Privacy-friendly User Location Tracking with Smart Devices: The BeaT Prototype

Jan H. Betzing[1], Marco Niemann[1], and C. Ingo Berendes[2]

[1] University of Münster, ERCIS, Münster, Germany
{jan.betzing|marco.niemann}@ercis.de
[2] Paderborn University, Paderborn, Germany
Ingo.berendes@upb.de

Abstract. Customers use smart devices to share their location data with service providers to co-create personalized, location-based services. However, mobile apps that record movement profiles not only yield value-added service but also bear potential for abuse. Especially apps utilizing GPS-based tracking pose a privacy risk because they could–once enabled–unnoticeably record data in private situations. In response, we developed a privacy-friendly solution, called *BeaT*, that tracks user locations without GPS and gives users full control over the time and scope of data collection. We leverage Bluetooth Beacon technology to confine the perimeter in which tracking takes place. This paper presents the requirements, algorithmic design, prototypical implementation, real-world use case, and evaluation setting for BeaT.

Keywords: User Location Tracking, Location-based Service, Privacy, Smart Device, Bluetooth Low Energy Beacon

Video: https://www.smartmarketsquare.de/tracking-with-beat

1 User Location Tracking–Friend or Foe?

Navigating by smart device or tracking a run in a fitness app are exemplary location-based services (LBS) where users share their location with service providers [1]. Even though service providers are limited in data exploration by data-protection regulations (e.g., required user consent and opt-in to data sharing), privacy risks and potentials for abuse remain [2,3]. Notably, once a mobile app has been granted permanent access to the GPS sensor, it can access the user's location even in private situations. As seen in the case of the fitness-tracking app Strava, unrestricted user tracking can–in the worst case–expose classified information such as the location of secret US military bases [4].

In response, this paper presents *BeaT, a privacy-friendly user location tracking mechanism for smart devices*, and its application in the smartmarket² research project, in which the authors developed a LBS for high street customers to track their shopping trips [see 3,5]. In addition to retail, BeaT can also be applied in other sectors such as healthcare or hospitality management to track time-logical user movement sequences.

14th International Conference on Wirtschaftsinformatik,
February 24-27, 2019, Siegen, Germany

Motivated by the disadvantages of existing solutions, we state the requirements for BeaT as follows: First, to prevent tracking in private situations, the solution must not use satellite or WiFi-based geolocation or access acoustic and visual sensors (R1). Additionally, the tracking perimeter should be defined ex-ante (R2). Second, while GPS only supports outdoor tracking, we want to track both indoor and outdoor locations (R3). Third, some LBS such as Foursquare use check-ins, i.e., users manually record the places they are visiting [1]. While this mechanism accounts for user control, it lacks convenience. Consequently, our solution should provide automatic tracking (R4) while retaining users' full control regarding the time and scope of data collection (R5). Fourth, users associate LBS such as navigation or AR games (e.g., Pokémon Go) with battery drain [6]. Our solution should limit mobile resource utilization regarding processing power, memory, (mobile) data, and battery to foster user acceptance (R6).

2 Prototypical Design and Implementation

2.1 Technology Selection and Setting

We selected Bluetooth Low Energy (BLE) beacons as the underlying tracking technology because (1) smart devices support the technology for a few years [7]; (2) beacons do not reach into private spaces (R1) as they have to be actively deployed in the perimeter within which tracking should commence (R2); (3) the BLE protocol has low mobile resource utilization (R6); and (4) beacons allow for both indoor and outdoor tracking (R3). Beacons are small low-range radio-frequency transmitters that frequently broadcast a predefined payload, consisting of a Universally Unique Identifier (UUID) and two alphanumeric values called major and minor [7]. Nearby devices can receive the signal, calculate their proximity to the beacon, and reason upon the payload [3].

In the smartmarket² case, customers can record their journey across multiple retailers that are geographically dispersed along the high street [5,8]. In return for their data, customers receive personalized offers from nearby stores. Beacon major values identify the store whereas beacon minor values indicate the purpose and location of a beacon (outside at an entrance, inside at a PoI, inside at a PoS) [3]. These purposes allow to distinguish customers passing by, entering a store, traversing a Point of Interest (PoI) such as a promotional display within a store, and visiting a Point of Sale (PoS). Additionally, a back-end database server holds the geocoordinates of each beacon.

