WEARABLE ACTIVITY TRACKERS AND PRIVACY: ASSESSMENT OF THE RISKS, THREATS, AND COUNTERMEASURES

Thesis summary – Noé ZUFFEREY

HEC Lausanne / octobre - 2023

Wearable devices, such as wearable activity trackers (WATs), are increasing in popularity.
Although they can help improve a person's quality of life, they also raise serious privacy issues. Although security aspects of WATs have been widely studied (e.g., Bluetooth security, inference of password or biometrics), as well as privacy-related aspects such as users' attitudes and concerns, we lack knowledge about the privacy of WAT users. Indeed, the security aspects that were studied in prior work are not enough to build a realistic adversary model, as these studies focus mostly on communication protocols and not on large-scale data collection. Furthermore, previous work related to data inference by using WATs focuses on only functionalities rather than on privacy (e.g., better monitoring of activity or health to improve user experience). Moreover, these studies focus only on the inference of behavioral patterns (e.g., activities, consumption) or conditions (e.g., diseases), but none of them investigate the inference of users' personal attributes (e.g., personality, religion, political views).

In this thesis, composed of three research papers and a literature review, we contribute to the WAT security \& privacy research field by analyzing how the data of WAT users can be accessed at a large scale by many potential adversaries, by evaluating how such data can be used to infer users' personal attributes and, finally, by proposing privacy enhancing technologies (PETs) to protect their privacy. Concretely, after analyzing the current literature about WAT security \& privacy, we conduct a user-survey study to better understand the WAT user's behaviors towards data sharing, especially with respect to third-party applications (TPAs) that can easily be used by adversaries to collect data. We then use a rigorous machine-learning approach to evaluate to what extent users' psychological profiles (Big 5) can be inferred from WAT data, and we discuss the related consequences on the users' privacy and society as a whole. Finally, to propose effective and likely-to-be-adopted protection mechanisms, we conduct a user-centered design study by using a participatory design methodology before analyzing and evaluating the proposed designs in order.

Les technologies portables, tels que les montres connectées ou traqueurs d'activité, sont de plus en plus populaires. Bien qu'elles puissent contribuer à améliorer la qualité de vie des utilisateur·trice·s, elles peuvent également causer de graves problèmes de protection de la vie privée. Bien que les aspects liés à la sécurité des traqueurs d'activité aient été largement étudiés (par exemple, la sécurité Bluetooth, ou l'inférence de mots de passe ou de données biométriques), ainsi que les aspects liés à la vie privée tels que les attitudes et les préoccupations des utilisateur·trice·s, nous manquons de connaissances sur la protection des données personnelles. En effet, les aspects liés à la sécurité qui ont été étudiés précédemment ne sont pas suffisants pour construire un modèle d'adversaire réaliste, la recherche s'est alors principalement concentrée sur les protocoles de communication et non sur la collecte de données à grande échelle. En outre, les travaux antérieurs relatifs à l'inférence de données à l'aide de traqueurs d'activité se concentrent uniquement sur les fonctionnalités et non sur la vie privée (par exemple, un meilleur suivi de leurs activités ou de leur santé afin d'améliorer l'expérience de l'utilisateur·trice). De plus, ces études se concentrent uniquement sur l'inférence de données comportementales (par exemple, activités, consommation) ou de conditions (par exemple, maladies), mais aucune d'entre elles ne porte sur l'inférence des attributs personnels des utilisateur·trice·s (par exemple, personnalité, religion, opinions politiques).

Dans cette thèse, composée de trois articles de recherche ainsi que d'une revue de la littérature, nous contribuons au domaine de recherche sur la sécurité de l'information relative aux traqueurs d'activité en analysant comment les données des utilisateur·trice·s peuvent être accessibles à grande échelle pour de

UNIL | Université de Lausanne
HEC Lausanne

nombreux adversaires potentiels, et comment ces données peuvent être utilisées pour inférer des données personnelles et sensibles des utilisateur·trice·s, ainsi qu'en proposant des technologies d'amélioration de la vie privée. Concrètement, après avoir analysé la littérature actuelle sur la sécurité des traqueurs d'activité et la protection de la vie privée, nous présentons une étude menée auprès des utilisateur·trice·s pour mieux comprendre leur comportement vis-à-vis du partage des données, en particulier en ce qui concerne les applications tierces qui peuvent facilement être utilisées par des adversaires pour collecter des données personnelles. Nous utilisons ensuite une approche rigoureuse de *machine learning* pour évaluer dans quelle mesure les profils psychologiques des utilisateur·trice·s (Big 5) peuvent être inférés à partir des données issues de traqueurs d'activité, et nous discutons des conséquences relatives à la vie privée des utilisateur·tirce·s et à la société dans son ensemble. Enfin, pour proposer des mécanismes de protection efficaces et susceptibles d'être adoptés, nous présentons une étude de conception centrée sur l'utilisateur·trice menée en utilisant une méthodologie participative avant d'analyser et d'évaluer différentes solutions conceptualisées par les utilisateur·trice·s mêmes.