The Smart Picture Privacy Tracker - Privacy in the Age of Wearable Computing

Research Outline

Katharina Krombholz and Adrian Dabrowski

May 21, 2015

1 Project Description

Motivation

Due to the ongoing proliferation of mobile and wearable devices with integrated cameras, the problem of unintentionally photographed individuals in public spaces amplifies. These new technologies are becoming more and more pervasive and pose new challenges for protecting the privacy of their users and bystanders. Particularly the discreet recording capabilities of such devices pose new challenges to consensual image disclosure. Therefore, new Privacy Enhancing Technologies (PETs) will be needed to help preserve our digital privacy. At this time, no feasible solution is available to get an informed consent between the photographer and unintentionally captured individuals on a picture. In the scientific literature, a handful of approaches has been presented to tackle the issue of picture privacy. In the course of my ongoing research, I reviewed and systematized these approaches [4] and found that most of them [6, 8, 10, 7, 9] only address narrow scenarios that ignore certain contextual dimensions. Furthermore, they require their users to perform a certain action in order to function. This requires the user's awareness of being recorded which is often not feasible when moving around in public spaces. As most previously published approaches also rely on the transmission of sensitive data to a third party over the Internet, new privacy challenges are introduced by resolving picture privacy. I am currently working on the *P3F*-project [2], where we are currently developing a clothing-based PET. To evaluate this approach, we conducted a comprehensive user study in the field with semi-structured interviews. Our preliminary results suggest that privacy-aware potential users of such technologies highly desire fully privacy-preserving tools. Furthermore, we found that some particularly unobtrusive PETs (such as P3F) are hard for users to understand and that PETs with low visibility do not sufficiently communicate cognitive models to the user. We also found that as a user interface, many participants desire only a single button to push as it gives them a sense of control. This work is currently under submission at *UbiComp 2015*[1] and motivates me for the project that I'm describing in the following.

Our Contribution

In the course of this project, we aim to improve the state of the art by developing the *Smart Picture Privacy Tracker*, a smartwatch-based PET that resolves the pitfalls of previously proposed approaches. We plan to develop a technology that works regardless of a pre-defined scenario and provides its users an intuitive user interface. The Smart Picture Privacy Tracker consists of a smartwatch app that notifies users about pictures taken on co-located cameras in smartphones or wearables (e.g. Google Glass or [1]) and then lets the user decide on the further use of the taken picture. It furthermore consists of a smartphone (and Google Glass selectively) app and lets photographers easily share pictures taken in crowded spaces with *Smart Picture Privacy Tracker*-enabled smartwatches nearby. The communication between the mobile or wearable camera and the smartwatch relies on ad-hoc networks that are created and terminated based on co-location. While such an ad-hoc network exists between two devices, a shared folder is created on both devices containing the taken pictures that require a decision on the further use. For privacy reasons, this folder is deleted after disconnection. Therefore, our approach does not require Internet connectivity or the transmission of (sensitive) information to a third party service. On the one hand, the app creates and raises awareness of pictures taken in its user's surroundings. On the other hand, it lets photographers