Customers use a mobile app to record their shopping trips. On the first start, the app requests access to the Bluetooth sensor. Once granted, the device is able to listen continuously for beacon signals. However, smartmarket² is deployed individually for each high street to fulfill R2. Hence, the app only declares a single UUID to monitor. Given that 2^{122} UUID exist [7], it is unlikely to receive a matching beacon signal outside the predefined area. Concerning R4 and R5, smart devices can receive beacon signals automatically in the background, but customers have to actively start and stop tracking in the app before any signal is sensed. Additionally, the app lists active and past trips and allows to inspect and delete the collected information (R5). Lastly, current mobile OS indicate active Beacon tracking and inform users on continuous monitoring.

When the user starts tracking and relevant beacons are in range, the app receives a list of these beacons and their coarse distance (far, near, immediate) once every second. A naïve approach is to record this data entirely and transmit it to the back-end server. As this would pose substantial resource utilization and violate R6, we developed a solution to extract and send only relevant information from the raw data stream–BeaT.

2.2 The BEAcon Tracking (BeaT) Algorithm

Suppose we have an active trip `tr`, a set of recently seen majors `M` (representing stores), and a set of beacon sightings, henceforth called touches `T`. For each touch `t`, we call the procedure BEAT, given in Algorithm 1, to update customer journey information.

Input: $(tr, M, t \in T)$ ▷ tr is the current trip; M is a set of active majors; t is a newly received beacon touch

1: **procedure** BEAT
2: $te \leftarrow$ GETBYMAJOR($t.major$) ▷ Try to obtain a trip entry te based on the major of touch t
3: **if** te != none **and** DIFF($te.end$, $t.time$) $<$ 10 min **then**
4: $tr.end \leftarrow t.time$ ▷ Earmark current t as potential last $t \in tr$
5: $te.end \leftarrow t.time$ ▷ Earmark current t as potential last $t \in te$
6: **switch** $t.type$ **do**
7: **case** "entrance"
8: **if** $te.entrance\_first$ == none **then** $te.entrance\_first \leftarrow t$
9: **if** $t.dist$ == "immediate" **then** $te.visited \leftarrow$ true ▷ Mark te (store) as visited
10: $te.entrance\_last \leftarrow t$ ▷ Earmark t as potential last sighting
11: **case** "PoI"
12: **if** t.dist != "far" **then**
13: te.visited $\leftarrow$ true ▷ Mark te (store) as visited
14: **if** t $\notin te.poi$ **then** SENDTODB(t) ▷ Send PoI touch t to the database server on first sight
15: $te.poi \leftarrow te.poi \cup t$ ▷ Add t to the set $te.poi$ of seen PoI
16: **case** "PoS"
17: **if** t.dist != "far" **then** te.visited $\leftarrow$ true ▷ Mark te (store) as visited
18: **if** t.dist == "immediate" **then**
19: **if** $te.pos\_first$ == none **then** $te.pos\_first \leftarrow t$
20: $te.pos\_last \leftarrow t$ ▷ Earmark t as potential last sighting
21: **if** DIFF($te.pos\_first$, $te.pos\_last$) $>$ 30 sec **then** $te.sale \leftarrow$ true
22: **else**
23: ENDEXPIREDTRIPENTRIES() ▷ End expired te and remove respective $te.major$ from M
24: $te \leftarrow$ CREATETRIPENTRY(t) ▷ Create new trip entry te based on touch t
25: $M \leftarrow M \cup t.major$ ▷ Add $t.major$ to active majors M
26: $tr.te \leftarrow tr.te \cup te$ ▷ Add te to current trip tr
27: BEAT(t) ▷ Execute BEAT again, having a te

Algorithm 1. BeaT

First we test, whether there was an interaction with this store (`t.major`) within the last ten minutes. If not, we create a new trip entry `te`, which represents one element in the customer journey, and add it to the trip `tr`. Also, inactive trip entries for stores that have not been seen in the last ten minutes are closed and their respective majors are removed from the set `M` of currently active majors. Depending on the type of touch (`t.type`) and the user's distance to the beacon (`t.dist`), the trip entry is updated. In effect, we store for each trip entry, when the store was first and last seen (`entrance_first|_last`), if the customer has entered the store (`visited`), a set of seen PoI, and if the customer has bought something (`sale`). The latter is approximated by testing, if the customer has been in immediate proximity to a PoS for

at least 30 seconds. PoI sightings are directly transmitted to the back-end server so that it can potentially return relevant notifications for the user. Each trip is either terminated in-app by the user or by a timed function that closes a trip after three hours without beacon sightings. The trip `tr` and all associated `te` and `t` are transmitted to the back-end server en bloc and tracking is disabled.

