Understanding the Privacy Dimension of Wearables through Machine Learning-enabled Inferences

David Mohaisen
mohaisen@ucf.edu
University of Central Florida
Orlando, Florida, USA

ABSTRACT

To keep up with the ever-growing user expectations, manufacturers and developers keep adding new features, including input/output (I/O) interfaces, to augment the use cases of wearable technologies, such as fitness trackers, augmented reality head-mounted devices (AR HMDs), and smart watches, without considering their security and privacy implications. In this talk, we will discuss some of our recent results on understanding the privacy dimension of wearable technologies through inference attacks facilitated by advances in machine learning. Our attacks target unconventional and new I/O mechanisms that allow an adversary to breach application-specific features. First, we will present an exploration of the attack surface introduced by fitness trackers [1, 4]. We propose an inference attack that breaches location privacy through the elevation profiles collected by fitness trackers. Our attack highlights that adversaries can infer the location from elevation profiles collected via fitness trackers. Second, we will review the attack surface introduced by smartwatches [5]. For that, we develop an inference attack that exploits the smartwatch microphone to capture the acoustic emanations of physical keyboards and successfully infers what the user has been typing. Third, we will present an exploration of AR HMDs security [2, 3, 6]. We design an inference attack that exploits the geometric projection of hand movements in the air. The attack framework predicts the typed text on an in-air tapping keyboard, which is only visible to the user. We will conclude with lessons learned, defense directions, and open research directions.

Wearable	Exploited Feature	Technique	Outcome
Fitness Tracker	Elevation Profiles	Representation	Location Breach
Smartwatch	Acoustics	Modeling	Keylogging
AR HMD	Geometric Projections	Mapping	Keylogging

Table 1: An overview of our explorations highlighting the targeted devices, exploited features, techniques, and outcomes.

CCS CONCEPTS

• **Security and privacy → Privacy protections**; **Mobile and wireless security**.

KEYWORDS

wearables, augmented reality, inference, privacy, machine learning

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).
SNTA '23, June 20, 2023, Orlando, FL, USA
© 2023 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-0165-8/23/06.
https://doi.org/10.1145/3589012.3594896

ACM Reference Format:
David Mohaisen. 2023. Understanding the Privacy Dimension of Wearables through Machine Learning-enabled Inferences . In *Proceedings of the 2023 Systems and Network Telemetry and Analytics (SNTA '23), June 20, 2023, Orlando, FL, USA.* ACM, New York, NY, USA, 1 page. https://doi.org/10.1145/3589012.3594896

BIOGRAPHY

David Mohaisen obtained his Ph.D. from the University of Minnesota in 2012. He is a Full Professor of Computer Science at the University of Central Florida, where he has been since 2017. Previously, he was an Assistant Professor at SUNY Buffalo, a Senior Scientist at Verisign Labs, and a researcher at ETRI. His research interests are in applied security and privacy, covering networked systems, software systems, IoT and AR/VR, machine learning, and blockchain systems. His research has been supported by several generous grants from NSF, NRF, AFRL, AFOSR, etc., and has been published in top conferences and journals, with multiple best paper awards. His work was featured in multiple outlets, including The New Scientist, MIT Technology Review, ACM Tech News, Science Daily, etc. Among other services, he is currently an Associate Editor of IEEE Transactions on Dependable and Secure Computing and served as an Associate Editor of IEEE Transactions on Mobile Computing, IEEE Transactions on Parallel and Distributed Systems, and IEEE Transactions on Cloud Computing. He is a senior member of ACM (2018) and IEEE (2015), a Distinguished Speaker of the ACM, and a Distinguished Visitor of the IEEE Computer Society.

REFERENCES

[1] Ülkü Meteriz, Necip Fazil Yildiran, Joongheon Kim, and David Mohaisen. 2020. Understanding the Potential Risks of Sharing Elevation Information on Fitness Applications. In *IEEE International Conference on Distributed Computing Systems, ICDCS*. IEEE, Singapore, 464–473. https://doi.org/10.1109/ICDCS47774.2020.00063

[2] Ülkü Meteriz-Yidiran, Necip Fazil Yildiran, and David Mohaisen. 2022. AcousticType: Smartwatch-Enabled Cross-Device Text Entry Method Using Keyboard Acoustics. In *ACM CHI Extended Abstracts*. ACM, New Orleans, LA, USA, 352:1–352:7. https://doi.org/10.1145/3491101.3519691

[3] Ülkü Meteriz-Yildiran, Necip Fazil Yildiran, Amro Awad, and David Mohaisen. 2022. A Keylogging Inference Attack on Air-Tapping Keyboards in Virtual Environments. In *IEEE Conference on Virtual Reality and 3D User Interfaces, VR*. IEEE, Christchurch, New Zealand, 765–774. https://doi.org/10.1109/VR51125.2022.00098

[4] Ülkü Meteriz-Yildiran, Necip Fazil Yildiran, Joongheon Kim, and David Mohaisen. 2023. Learning Location from Shared Elevation Profiles in Fitness Apps: A Privacy Perspective. *IEEE Transactions on Mobile Computing* 2023, 1 (2023), 1–16. https://doi.org/10.1109/TMC.2022.3218148

[5] Ülkü Meteriz-Yildiran, Necip Fazil Yildiran, and David Mohaisen. 2021. SIA: Smartwatch-Enabled Inference Attacks on Physical Keyboards Using Acoustic Signals. In *ACM Workshop on Workshop on Privacy in the Electronic Society, WPES*. ACM, Seoul, South Korea, 209–221. https://doi.org/10.1145/3463676.3485607

[6] Necip Fazil Yildiran, Ülkü Meteriz-Yildiran, and David Mohaisen. 2022. AiRType: An Air-tapping Keyboard for Augmented Reality Environments. In *2022 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops, VR Workshops*. IEEE, Christchurch, New Zealand, 676–677. https://doi.org/10.1109/VRW55335.2022.00189