PriFi Beacons: Piggybacking Privacy Implications on WiFi Beacons

Bastian Könings
Institute of Media Informatics
Ulm University
89081 Ulm, Germany
bastian.koenings@uni-ulm.de

Florian Schaub
Institute of Media Informatics
Ulm University
89081 Ulm, Germany
florian.schaub@uni-ulm.de

Michael Weber
Institute of Media Informatics
Ulm University
89081 Ulm, Germany
michael.weber@uni-ulm.de

UbiComp'13 Adjunct, September 8–12, 2013, Zurich, Switzerland.
ACM 978-1-4503-2215-7/13/09.

http://dx.doi.org/10.1145/2494091.2494115

Abstract
Making users aware of privacy implications in ubiquitous computing is a critical challenge to support user acceptance and trust. However, the invisible and embedded nature of UbiComp systems prevents users from naturally perceiving active sensors or even the presence of systems. Furthermore, autonomous interventions of systems in the user's environments or undesired interactions with the user may be disturbing and could violate a user's privacy expectations. We propose *PriFi beacons* to support users in perceiving ongoing observations and potential disturbances from systems in the user's current environment. Privacy awareness information is piggybacked on WiFi beacons by leveraging their information elements. The information is extracted by an Android-based privacy client and presented to the user in a privacy awareness interface.

Author Keywords
privacy awareness; sensors; actuators; beacons; wifi.

ACM Classification Keywords
K.4.1 [Public Policy Issues]: privacy; C.2.1 [Network Architecture and Design]: wireless communication; H.5.2 [User Interfaces]: Prototyping.

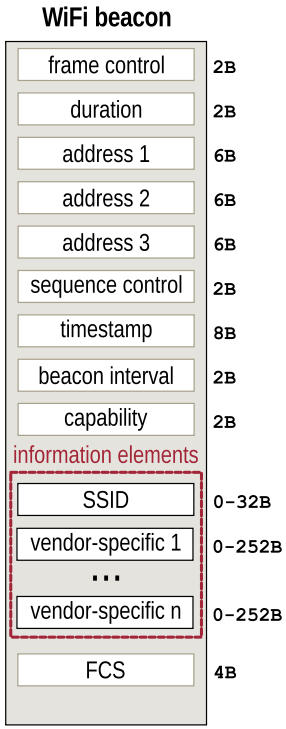

Figure 1: Frame format of WiFi beacons as defined in the IEEE 802.11 standard [4].

Introduction

Due to the invisible nature of ubiquitous computing (UbiComp) systems, privacy of users is a challenging topic. Users are often not aware of a system's sensing and acting capabilities, or even of the system's presence. This lack of awareness may lead to discomfort and the feeling of violated privacy expectations when users discover at a later state that they have been observed by the system. The same effect could be caused by disturbances of the system, either by undesired interventions in the user's environment or by undesired interactions. These physical privacy aspects are often neglected in existing privacy research, which primarily focuses on information-centric privacy aspects. From an access control point of view, privacy can be described as *"the condition of being protected from unwanted access by others – either physical access, personal information, or attention."* [1] A more simplistic definition describes privacy as *"a state in which one is not observed or disturbed by others"* [8]. Especially in UbiComp, such non-information-centric privacy aspects will gain more importance [5].

In this paper, we propose *PriFi beacons* as an approach to support awareness of privacy implications of systems and devices in a user's current environment, with respect to observations and disturbances. PriFi beacons utilize information elements of WiFi beacons to piggyback information about privacy implications and to broadcast them in a system's proximity. The approach allows simple and fast discovery of privacy implications without the need of a preliminary established connection. We implemented a prototype of our approach that enables devices and systems to send PriFi beacons. We further adapted the Android WiFi stack to support extraction of the privacy information element and implemented an awareness user interface to present privacy implications to users.

Related Work

Announcing privacy information in broadcast beacons has originally been proposed by Langheinrich as part of his privacy awareness system pawS [7]. His prototype was based on infrared beacons, which require the receiver to be in visible range. Furthermore, the original privacy beacons did not consider potential disturbances.

The main design goals for effective privacy announcements in UbiComp are minimal connection overhead, fast and reliable transmission, and scalability. Most existing wireless technologies require initial connection establishment to exchange data. A possible solution to mitigate a required connection is to utilize customizable information in discovery or setup processes. Davis et al. [3] used Bluetooth device names to enable spontaneous interaction between users and smart environments. However, the main drawback of this approach is the long discovery period of up to 15 seconds.