3 Evaluation and Outlook

BeaT was added to the prototypical smartmarket² platform [5], which provides the socio-technical context to investigate user location tracking in the target high street environment. BeaT is the result of multiple cycles of building, testing and evaluation activities. We already asserted the general viability of beacon tracking in an artificial setting [3]. Advancing further along the continuum of Venable et al.'s *Human Risk & Effectiveness Strategy* [9] to evaluate IT artifacts, we will conduct a summative naturalistic evaluation in the fourth quarter of 2018. About 40 businesses in a German high street will install beacons and we invited about 400 high street customers to engage in customer journey tracking using BeaT over the course of two months. Besides judging how well BeaT achieves its envisioned environmental utility [9], we also designed our field test to shed light on the socio-technical issues of adoption and use of privacy-friendly LBS, which will subsequently yield additions to the knowledge base.

Large facilities such as hospitals, shopping malls, and airports already use BLE beacons to provide indoor navigation [7]. Besides its merits for high streets, BeaT could also constitute a viable extension to existing mobile service in these domains. For example, in hospitals, patients could use BeaT to record which doctors and wards (service providers) they have visited and–based on their current patient journey–receive further digital and personal service. Lastly, in future research, we will use the location data collected through BeaT to map, analyze, and predict customer journeys [8].

Acknowledgements

The authors thank the following undergraduate students from the University of Münster, who helped with designing and implementing the BeaT algorithm: Tim Hummelt, Leon Papke, David Pucka, Cedric Pumpe, Lennart Schäpermeier, and Pia Vollmer. This paper was developed in the research project smartmarket² (www.smartmarketsquare.de), which is funded by the German Federal Ministry of Education and Research (BMBF), promotion signs 02K15A073-02K15A074. The authors thank the Project Management Agency Karlsruhe (PTKA).

References

1. Dhar, S., Varshney, U.: Challenges and business models for mobile location-based services and advertising. Communications of the ACM 54(5), 121–129 (2011)
2. Schaub, F., Balebako, R., Durity, A.L., Cranor, L.F.: A Design Space for Effective Privacy Notices. In: Proceedings of the 11th Symposium on Usable Privacy and Security. pp. 1–17. SOUPS '15 (2015)
3. Betzing, J.H.: Beacon-based Customer Tracking across the High Street: Perspectives for Location-based Smart Services in Retail. In: 24th Americas Conference on Information Systems. AMCIS '18, New Orleans, LA, US (2018)
4. Woollacott, E.: Pentagon Bans GPS Fitness Apps, Says They're 'Significant Risk' To Troops. Forbes (aug 2018), https://www.forbes.com/sites/emmawoollacott/2018/08/07/pentagon-bans-gps-fitness-apps-says-theyre-significant-risk-to-troops/, last accessed: 2018-11-12
5. Bartelheimer, C., Betzing, J.H., Berendes, I., Beverungen, D.: Designing Multi-sided Community Platforms for Local High Street Retail. In: 26th European Conference on Information Systems. ECIS '18, Portsmouth, UK (2018)
6. Faragher, R., Harle, R.: Location Fingerprinting with Bluetooth Low Energy Beacons. IEEE Journal on Selected Areas in Communications 33(11), 2418–2428 (2015)
7. Statler, S.: Beacon Technologies. Apress, Berkeley, CA (2016)
8. Berendes, I., Bartelheimer, C., Betzing, J.H., Beverungen, D.: Data-driven Customer Journey Mapping in Local High Streets: A Domain-specific Modeling Language. In: 39th International Conference on Information Systems. ICIS '18, San Francisco, CA, USA (2018)
9. Venable, J., Pries-Heje, J., Baskerville, R.: FEDS: a Framework for Evaluation in Design Science Research. European Journal of Information Systems 25(1), 77–89 (2016)