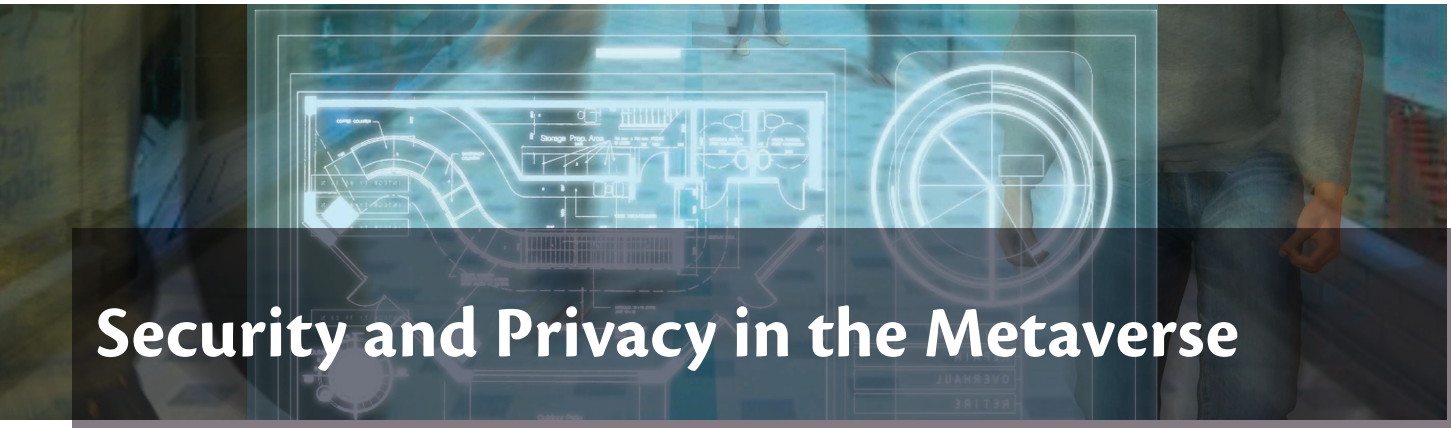

Security and Privacy in the Metaverse

Franziska Roesner and Tadayoshi Kohno | University of Washington

This special issue explores current and future security, privacy, and safety challenges that will arise with the increasingly widespread adoption of sensor-rich augmented, mixed, and virtual reality technologies that mediate users' perceptions of the physical world.

The "metaverse" is upon us: augmented (AR), mixed (MR), extended (XR), and/or virtual (VR) reality technologies are no longer future visions but have become commercially available, with significant investments and advancements from major technology companies in recent years. These technologies, including hardware, platforms, and applications, have the potential to fundamentally transform how people interact with the physical and digital worlds. However, as with any emerging technology, it is crucial that we anticipate and proactively address the potential security, privacy, and safety risks that will inevitably arise. This special issue explores these risks and how we might begin to address them.

These technologies, including hardware, platforms, and applications, have the potential to fundamentally transform how people interact with the physical and digital worlds.

For example, consider the serious privacy implications of MR headsets that capture rich sensor data about users, bystanders, and their physical surroundings. Compared even with smartphones, these sensor data are richer, more invasive (e.g., including eye tracking), and continuously collected and/or processed. Consider also the output created by these platforms and applications: virtual content that seamlessly integrates with a user's perception of the physical world. Buggy or malicious applications might create content that, for example, deceives users about the physical world or manipulates them physiologically, enabling a new class of perceptual manipulation attacks that exploit "vulnerabilities" in a person's brain.

When we first started our own work in the area of security and privacy for AR, with David Molnar (then at Microsoft Research) in 2011, our first (admittedly imperfect) article on the topic was rejected. We like to tell this story to students, to help illustrate how the topic of a rejected article in one decade can grow into a budding research area in the next. We offered more of our perspective on this emerging field in our 2021 retrospective.[1] We are thrilled to see increasing numbers

Digital Object Identifier 10.1109/MSEC.2023.3333989
Date of current version: 19 January 2024

of researchers and practitioners each year picking up the challenge and to have the opportunity to showcase some of this work in this special issue.

This special issue begins with an article by Cayir et al.[A1] in which the authors provide a broad assessment of the security and privacy risks faced by existing XR devices. Their analysis was informed through an extensive investigation of existing literature, as well as publicly available information about currently available XR devices. The authors consider both attacks and defenses, as well as future directions for the field. We encourage all readers interested in doing XR-related security and privacy work themselves to include this article as part of their initial reading list.

The next articles spotlight two different but equally important aspects of privacy: privacy for the user and privacy for bystanders. Modern and future XR devices can and will contain numerous sensors, sensors capable of both measuring properties of the user (e.g., the user's movement) *and* sensing the world. Nair et al.,[A2] in their article, offer both a rich exploration of how users' privacy might be compromised via data collected about their motion and a glimmer of hope through the exploration of methods to safeguard user privacy in a world of ubiquitous motion data collection. Examples of outward-facing sensors are cameras and microphones, which, if constantly sensing, have the potential impact the privacy of those in the user's vicinity. Corbett et al.,[A3] in their article, provide an in-depth discussion of the so-called "bystander privacy problem," offering as a case study Google Glass and providing guidance on how to protect bystander privacy in the future.

