shows Fingerhinter [4], a device designed to deliver on-finger kinesthetic feedback, i.e., hyper-extensions of the index finger that signal various notifications to the user. By repurposing the user's body for output, Fingerhinter demands control over a body part with direct implication on the perceived sense of agency and bodily integration with technology. Potential attack risks in this context target *compromised dexterity, denial of movement,* and *physical harm* to the wearer and others. Figure 1, bottom

shows ARTV journeys [5], an AR system for television, where users can choose their preferred view of a movie rendered in a hybrid, physical-virtual environment, e.g., from a virtual screen resembling a conventional TV set to high immersion in the story of the movie displayed in the living room around the user. As users navigate through different representations of the same content, they willingly embrace mediation of their perception of the physical reality around them. Potential attacks for the ARTV journey system include *injection of malicious content* and *delivery of fake news,* both of which can have a detrimental impact on users' perception of the physical world around them.

2. Roadmap to Identifying Security and Privacy Threats of Ability-Mediating Wearables

We start our discussion from a set of threat categories that have been documented for wearables [1] and consumer VR systems [3]. Shrestha and Saxena [1] listed several security and privacy requirements for wearable computing systems. Security requirements include *confidentiality* (i.e., only authorized parties should be able to access data from the wearable), *integrity* (unauthorized parties should not be able to modify the data recorded by the wearable), *availability* (resistance against denial-of-service attacks), *authentication* (only the legitimate owner should be allowed to access the wearable), *access control* (use of data from wearables should be controlled via access policies), and *nonrepudiation* (the wearable cannot deny being the source of the data it generated). Privacy requirements refer to *device identification* (i.e., wearables should not be traced by unauthorized parties), *device log and measurement* (data logs from the wearable should not be accessible by unauthorized parties), and the *wearer* and *bystanders* (who should not be identified using the data from the wearable). Regarding consumer VR devices as a specific category of wearable systems, Casey et al. [3] identified several types of immersive attacks: the *chaperone attack* (i.e., modification of the virtual world boundaries), *overlay attack* (overlaying unwanted content on the user's view), *disorientation attack* (inducing dizziness or confusion experienced by the immersed user), and the *human joystick attack* (controlling the user's physical movement to a specific physical location without the user's knowledge).

This prior work also applies to wearable systems designed to mediate perception and/or motor action. However, there are specific risks that can be identified for these systems when *the attack targets a user's ability*, such as impairing vision or hindering dexterity. Unmasking such attacks needs a proper conceptual framework for perception and action-mediation systems. To this end, we propose several directions to guide future work in this area:

- Sensorimotor Realities (SRs) [10] are a recently introduced concept in the XR landscape that provides a technology-agnostic framework for computer-mediated perception and motor action. By building on the principle of mediation, SRs capitalize on the heterogeneity of human sensorimotor abilities to support conceptualization, characterization, and design of computer technology that leverages existing abilities in new, computer-mediated worlds. The SRs conceptual space consists of six dimension: *sensory mediation, motor mediation, virtuality, imaginarity, body augmentation,* and *environment augmentation.* For example, motor mediation specifies the effect that a device has on a specific motor ability, from *amplification* (to enhance an existing motor ability, e.g., lifting heavier objects

that normally possible) and *extension* (motor skills are enabled beyond the possibilities offered by one's anatomy, e.g., a sixth finger to grasp and hold large objects) to *diminution* (restriction of the limits of motor action) and *contraction* (refusal of a motor ability). Due to its specific focus on abilities and ability-mediating design [10], the SRs conceptual space may be used to identify relevant security and privacy threats that may lead to attacks targeting a specific sensorimotor ability.

- Vatavu [11] identified parallels between the foundational principles of ambient intelligence and AR systems, and reported a significant philosophical overlap between their visions: the concept of an environment that undergoes a form of *augmentation*, the process of an *integration* involving the environment, and the emergence of a *new type of media* congruent with the characteristics of the environment. These parallels identify key elements that may constitute the vehicles for potential attacks: alteration of the environment, the characteristics and implementation technology of the integration, and injection and overlay of attacker-generated media.
- Human-computer integration [8], the computing paradigm where humans and computers are closely interwoven, opens another direction for identifying risks of perception and motor-mediation wearables. The process of human-computer integration can be characterized as either *symbiosis* or *fusion* through the map of integration, a two-dimensional conceptual space with the *agency* axis (humans are in control, shared control, and device control) and the *integration scale* (organ, individual, and societal).

