Spybuster - a Community-Based Privacy Tagging Platform

Johannes Kiemer, Till Ballendat, Tim Langer, Wenqi Zhang, Alexander De Luca
Media Informatics Group, University of Munich
Amalienstr. 17, 80333 Munich, Germany
{kiemer, ballendat, langert, zhangw}@cip.ifi.lmu.de, alexander.de.luca@ifi.lmu.de

ABSTRACT
The goal of *Spybuster* is to provide a powerful and easy accessible community platform, which helps the members to cope with the increasing number of threats for everyone's privacy in everyday life. Spybuster uses a geotagging system to associate privacy threats with their locations. Users can add supplemental information such as a description of the threat and the exact address. The resultant tags can either be accessed over a mobile application with an interactive radar or a website using a Google Maps-mashup for displaying tags in a certain area. Due to a shared database users can organize their tags on both platforms.

Categories and Subject Descriptors
H.5.0 [**INFORMATION INTERFACES AND PRESENTATION**]: General: information interface for a mobile and a web platform.

General Terms
Design, Security

Keywords
Privacy, community, mobile device, geotagging, GPS.

1. INTRODUCTION
More and more, privacy threats enter our everyday life – covert or at least inconspicuous. One example is the almost omnipresent camera surveillance. Many public spaces are already monitored and only few people are aware of that fact. Whenever we move in the public, the chance is high that we are monitored without knowing it. Yet other threats for everyone's privacy lurk in hidden data mining such as RFID readers, biometric sensors and the like. For instance some stores collect data about buying patterns each time customers use the store's customer-card. And again, people do not realize that. From this circumstance the basic concept of this work evolved: raise the awareness of privacy threats.

One of the first work that explicitly tried to make invisible privacy threats visible has been performed by Belotti et al. [1]. They enhanced rooms at a campus with physical hints pointing to video surveillance, voice recording and the like to enable the people there to avoid such places when desired. Similar work has been performed by Ngyuen et al. [3] that used screens and similar equipment to make people aware of sensors. Gisch et al. [2] created a visualization for mobile devices that displays privacy related data in a user-friendly way when interacting with ubicomp service environments.

The previous mentioned approaches have one thing in common: in those cases responsible persons for the privacy threats provide privacy hints to the people. The problem is, that in many cases those people might not want to give such hints and thus it is hard to create a system that can support its users in such a situation.

Therefore, this paper presents Spybuster, a community-based privacy platform that has been created to overcome this gap by relying on a web community as the provider for the privacy information.

2. GEOTAGGING OF PRIVACY THREATS
In order to achieve this goal Spybuster utilizes so-called geotagging to store privacy threats. This means users can describe and categorize threats and link them to a specific GPS-coordinate. Thus, these tagged privacy threats can be identified by others. Geotagging is a widely used approach. For instance flickr[1] offers its users the possibility to tag their photos with the GPS-coordinates where they have been made.

Geotagging in the Spybuster system is supported on two platforms: a mobile application for cell-phones and a website. On the mobile device the geotagging is conducted with an inbuilt or an external GPS-receiver. Alternatively, the exact GPS-position can be identified by the method used on the website: The GPS-position for a given address is obtained via a Google-Maps-request.

3. PROTOTYPE
As mentioned before, the Spybuster Prototype consists of two applications. The first one is a browser based application that uses simple user interface paradigms while the second one has been created for mobile devices and thus uses some specialized small screen representation that has been especially developed for.

3.1 Mobile Application
The mobile application has been programmed using the Java Micro Edition. The software is designed to have the full set of functionalities that Spybuster supports, so that users do not necessarily have to access the web-platform at any time.

After a one-time registration during which the users choose their username and a personal password, they can log in and start using

MobileHCI 2008, September 2–5, 2008, Amsterdam, the Netherlands.
ACM ISBN 978-1-59593-952-4/08/09.

[1] http://www.flickr.com

the system. If the login was successful, the main screen is shown to the user. This screen consists of the zoomable Spybuster-radar as shown in Figure 1.

