Delphine Christin: *Impenetrable Obscurity vs. Informed Decisions: Privacy Solutions for Participatory Sensing*. In: Proceedings of the 8th International Conference on Pervasive Computing and Communications (PerCom), pp. 847-848, 2010.

Impenetrable Obscurity vs. Informed Decisions: Privacy Solutions for Participatory Sensing

Delphine Christin
Secure Mobile Networking Lab, Technische Universität Darmstadt, Mornewegstr. 32, 64293 Darmstadt, Germany
delphine.christin@seemoo.tu-darmstadt.de

***Abstract*—By harnessing sensors embedded in personal end devices, Participatory Sensing enables novel applications, but also raises severe privacy concerns. Instead of using existing centralized privacy mechanisms that remain obscure to the participants, we propose to involve the participants themselves into the process to protect privacy by interacting directly with others users using their available sensors. Furthermore, our decentralized solution helps in limiting the dissemination of sensitive data, which eliminates some threats to privacy.**

I. Introduction and Motivation

The sensing process in wireless sensor networks is no more limited to only dedicated sensor platforms, but also includes sensors such as accelerometers or microphones embedded in personal end devices. Designated as "Participatory Sensing", the utilization of these embedded sensors allows taking advantage of an already existing sensor deployment, i.e., utilizing millions of smartphones without requiring additional hardware investments. In addition to improving the sensing process for existing scenarios, such deployments open the door to innovative applications that remain impractical with dedicated sensor platforms. However, the exploitation of sensor data gathered by personal end devices endangers the private sphere of the participants. To encourage participation and improve the relevance of the results, mechanisms protecting the users' privacy are therefore mandatory. Privacy in Participatory Sensing centers on two tightly coupled components: people and data. Participants have to understand, choose and control the disclosure of data gathered during the sensing process, and as well select data recipients and duration of data availability [1].

In the existing solutions, the human-centric aspect is often neglected, as the privacy mechanisms are exclusively managed by the infrastructure and kept hidden from the users. If they exist, privacy policies are often only laid out in technical terms. Users are not aware of the tremendous implications it might have if their data is e.g. stored for indefinite time. Also, the selection and control of the privacy settings is not in the center of attention of existing solutions. Nevertheless, aspects of privacy depend on individuals and are difficult to capture with purely technology-based solutions. Interventions of the participants are therefore required to tune the parameters according to their preferences. Consequently, the obscurity surrounding privacy mechanisms in Participatory Sensing needs to be addressed.

Within the scope of this extended abstract, we consider two application scenarios and examine how the understanding of privacy and its control are supported. We then present our concept and give an outline of the future work before drawing conclusions.

II. Related Work

Depending on the application scenarios, different dimensions, such as location or personal data, need to be protected against privacy violations. Scenarios carrying out analyses of transportation traffic patterns [2] mainly require mechanisms to protect the participants' location, whereas health-related applications like AndWellness [3] mandate additional privacy mechanisms, because critical information, such as the current activity of users, is monitored. AnonySense [4] is one example of an architecture that ensures location privacy. By replacing precise position coordinates by the identifier of the surrounding area, attackers are unable to distinguish and localize users within this defined area. However, the location privacy is efficiently preserved, the proposed mechanism relies mainly on a centralized infrastructure. With a single point of failure, such architectures are vulnerable because malfunctions and malicious attacks directed against the central entity can reveal or damage the entire data storage. Moreover, sensitive data are first transferred to the central entity that anonymizes them afterwards. Private data are accessible by the campaign organization and the privacy policies are entrusted to the infrastructure, so the users have no possibility to completely withdraw their data once they were uploaded. Still under development, the AndWellness project proposes an approach to solve this issue by allowing users to modify, hide or delete data before being uploaded. With users participating actively to the privacy process, this approach is the closest to our concept. However, the proposed solution is also based on a central architecture that may encounter the aforementioned problems.