3. Conclusion

Understanding the new risks posed by wearable systems designed to mediate user perception and/or action requires careful consideration as we move towards unprecedented levels of immersive environments and integration between humans and computers. This process needs the use of appropriate conceptual frameworks, including technological ones [8, 10, 11] as proposed in this work, as well as cultural and philosophical frameworks [12] that provide a broader context. It is the author's hope that this position paper will inspire further investigations towards attack-resilient mediated embodiment.

Acknowledgments

This work was supported by a grant of the Ministry of Research, Innovation and Digitization, CNCS/CCCDI-UEFISCDI, project number PN-III-P4-ID-PCE-2020-0434 (PCE29/2021), within PNCDI III. The photographs from Figure 1 were made by Adrian-Vasile Catană (top) and Cristian Pamparău (bottom).

References

[1] P. Shrestha, N. Saxena, An offensive and defensive exposition of wearable computing, ACM Comput. Surv. 50 (2017). doi:10.1145/3133837.

[2] M. Friedewald, E. Vildjiounaite, Y. Punie, D. Wright, Privacy, identity and security in ambient intelligence: A scenario analysis, Telemat. Inf. 24 (2007) 15–29. doi:10.1016/j.tele.2005.12.005.

[3] P. Casey, I. Baggili, A. Yarramreddy, Immersive virtual reality attacks and the human joystick, IEEE Transactions on Dependable and Secure Computing 18 (2021) 550–562. doi:10.1109/TDSC.2019.2907942.

[4] A.-V. Catană, R.-D. Vatavu, Fingerhints: Understanding users' perceptions of and preferences for on-finger kinesthetic notifications, in: Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems, CHI '23, ACM, New York, NY, USA, 2023, pp. 518:1–17. doi:10.1145/3544548.3581022.

[5] C. Pamparău, R.-D. Vatavu, The user experience of journeys in the realm of augmented reality television, in: Proceedings of the ACM International Conference on Interactive Media Experiences, IMX '22, ACM, New York, NY, USA, 2022, p. 161–174. doi:10.1145/3505284.3529969.

[6] J. Bergström, K. Hornbæk, Human–computer interaction on the skin, ACM Comput. Surv. 52 (2019). doi:10.1145/3332166.

[7] H. Jiang, S. Lin, V. Prabakaran, M. R. Elara, L. Sun, A survey of users' expectations towards on-body companion robots, in: Proceedings of the 2019 on Designing Interactive Systems Conference, DIS '19, ACM, New York, NY, USA, 2019, p. 621–632. doi:10.1145/3322276.3322316.

[8] F. F. Mueller, P. Lopes, P. Strohmeier, W. Ju, C. Seim, M. Weigel, S. Nanayakkara, M. Obrist, Z. Li, J. Delfa, J. Nishida, E. M. Gerber, D. Svanaes, J. Grudin, S. Greuter, K. Kunze, T. Erickson, S. Greenspan, M. Inami, J. Marshall, H. Reiterer, K. Wolf, J. Meyer, T. Schiphorst, D. Wang, P. Maes, Next steps for human-computer integration, in: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, CHI '20, ACM, New York, NY, USA, 2020, p. 1–15. doi:10.1145/3313831.3376242.

[9] L. Aymerich-Franch, Is mediated embodiment the response to embodied cognition?, New Ideas in Psychology 50 (2018) 1–5. doi:10.1016/j.newideapsych.2018.02.003.

[10] R.-D. Vatavu, Sensorimotor realities: Formalizing ability-mediating design for computer-mediated reality environments, in: Proceedings of the IEEE International Symposium on Mixed and Augmented Reality, ISMAR '22, IEEE, USA, 2022, pp. 685–694. doi:10.1109/ISMAR55827.2022.00086.

[11] R.-D. Vatavu, Are ambient intelligence and augmented reality two sides of the same coin? implications for human-computer interaction, in: Extended Abstracts of the 2022 CHI Conference on Human Factors in Computing Systems, CHI EA '22, ACM, New York, NY, USA, 2022, pp. 362:1–8. doi:10.1145/3491101.3519710.

[12] B. Popoveniuc, R.-D. Vatavu, Transhumanism as a philosophical and cultural framework for extended reality applied to human augmentation, in: Proceedings of the 13th Augmented Human International Conference, AH '22, ACM, New York, NY, USA, 2022, pp. 6:1–8. doi:10.1145/3532525.3532528.