Figure 1: Spybuster-radar: the middle visualizes the user. The black dots mark possible privacy threats.

A red dot in the center of the radar presents the current GPS-position of the users. If there are any tags near that position, they are displayed as black dots. Each black dot stands for one specific privacy threat.

The users can now select those dots to get further information about the threat. The information screen displays the name, category and description of the tag, optionally the address for easier location. For users with a GPS-device the radar will automatically update all the tags as the user changes location. The radar is zoomable, which enables it to automatically choose a zoom rate that displays a reasonable amount of threats close to the user.

Another option that is supported by the application is to create new tags at the current position using a simple input form. The tag will then be sent via http-post request to a server, which saves it to the database. The new tag is instantly accessible for all web and mobile users. To distinguish the usefulness of the tags, which are produced by the community, everybody has the possibility to rate tags of other users. Furthermore, it is possible to ignore single tags, whole categories or low rated tags, so that they are not displayed in the personal radar anymore.

3.2 Website

In addition to the mobile application, Spybuster provides a web platform, which has the same functionality, but with a user interface optimized for big screens. Instead of the radar users can access the tag-database via a personalized and interactive map using the Google maps API. As depicted in Figure 2, all relevant privacy threat tags are shown on the map. They can be selected for further information or modification. Additionally, the website can be used to modify the personal settings and the created tags of a user, no matter whether they have been created with the mobile application or the web platform.

3.3 Database

All the user data and privacy threat tags are stored in a MYSQL-Database, for which we designed an object orientated PHP interface. Both mobile and web use the same classes to interact with the database in order to minimize code-redundancy.

4. USE CASE

One conceivable use case could be the following. Alice walks through the pedestrian area and recognizes a surveillance camera. She is a member of the Spybuster-community and wants to check on her cell phone whether this camera has already been tagged by another user. After starting the application and logging in, she sees that the place is marked with no privacy tags. Therefore, she adds a tag for this camera via her cell phone to make the community aware about this privacy threat. But she does not have enough time to complete the whole tag entry since she is on her way to an important meeting. Thus, she decides to upload the tag without any detailed description. In the evening at home she logs in to the website and adds the missing information to the tag using the web platform.

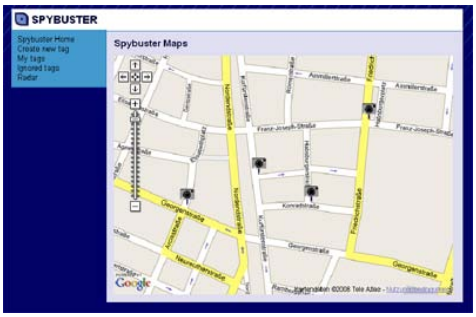

Figure 2: Spybuster Web Application

5. CONCLUSION AND FUTURE WORK

In this paper, we presented Spybuster, a community-based system created to support people to keep their privacy in everyday's life. We created two applications, a mobile and a browser based, to enable the users to use and enhance the system at any time (just an internet connection is required). Spybuster has been created on a community basis to overcome the problem that the people responsible for such threats might not be willing to highlight them themselves whereas in a community, this task will be done by the masses.

A major task for the near future will be a user study to evaluate both platforms in terms of interface design, performance and usability. Additional features that do not affect the core concept of Spybuster, like a community-forum and compatibility with more mobile phones, will be implemented concurrently. Another feature that seems useful is the offline storage of privacy threat tags so that the system can be used without an internet connection.

6. REFERENCES

[1] Bellotti, V., Sellen, A. Designing for Privacy in Ubiquitous Computing Environments. In: The third European Conference on Computer-Supported Cooperative Work. Milan, Italy. September 1993.

[2] M. Gisch, A. De Luca, M. Blanchebarbe. The Privacy Badge - A Privacy-Awareness User Interface for Small Devices. In Proceedings of the Mobility Conference 2007. Singapore, September 10 - 12, 2007.

[3] Ngyuen, D., Mynatt, E. Privacy Mirrors: Making Ubicomp Visible. In CHI 2001. Seattle, WA.