[1] http://ubicomp.org/ubicomp2015/

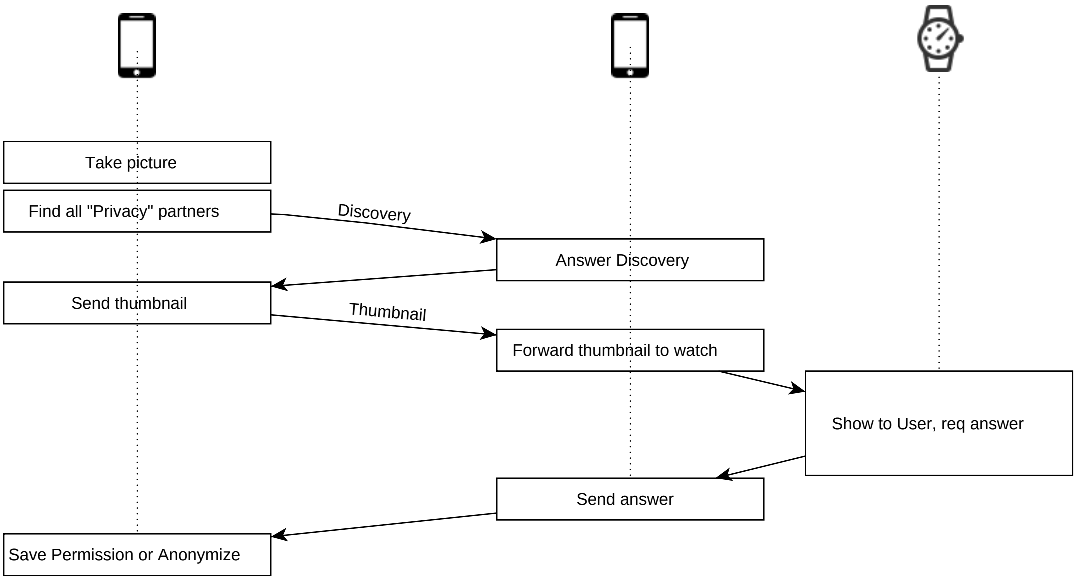

Figure 1: Messages exchanged between camera phone and the smart watch

and photographed individuals obtain informed consent on the use of the taken pictures immediately after they have been taken. Researchers have found that privacy preferences are strongly tied to the context [3, 5]. In comparison to most previously published approaches (as analyzed in [4]), the *Smart Picture Privacy Tracker* is designed to work regardless of a certain context as soon as the privacy toggle button is pushed.The user interface is intuitive and simple and should also allow marginalized groups (such as users with certain impairments) to preserve their digital privacy.

2 System Design

In general, we plan to implement two Apps, (1) a photo app for smartphones and/or Google Glass, and (2) a privacy tracker app for smartphones that sends notification to paired smartwatches. We plan to use the following Hardware for our prototype implementation:

- Nexus 5 with Android 5.0 Lollipop
- Moto360 smartwatch
- (Optional: Google Glass Explorer Version)

Our prototype will consist of the following components:

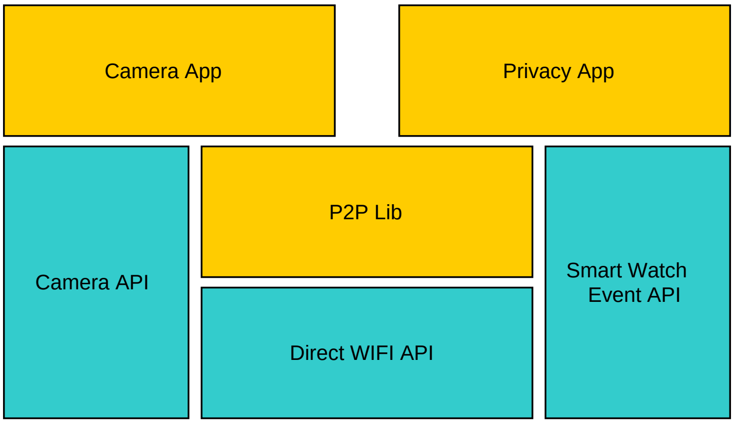

Figure 2: Both Apps sharing a common messaging library build on top of WiFi-Direct

2.1 Photo App

The main component running on a smartphone and or Google Glass is a simple PhotoApp with additional functionality to ask photographed individuals for permission. Asking for permission is performed by sending the respective picture to nearby devices connected via Wi-Fi Direct. Upon approval (or disapproval), the pictures is transmitted back to the PhotoApp. In order to not disrupt the photographer in taking additional pictures, the respective pictures are stored in the Photo directory with additional flags and/or modifications of the picture. The Photo App allows users to release individual photos to nearby devices by simply tapping on the privacy icon on the upper right corner of the screen.

2.2 Privacy Tracker App

The core of the privacy tracker app is intended to run on a smartphone that is paired with an associated smartwatch. This is due to the fact that smartwatches are generally not compatible with Wi-Fi Direct. Furthermore, the app can be used by smartphone users and does not require a smartwatch in order to function. For smartwatch users, interaction is possible by just using the smartwatch with a few taps. If multiple pictures are shared for approval, they can be swipped through (swipe left - right). In order to blur his/her face on a picture, the user is required to tap on the respective face. To transmit the pictures back to the photo app, the user simply needs to swipe up to release the picture.