PriFi Beacons

A faster discovery period of only a few seconds can be achieved by using IEEE 802.11 (WiFi) beacons [4]. WiFi beacons (see Fig. 1) announce available WiFi networks and provide two possible ways of integrating custom information. The first way is using the service set identifier (SSID). The SSID is typically used for user-friendly names of WiFi access points. However, in contrast to Bluetooth device names with a maximum length of 248 bytes, SSIDs are limited to only 32 bytes. The second way provided by WiFi beacons is the use of custom *information elements*. Information elements are appended to beacons in order to carry optional information, e.g., the SSID mentioned before. A special type are vendor-specific information elements which allow to carry nonstandard information. A single information element can carry up to 252 bytes. An

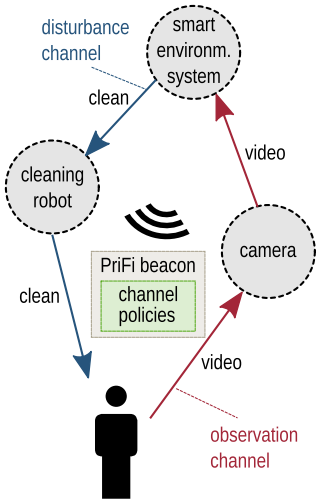

Figure 2: Privacy model for three entities. Channel policies are included in the PriFi beacon.

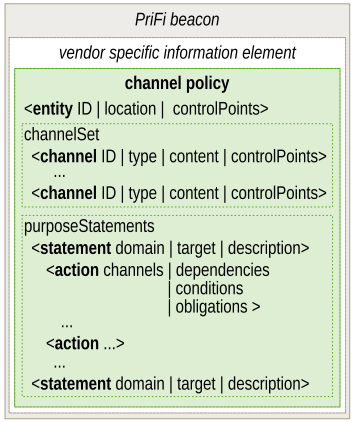

Figure 3: Channel policy format.

information element of the same type can be appended multiple times, which allows to transmit a maximum payload of 2,272 bytes in one beacon frame. For transmission, larger messages could be split into multiple fragments contained in multiple beacons as proposed by Chandra et al. [2]. However, this approach decreases the reliability of transmissions.

We propose PriFi beacons as a combination of SSID and information element customization. Although attaching custom information elements is standard compliant, existing WiFi drivers require manual patching in order to pass information elements to the application level. Thus, we also use customized SSIDs to provide a fallback mechanism for non-patched devices.

The information provided in PriFi beacons is based on our prior work of a territorial privacy model [5] and *channel policies* [6]. The model captures which entities (who) might affect a user's privacy, through what kind of observations and disturbances (how), and for what purpose (why). Observations, (e.g., by a video camera) and disturbances (e.g, from a cleaning robot) are modelled as channels between the user and such entities (see Fig. 2). Channels can be forwarded between entities, for instance the camera forwards the video channel to the smart environment system (SES), which triggers the cleaning robot to start cleaning. The model is instantiated by discovering channel policies from involved entities. The general format of a channel policy is depicted in Figure 3.

In our example, the channel policy of the video camera allows to receive information about the camera, like its location, and to notice that the video channel is forwarded to the SES. Whenever a channel is forwarded to another entity, the channel policy contains a reference to that entity's channel policy, which is either provided by another beacon or can be obtained from a remote URL. The SES's policy allows to infer how the video channel is used, e.g., for security purposes. The policy further indicates when the cleaning robot will be triggered, e.g., before time periods with low electricity rates to save money when recharging.

All channel policies could be included in separate PriFi beacons. However, in case of a central UbiComp system like in our example, it makes sense to combine policies into a single beacon to avoid unnecessary transmissions. Thus, all policies can be included in multiple vendor specific information elements of the same beacon.

Discovery & Control

We envision PriFi beacons as one part of a more comprehensive discovery process for privacy awareness. Different discovery approaches can be applied depending on the user's environment. The beaconing approach is especially suited for public environments (e.g., train stations or shopping malls) and semi-public environments (e.g., schools or offices) where users are usually not connected to the network infrastructure of surrounded systems. Here, beacons allow users to easily gain awareness of privacy implications. However, user control will mostly be limited or impossible in such environments.

