Exploring the Design Space for Geo-Fenced Connected Devices and Services at Home

Geert Vanderhulst
geert.vanderhulst@alcatel-lucent.com
Alcatel-Lucent Bell Labs
Copernicuslaan 50, 2018
Antwerp, Belgium

Marc Van den Broeck
marc.van_den_broeck@alcatel-lucent.com
Alcatel-Lucent Bell Labs
Copernicuslaan 50, 2018
Antwerp, Belgium

Fahim Kawsar
fahim.kawsar@alcatel-lucent.com
Alcatel-Lucent Bell Labs
Copernicuslaan 50, 2018
Antwerp, Belgium

UbiComp '14, September 13 - 17 2014, Seattle, WA, USA Copyright 2014 ACM 978-1-4503-3047-3/14/09. . . $15.00.
http://dx.doi.org/10.1145/2638728.2641706

Abstract
This paper offers a reflection on the design space for a geo-fenced connected device and service (GFS) - a specification enforcing that a connected device can only be used within a virtual perimeter. Many connected devices are nowadays being accessed through applications running on mobile devices instead of tangible controls. Whilst this ubiquitous access is highly convenient, it is also making connected devices more vulnerable. As such, we reintroduce location-constrained interaction, adapted to connected devices present in a modern home, and explore three design cardinals: (i) spatial granularity, (ii) roles and delegation, and (iii) access control. We report on a qualitative study that explored this design space through a prototype geo-fenced connected lighting system. Our findings suggest that users would like to have geo-fencing for a subset of connected devices, prefer to define geo-fences statically but with different granularities for different devices, and desire access control through location verification and credentials.

Author Keywords
Home Computing, Connected Device, Access Control

ACM Classification Keywords
H.5.m. [Information Interfaces and Presentation (e.g. HCI)]: Miscellaneous

Introduction

With the advent of the Internet of Things, an increasing number of household devices are now becoming connected to the Internet to offer value-added services beyond their primary established purposes. Manufacturers of these devices embrace the flexibility of the cloud for hosting their services, and expose the features of their products in digital user interfaces rather than tangible controls. An archetypical example of this trend is the Philips Hue light [6], connected bulbs that ship without hardware buttons. The lights' intensity and colour can be exclusively altered using applications running on e.g., an Android or iOS device. A more hybrid example includes the Nest thermostat [3] which combines basic interaction controls with remote access via mobile applications, also outside the local network. Whereas the design of a light switch or thermostat button on the wall demands for physical presence in a room to operate it, the presence of a service in the cloud liberates us from geographical boundaries. However, this flexibility of using any device anywhere for accessing e.g., our home environment also has its dark side. An intruder can cause connected lights to be turned on or off, an adversary can unlock a connected door lock remotely, or a hacker might snoop on security cameras. Because of the different affordances these devices offer, a traditional password-based access control mechanism may no longer be appropriate. A number of recent studies have already started to explore the requirements of access control for connected devices at home with qualitative interviews [9–11, 14, 17].

To mitigate the security risks, we advocate for geo-fenced connected devices and services (GFS) in this work. With GFS we aim to bring back the notion of local interactions such that access to a device is strictly confined to one or more venues, despite of where the device's services actually run. We explore three design cardinals for GFS: *spatial granularity*, *roles and delegation* and *access control*. Furthermore, we report on a qualitative study in which 12 individuals subjectively assessed different aspects of GFS using a technology probe.

Design Space for Geo-fenced Services

In its simplest form, geo-fencing is analogous to a WiFi network, where a networked service can only be accessed within a spatial perimeter. GFS takes this metaphor further and applies it to individual connected devices such that their services can only be accessed within a confined spatial boundary defined by end-users themselves. To this end, we observe that there are three design cardinals that need to be considered for GFS: *spatial granularity*, *roles and delegation* and *access control* respectively addressing how to define geo-fences, how to maintain ownership and manage conflicts, and how to assign access rights.

Spatial Granularity

Spatial granularity specifies the range of a geo-fence which can be defined either *statically* or *dynamically*. For a static fence, one may set a range based on a specific distance (e.g., 10 meters, 20 meters, etc) that remains constant once defined. The range of a dynamic fence, however, could vary depending on a number of contextual factors – time of the day, location of the user, type of device, and social context (e.g., presence of visitors). While static fences are simpler to maintain, dynamic fences require active management with user-defined rules. The formation of a geo-fence can be achieved by one or multiple location beacons embedded into the device itself or nearby physical objects. Especially with the proliferation of Bluetooth Low Energy (BLE) proximity sensing, we consider the formation of a geo-fence to become increasingly simple.