III. Informed Decisions in Participatory Sensing

Our concept includes two main dimensions: awareness of participants that actively take part in the privacy process, and the construction of a decentralized "web of trust", as basis for additional security mechanisms. The goal of the

first dimension is to increase the consciousness of the users concerning privacy issues, like the Privacy Bird [5] symbolizing the privacy policies of websites by different colors; thus allowing the users to select the privacy settings corresponding to their preferences. To reach this goal, the users are introduced in the loop of the data acquisition process via simple, clear and active interactions. We propose to base these interactions on concepts and physical interactions that characterize the Participatory Sensing deployments, such as locality, being situated and collaboration among users. The sensors embedded in the personal end devices including camera, microphone, accelerometers and GPS are exploited in a way similar to existing work on secure device pairing such as [6]. In addition to provide a reliable authentication mechanism and to eliminate potential man in the middle attacks, such interactions can allow the users to select their partners to exchange information consciously and easily. Furthermore, the authentication mechanisms based on the embedded sensors can be extended to adjust additional privacy settings. Interactions can be classified according to their complexity and associated to categories of data to share as well as their duration of availability. For example, shaking simultaneously two smartphones is a conscious action that could authorize data transfer between both devices. The duration and the amplitude of the shaking pattern could determine the privacy level of the exchanged data as well as their duration of validity. A direct interaction with a software interface could be considered as an easiest alternative. Nevertheless, we think that a simple, visual and understandable scheme increases the user awareness as well as eases the selection and control of the privacy settings.

Extending this concept to all participants of the participatory sensing space allows the achievement of the second goal of our concept: the construction of a decentralized network of trust. Each new device joining the network is authenticated based on interactions with already trusted members and the privacy settings are directly adjusted by the users. The introduction of a privacy propagation scheme helps in limiting the dissemination of sensitive data among the users, as the sensitivity of the shared data decreases with the distance to the source. This eliminates potential threats to privacy because attackers can only access less sensitive data originating from fewer sources in comparison with a centralized architecture, where attackers–in the worst case–can access the whole set of sensitive information (Fig. 1).

IV. Outline of Future Work

Before implementing our proof of concept, three main steps are necessary. First, the capabilities of the sensors have to be explored in order to build an extensive library of reusable mechanisms for different deployment scenarios. Simplicity, versatility and pleasure [7] are examples of criteria that will be taken into account during the selection process of appropriate mechanisms. The type of data to transfer as well as the availability duration will then be mapped to the available parameters for each library component. A trade-off between interruptibility and awareness of the users has to be found. Requesting frequent interventions in the privacy process may irritate the users, thus provoking the inverse effects or leading to massive abandonments. Finally, the scheme of the trust propagation has to be designed that implies filtering successively the information transmitted according to the settings selected by the user during the joining phase. Additional mechanisms to upgrade or downgrade the privacy preferences also have to be conceived.

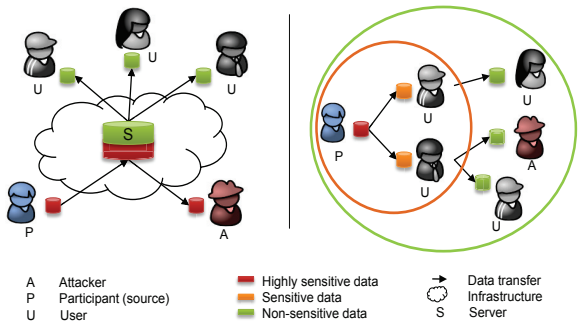

Figure 1. Protection of sensitive data: centralized vs. decentralized structures

V. Conclusion

Within the scope of this extended abstract, we propose to involve the participants in the process of achieving privacy by exploiting the inherent mechanisms of Participatory Sensing in order to raise users' awareness on privacy issues. The exploitation of these mechanisms at large scale will additionally lead to the construction of a decentralized and trusted network, where the sensitivity of the transferred data will decrease with the distance to the source, which eliminates certain threats to privacy.

References

[1] K. Shilton, "Four billion little brothers?" *Communications of the ACM*, vol. 52, no. 11, 2009.

[2] Thiagarajan, A. et al., "VTrack: Accurate, Energy-Aware Road Traffic Delay Estimation Using Mobile Phones," in *Proc. of SenSys*, 2009.

[3] Center for Embedded Networked Sensing. AndWellness: Improving Wellness with Mobile Personal Sensing. [Online]. Available: http://research.cens.ucla.edu

[4] Cornelius, C. et al., "AnonySense: Privacy-Aware People-Centric Sensing," in *Proc. of MobiSys*, 2008.

[5] Cranor, L.F. et al., "User Interfaces for Privacy Agents," *ACM Transactions on Computer-Human Interaction*, vol. 13, no. 2, 2006.

[6] Mayrhofer, R. et al., "Shake Well Before Use: Authentication Based on Accelerometer Data," *Pervasive Computing*, 2007.

[7] D. A. Norman, *The Invisible Computer*. MIT Press, 1999.