In personal environments like the own home, users are usually connected to the same network as existing UbiComp systems. Thus, discovery of channel policies is not limited to PriFi beacons and can be extended with different approaches, e.g., UPnP-based discovery. Furthermore, channel policies could provide references to an entity's control points, which allow users to deactivate the entity or its channels. A simple solution in terms of authorization is to grant access to control points only from

Figure 4: PriFi enabled webcam.

Figure 5: PriFi enabled Roomba.

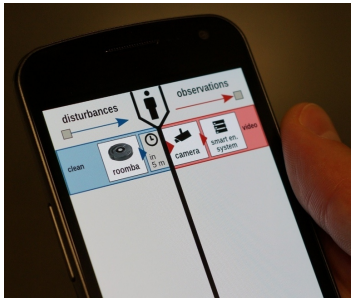

Figure 6: Privacy awareness client.

users in the same network, e.g, the camera and cleaning robot can be switched off from all users in the same WPA-protected WiFi network. The control point reference can be a simple URL, e.g., http://192.168.2.23/camera/.

Prototype

We implemented a prototype of the beaconing approach based on a Raspberry Pi and a patched Android device for sending and receiving PriFi beacons. The Pi has been equipped with a USB-WiFi stick (RT2870/RT3070 chipset), which runs in monitor mode in order to send custom WiFi frames. We used the Python library Scapy to frame the PriFi beacons and transmit them with a beacon interval of 500ms. We equipped a webcam (Fig. 4) and cleaning robot (Fig. 5) with such Pis, which also provided control points to users in the same WPA-protected WiFi. Currently, the range of PriFi beacons can only be adapted by changing the sender's signal strengh. A future prototype will also investigate geo-fencing techniques [9] to provide more precise coverage areas.

In order to extract the privacy information element on the client site, we patched the Android WiFi stack (version 4.0.4). We implemented an Android application for browsing discovered devices and their privacy implications (see Fig 6). In order to also allow users with unpatched devices to discover privacy implications, the PriFi beacon's SSID was composed of the string `PB|<type>|<URL>`, where `PB` stands for PriFi beacon, `<type>` is either *observation* or *disturbance*, and `<URL>` refers to a remote location of the entity's channel policy, which was subsequently fetched by the application.

Summary & Future Work

PriFi beacons provide a simple, reliable, and fast solution for announcing privacy implications of systems in a user's environment. Privacy-relevant information is integrated in vendor-specific information elements of WiFi beacons. Our prototype shows the feasibility of our approach for announcing observations of a video camera and potential disturbances from a cleaning robot. In future work, we plan to integrate further discovery mechanisms in an Android-based client and provide a more sophisticated user interface for supporting users' awareness and control of privacy in UbiComp.

References

[1] Bok, S. *Secrets: On the Ethics of Concealment and Revelation*. Pantheon Books, 1982.

[2] Chandra, R., Padhye, J., Ravindranath, L., and Wolman, A. Beacon-stuffing: Wi-fi without associations. In *Proc. HotMobile*, IEEE (2007), 53–57.

[3] Davies, N., Friday, A., Newman, P., Rutlidge, S., and Storz, O. Using bluetooth device names to support interaction in smart environments. In *Proc. MobiSys*, ACM (2009), 151–164.

[4] IEEE. 802.11 standard for LAN/MAN, 2012.

[5] Könings, B., Schaub, F., Kargl, F., and Weber, M. Towards territorial privacy in smart environments. In *Proc. of the Intelligent Information Privacy Management Symposium*, AAAI (2010), 113–118.

[6] Könings, B., Schaub, F., and Weber, M. Who, how, and why? enhancing privacy awareness in ubiquitous computing. In *Proc. WiP PerCom*, IEEE (2013).

[7] Langheinrich, M. *Personal Privacy in Ubiquitous Computing – Tools and System Support*. PhD thesis, ETH Zurich, Switzerland, 2005.

[8] Oxford University Press. *"Privacy" Definition*, 2nd ed. Oxford Dictionary of English, 2005.

[9] Sheth, A., Seshan, S., and Wetherall, D. Geo-fencing: Confining wi-fi coverage to physical boundaries. In *Pervasive Computing*, vol. 5538. Springer, 2009.