Roles and Delegation
Previous studies have shown that shared ownership is the dominant dynamic for connected devices at home with temporal exceptions [9, 10]. We expect that the ownership dynamics for GFS would be similar, which is also confirmed in our qualitative study as discussed later in this paper. The major use case for GFS is short-lived interactions with devices at home. Hence actions performed through a GFS are likely to change the state of devices. In the analog world with tangible controls, the user nearest to the control has priority. However, considering each user now carries her own instance of a light switch or television remote on her mobile device, concurrent use of GFS by multiple users can lead to conflicts. There are multiple alternatives to address such conflicts, e.g., priority can be set based on authority, proximity or first come, first served basis. A special situation occurs when a GFS is already in use and now requested by a user with a higher priority. In this case, we foresee a short grace period after which the new user can claim the GFS, i.e., access is handed over. The strict confinement of a GFS to a space might sometimes be too restrictive, losing the convenience of remote access. As a compromise between global access and local security, a user can be allowed to explicitly associate herself with a GFS through the device of another user who resides at the space where the GFS is running. The *physical delegate* then receives a request from the remote user and by confirming it she delegates access to a GFS on her behalf.

Access Control
Solutions exist to enforce virtual perimeters, which specify the geographical boundaries from where a location-based service can be accessed [8]. However, since the location of a user is typically tracked via her personal device, it is implicitly assumed that users are honest about their current whereabouts, which might not be the case. A number of past research works have explored location (with verification) for access control [12, 13, 15, 16, 18]. These works are typically tailored to either one of the following scenarios: instant authentication (i.e. location is used as a password) and delayed verification (i.e. a location proof is used as an alibi to the police or to show a teacher that a student physically attended a class). Building upon these works, we consider that the explicit presence at the physical location of a connected device offers a good design alternative for access control besides conventional password-based authentication. In our proposed solution, the location verification process not only relies on the user's claimed location but also on feedback from trusted co-located witnesses at the device's location.

Figure 1 depicts the flow of actions in our witness-based access control protocol which leverages iBeacon technology [1]. The first step, the automated discovery of a GFS, is treated as optional since a GFS runs in the cloud and can be invoked manually. In the next step, a user device pro-actively shares the user's identity and her location to the GFS in order to obtain a personalised instance of the GFS. This step is very well understood and supported by standards such as OpenID [5] and OAuth [7]. As a secondary authentication mechanism, the location claimed by the user's device is verified. To this end, the GFS generates a unique verification token – a Unique Universal Identifier (UUID) – which is sent to the device. The device now broadcasts this UUID over Bluetooth, just long enough for nearby witnesses to pick it up. These witnesses detect the signal emitted by the user's device and notify subscribed services about the UUIDs, signal strength and approximate distance they sense. Upon receiving this information from its witnesses,

a GFS can be assured that the user indeed resides at the venue. After successfully passing the location verification process, an authorization token is obtained and interaction can start. Note that since UUIDs are randomly generated by a GFS and only used once, they do not give away the user's identity at any point.

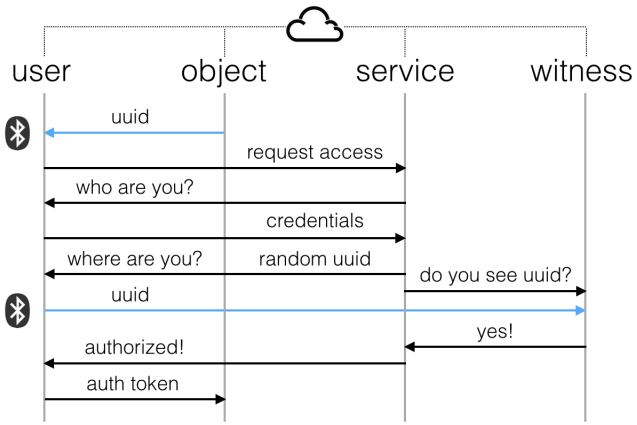

Figure 1: Access Control Protocol.