The next two articles turn to specific application areas. The first application area is online advertising. The second is future VR classrooms. These two application areas present a fascinating dichotomy. The first (advertising) is often viewed as an adversarial technology by the computer security community, whereas the latter is not. Advertising in VR is not a hypothetical. As Mhaidli et al.[A4] discuss in their article, companies are, today, increasingly using VR for advertising. In their article, they provide an analysis of current VR marketing experiences, identify existing risks to users, and extrapolate to identify potential future risks. The authors then provide broad guidance to researchers, industry practitioners, and regulators on how to mitigate risks with VR advertising. Brehm and Shvartzshnaider,[A5] in their article, consider privacy in VR classrooms, including the privacy violations that users might encounter as well as a contextual integrity-based framework for mitigating privacy risks.

Finally, our special issue includes a viewpoint article by O'Hagan et al.[A6] In this article, the authors look ahead to a future in which AR technologies have been widely adopted and integrated into the daily lives of many people. In that context, they explore the societal challenges and harms raised by AR's ability to modify our perception of the physical world. Toward addressing these risks, the authors raise the question of whether we will need "perceptual human rights" and explore what these might look like.

Stepping back, while we cannot predict with certainty when and how the "metaverse" will be integrated into the daily lives of end users the way that smartphones are now, we know a change is coming that will continue to transform our interactions with the increasingly integrated physical and digital worlds and with each other. It is our collective responsibility to help ensure that this future is a positive one, where the security, privacy, and safety of all stakeholders are protected. We hope that the articles in this special issue can help move us toward that future and can help inspire others to join us in this vision.

Finally, we would like to express our gratitude to all of the people who helped make this special issue possible: the authors who submitted their articles, the generous reviewers who provided essential input to our final selections, and the *IEEE Security & Privacy* editors and staff, especially Editor in Chief Sean Peisert and Associate Editor in Chief Mary Ellen Zurko, who oversaw the process for this special issue. Our reviewers included Kevin R.B. Butler, Rahul Chatterjee, Kaiming Cheng, Pardis Emami-Naeini, Earlence Fernandes, Alisa Frik, Uwe Gruenefeld, Weijia He, Diane Hosfelt, Umar Iqbal, Eakta Jain, Apu Kapadia, Mohamed Khamis, Tianshi Li, Jingjie Li, David Lindlbauer, Blair MacIntyre, Florian Mathis, Michael Nebeling, Amir Rahmati, Kimberly Ruth, R. Benjamin Shapiro, Yuan Tian, Yukang Yan, and Eric Zeng. Thank you! ■

Appendix: Related Articles

A1. D. Cayir, A. Acar, R. Lazzeretti, M. Angelini, M. Conti, and S. Uluagac, "Augmenting security and privacy in the virtual realm: An analysis of extended reality devices," *IEEE Security Privacy*, vol. 22, no. 1, pp. 10–23, Jan./Feb. 2024, doi: 10.1109/MSEC.2023.3332004.

A2. V. Nair, L. Rosenberg, J. F. O'Brien, and D. Song, "Truth in motion: The unprecedented risks and opportunities of extended reality motion data," *IEEE Security Privacy,* vol. 22, no. 1, pp. 24–32, Jan./Feb. 2024, doi: 10.1109/MSEC.2023.3330392.

A3. M. Corbett, B. David-John, J. Shang, Y. Charlie Hu, and B. Ji, "Securing bystander privacy in mixed reality while protecting the user experience," *IEEE Security Privacy*, vol. 22, no. 1, pp. 33–42, Jan./Feb. 2024, doi: 10.1109/MSEC.2023.3331649

A4. A. Mhaidli, S. Rajaram, S. Fidan, G. Herakovic, and F. Schaub, "Shockvertising, malware, and a lack of

accountability: Exploring consumer risks of virtual reality advertisements and marketing experiences," *IEEE Security Privacy*, vol. 22, no. 1, pp. 43–52, Jan./Feb. 2024, doi: 10.1109/MSEC.2023.3332105.

A5. K. Brehm and Y. Shvartzshnaider, "Understanding privacy in virtual reality classrooms: A contextual integrity perspective," *IEEE Security Privacy,* vol. 22, no. 1, pp. 53–62, Jan./Feb. 2024, doi: 10.1109/MSEC.2023.3336802.

A6. J. O'Hagan, J. Gugenheimer, F. Mathis, J. Bonner, R. Jones, and M. McGill, "A viewpoint on the societal impact of everyday augmented reality and the need for perceptual human rights," *IEEE Security Privacy*, vol. 22, no. 1, pp. 64–68, Jan./Feb. 2024, doi: 10.1109/MSEC.2023.3333988.

Reference

1. F. Roesner and T. Kohno, "Security and privacy for augmented reality: Our 10-year retrospective," in *Proc. 1st Int. Workshop Secur. XR XR Secur. (VR4Sec)*, Aug. 2021, pp. 1–5. [Online]. Available: https://ar-sec.cs.washington.edu/files/ARSec-10YearRetrospective.pdf

Franziska Roesner is an associate professor in the Paul G. Allen School of Computer Science and Engineering at the University of Washington, Seattle, WA 98195 USA. Her research interests include computer security and privacy for end users of existing and emerging technologies, and AR security. Roesner received a Ph.D. in computer science and engineering from the Univeristy of Washington. She is a Member of IEEE. Contact her at franzi@cs.washington.edu.

Tadayoshi Kohno is a professor in the Paul G. Allen School of Computer Science and Engineering at the University of Washington, Seattle, WA 98195 USA. His research interests include helping protect the security, privacy, and safety of users of current- and future-generation technologies, including AR technologies. Kohno received a Ph.D. in computer science from the University of California. He is a Fellow of IEEE. Contact him at yoshi@cs.washington.edu.

Digital Object Identifier 10.1109/MSEC.2023.3343885