2.3 Communication Layer

In order to enable the communication between the devices, we consider Wi-Fi Direct an ideal standard. Wi-Fi direcct enables devices to easily connect without a wireless access point. The main advantage for our use case is that devices can connect even if they are from different manufacturers. Only one device needs to be compliant with Wi-Fi Direct to a establish a peer-to-peer connection in order to transfer information from one device to another. Bluetooth for this purpose has a variety of disadvantages, one and probably the most dominant one for our use case is that it will according to the Bluetooth API trigger pairing if the devices have not been paired before (requires manual intervention by the user). In our use case, we assume that ad-hoc networks are created by devices that have not yet been paired before.

3 Optional Functionality

In this section, we briefly describe additional functionality that could supplement the smart picture privacy tracker in order to enhance the user experience.

3.1 Face Recognition

By using face recognition, we could reduce user interaction, as all pictures transmitted to the smart picture privacy tracker could be checked for faces that correspond its users face (if previously configured by the user). In order to train a face recognition system, the user needs to take several pictures from different angles. As face recognition is performed locally on the smartphone, it doesn't violate its users' privacy but can be used to efficiently sort out pictures that do not have the user on it.

3.2 Location Markers

As an additional functionality, we plan to implement *Location Markers* to define privacy-sensitive spaces and to notify mobile and wearable cameras a soon as they enter such a privacy-sensitive space. The definition of these spaces will be implemented with iBeacons. We chose this approach in order to avoid the transmission of location information to a third party service over the Internet. iBeacons can be used for 3D positioning indoors and outdoors. Furthermore, they cannot send push-notifications or collect user data of nearby devices. Instead, iBeacons can only send information about their own identity (UUID, major, minor). We therefore consider this technology an ideal solution to define privacy-sensitive spaces for the *Smart Picture Privacy Tracker* in the most privacy-preserving manner.

References

[1] Which smart glasses will be right for you? `http://venturebeat.com/2014/03/30/which-smart-glasses-will-be-right-for-you/`, accessed August 18th 2014.

[2] Adrian Dabrowski and Katharina Krombholz. P3f - the picture privacy policy framework. `p3f.at`, last accessed on 2015/4/24.

[3] Tamara Denning, Zakariya Dehlawi, and Tadayoshi Kohno. In situ with bystanders of augmented reality glasses: perspectives on recording and privacy-mediating technologies. In *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*, pages 2377–2386. ACM, 2014.

[4] Katharina Krombholz, Adrian Dabrowski, Matthew Smith, and Edgar Weippl. Ok glass, leave me alone: Towards a systematization of privacy enhancing technologies for wearable computing. In *Proceedings of the WEARABLE S&P Workshop, Financial Cryptography and Data Security 2015 (FC'15)*, 2015.

[5] Linda Lee, Serge Egelman, Joong Hwa Lee, and David Wagner. Risk perceptions for wearable devices. *arXiv preprint arXiv:1504.05694*, 2015.

[6] Frank Pallas, Max-Robert Ulbricht, Lorena Jaume-Palasí, and Ulrike Höppner. Offlinetags: A novel privacy approach to online photo sharing. In *CHI '14 Extended Abstracts on Human Factors in Computing Systems*, CHI EA '14, pages 2179–2184, New York, NY, USA, 2014. ACM.

[7] Jeremy Schiff, Marci Meingast, Deirdre K Mulligan, Shankar Sastry, and Ken Goldberg. Respectful cameras: Detecting visual markers in real-time to address privacy concerns. In *Protecting Privacy in Video Surveillance*, pages 65–89. Springer, 2009.

[8] Robert Templeman, Mohammed Korayem, David Crandall, and Apu Kapadia. Placeavoider: Steering first-person cameras away from sensitive spaces. In *Network and Distributed System Security Symposium (NDSS)*, 2014.

[9] Takayuku Yamada, Seiichi Gohshi, and Isao Echizen. Privacy Visor: Method for Preventing Face Image Detection by Using Differences in Human and Device Sensitivity. 2013. unpublished, under review for CMS 2013.

[10] Roberto Yus, Primal Pappachan, Prajit Kumar Das, Eduardo Mena, Anupam Joshi, and Tim Finin. Demo: Faceblock: privacy-aware pictures for google glass. In *Proceedings of the 12th annual international conference on Mobile systems, applications, and services*, pages 366–366. ACM, 2014.