A Qualitative Study

To evaluate the usability of a GFS at home and its different design alternatives, we have conducted a qualitative study. We developed a geo-fenced connected lighting system with Philips Hue Lights that was used by our participants. The Philips Hue Lights are wireless LED lights that can be controlled via mobile applications, i.e. their state, intensity and colour can be configured. In our setup, two lights were augmented with iBeacons for proximity sensing. An iBeacon [2] is based on Bluetooth Low Energy (BLE) and can notify nearby devices (running iOS or Android) of its presence [1]. A device receiving an iBeacon transmission can approximate the distance from the iBeacon, which is categorized into three distinct ranges: (i) immediate (within a few centimeters), (ii) near (within a couple of meters) and (iii) far (more than 10 meters way). In our setup, these iBeacons were used to discover the connected device's services as well as to define the spatial perimeter of the geo-fence (either immediate or near). For the location witnesses we used three android dongles attached to a large display and walls next to the lights. These dongles run a custom built Android application for discovering iBeacon signals emitted by local devices. Finally, we developed a simple iOS application to interact with the lights (switching on and off, dimming, and changing colours). Next to traditional username and password authentication, the application also implements our location verification protocol. Via a range indicator, users are made aware whether they are within the geo-fence or not. For instance, a green, yellow and red range respectively indicate that a user is well within, just within or outside the geo-fence. The application can also make the device act as an iBeacon (peripheral mode) to announce its presence. All these components were connected to a node.js [4] web server that managed the geo-fencing aspects. Our experimental setup and application screenshots are illustrated in Figure 2.

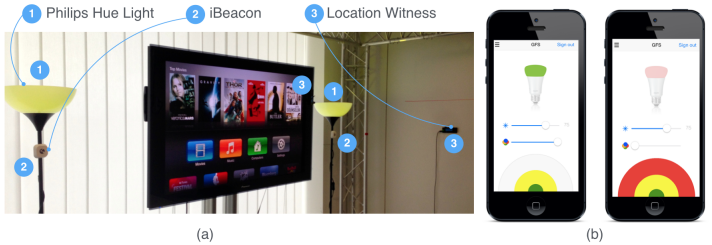

Figure 2: Experimental setup and application screenshots.

Study Methodology
We recruited 12 individuals (7 Males, 5 Females, age range 25-54) through an open invitation in a corporate mailing list. 10 of them own either a smart phone or a tablet, and 6 of them already have at least one connected device at home, e.g., connected lights, a connected TV, etc. Our participants include business professionals and office administrators. As a gratitude for participating in the study, all participants were part of a lottery for a Nike+FuelBand wearable device.

The study session had three components: a demographic questionnaire, an exercise session, and a semi-structured discussion. We started the session by gathering demographic information and asked users about their familiarity with a variety of connected devices at home. To ground the discussion, we provided them with a list of connected devices grouped into six categories: infrastructure (e.g., heating, water, etc), entertainment (e.g., TV, speakers, etc), cooking devices (e.g., pot, oven, etc), general devices (e.g., washing machine, fridge, etc), wellbeing devices (e.g., weight scale, etc) and safety devices (e.g., door lock, security camera, etc). Next, we had an exercise session with two subtasks. In the first subtask, we exposed the participants with two scenarios – without geo-fencing and with geo-fencing – to turn the Philips Hue Lights on and setting the colour to bright green with full intensity with our iOS application. In the second subtask, the participants were exposed to two access control techniques for GFS – with location verification, and with both location verification and credentials – while performing the same tasks as they did for the first subtask. In both subtasks the scenario order was counterbalanced to minimize order effects. After each subtask, we asked for subjective assessment of the participants on convenience and credibility (trust) respectively. Finally, in the semi-structured discussion phase, we collected feedback on different design alternatives for GFS.

Study Results
Our participants generally welcomed the idea of GFS, with 11 participants explicitly mentioning they would love this capability at their home for a variety of devices. Figure 3 illustrates their subjective assessment on convenience before and after introducing geo-fencing. A Wilcoxon Signed-Rank test ($Z = 0.8528$, $p = 0.625$) shows that there is no statistically significant effect of geo-fencing, suggesting that the participants did not feel any additional overhead. To further understand why they prefer this capability we presented them with four contextual factors – simplicity, security, frequency of use and control – against six categories of connected devices enumerated earlier. We conducted a two-way contingency table analysis to see if these factors affected their preference and found a significant association – Pearson $\chi^2(15, N = 60) = 24.3191$ and $p < 0.05$. Examining these further, we have observed that participants preferred infrastructure and safety devices for enhanced security and control. Keeping fine-grained control over device functionalities was also seen as a strong point of GFS.

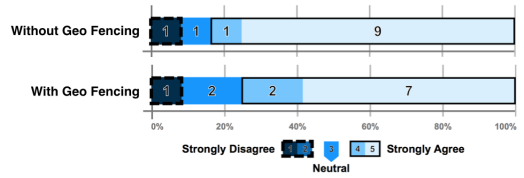

Figure 3: Feedback on convenience.

