Figure 4: PriFi enabled webcam.

Figure 5: PriFi enabled Roomba.

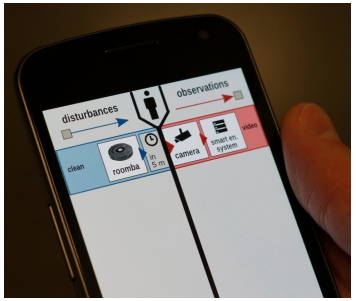

Figure 6: Privacy awareness client.

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.