Time Is Running Out

Assessing Temporal Privacy of Privacy Zones in Fitness Tracking Social Networks

Deleu, Wout
KU Leuven, Campus Rabot
Ghent, Belgium

***Abstract*—In a society where social media is so ubiquitous, the privacy concerns around them are more relevant than ever. During this article, the main focus will be on the privacy policies of fitness trackers. Fitness trackers are platforms which store and display data related to sport activities. These can be shared with other users. This data may include heart rate, GPS-locations, etc. This type of data sharing can however cause unintentionally sharing of sensitive information, like home addresses.**

Most fitness tracking networks are aware of this danger and implement a series of countermeasures to prevent this. One of these countermeasures is the use of Endpoint Privacy Zones (EPZs) which is a zone around a sensitive location, which hides the part of the trajectory which ends or begins in this zone. Previous research has shown that it is possible to retrieve the sensitive location using the available data from the activity. Dhondt et al. showed that based on the total distance travelled, the sensitive location can be retrieved using an 'inference attack' [1]. This study will investigate the possibilities of such inference attacks using other data than the distance. We want to recreate the results as good as possible using the speed and tempo of the activity, together with GPS-locations. This can result in an attack model with a success rate up to 75%. This is lower than the previous implementation of Dhondt et al., but this shows that the attack is still possible under circumstances where the distance is rendered unusable. This also includes some countermeasure described by Dhondt et al. But countermeasures like enlarging the EPZ or shifting endpoints still have effect.

Keywords: fitness-trackers, privacy, gps-locations, endpoint privacy zone, inference attack

I. Introduction

References

[1] K. Dhondt, V. Le Pochat, A. Voulimeneas, W. Joosen, and S. Volckaert, "A run a day won't keep the hacker away: Inference attacks on endpoint privacy zones in fitness tracking social networks," osf.io/3m5ut, Nov 2022.