On spatial granularity our participants had mixed opinions. The majority of the participants (8 out of 12) mentioned that the range should be statically defined.

Multiple participants remarked that it is sufficient to confine the range to a room level, i.e. a device can only be operated in the room of its placement. All of our participants, however, mentioned that they would like to have the capability to define the radius of a static geo-fence or to define rules for extending and contracting fences with minimal effort. Besides, they also suggested that the range for different devices should be different. For example, infrastructure and safety devices should have a longer range than entertainment or cooking devices. One interesting observation was the notion of temporary geo-fencing, i.e. applying location constraints only for a specific time period, e.g., when there are visitors at home.

All of our participants opted for a shared ownership model, i.e. they would like to share the ownership of the geo-fenced devices with the family members. 7 participants mentioned that they should have the control to impose or revoke the full ownership on demand basis. However, in contrast to previous research [11], our participants did not mention the need for variable accessibility (e.g., full or restricted access). For conflict resolution, i.e., when multiple persons want to interact with a GFS, 8 of our participants mentioned that it should be resolved by authority instead of proximity or first come first served basis, which is slightly in contrast to the interaction model with tangible controls.

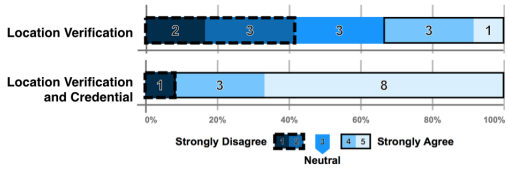

Figure 4: Feedback on verification credibility.

8 participants prefer the combination of location verification and credentials as a mechanism for gaining access to a GFS. Figure 4 illustrates their subjective assessment on credibility for two alternative approaches. A Wilcoxon Signed-Rank test ($Z = -2.4556$, $p < 0.05$) shows that there is a significant effect of the access control method on the user assessment of the system's credibility (perceived trust). Our qualitative interview also revealed that participants felt safer having both password- and location-based verification. However, it was observed from multiple remarks that for some geo-fenced devices (e.g., entertainment, cooking, etc) location verification on its own should be sufficient to manage the access control.

Concluding Remarks

As an increasing number of household devices is becoming connected, their control mechanisms are no longer physical. While this departure from physicality can benefit users, it also introduces opportunities for abuse. Geo-fencing is an interesting option for vulnerability protection by bringing back location constraints. To this end, we presented a witness-based access control protocol. Using a technology probe, we uncovered people's preferences for different design choices for GFS, which can be summarized into three design guidelines:

1. Infrastructure and safety devices are the best candidates for geo-fencing to enhance security and user experience.
2. Users should be given full flexibility to define the range and rules for geo-fences for different devices at home.
3. Location verification can be a usable access control mechanism besides password-based authentication, albeit the dependency on location witnesses requires connected devices to be shipped with additional components.

References

[1] iOS: Understanding iBeacon. http://support.apple.com/kb/HT6048.

[2] Kontakt ibeacon. http://kontakt.io.

[3] Nest. https://nest.com.

[4] node.js. http://nodejs.org.

[5] OpenID Authentication 2.0. http://openid.net/specs/.

[6] Philips Hue. http://meethue.com.

[7] The OAuth 2.0 Authorization Framework. http://tools.ietf.org/html/rfc6749.

[8] Bareth, U. Privacy-aware and Energy-efficient Geofencing through Reverse Cellular Positioning. In *Proceedings of IWCMC'12* (2012), 153–158.

[9] Brush, A. J. B., Lee, B., Mahajan, R., Agarwal, S., Saroiu, S., and Dixon, C. Home automation in the wild: challenges and opportunities. In *Proceedings of CHI'11* (2011), 2115–2124.

[10] Kawsar, F., and Brush, A. J. B. Home Computing Unplugged: Why, Where and when People Use Different Connected Devices at Home. In *Proceedings of UbiComp'13* (2013), 627–636.

[11] Kim, T. H.-J., Bauer, L., Newsome, J., Perrig, A., and Walker, J. Challenges in Access Right Assignment for Secure Home Networks. In *Proceedings HotSec'10* (2010).

[12] Kindberg, T., Zhang, K., and Shankar, N. Context Authentication Using Constrained Channels. In *Proceedings of WMCSA'02* (2002), 14–21.

[13] Luo, W., and Hengartner, U. VeriPlace: A Privacy-aware Location Proof Architecture. In *Proceedings of GIS'10* (2010), 23–32.

[14] Mennicken, S., and Huang, E. M. Hacking the Natural Habitat: An In-the-wild Study of Smart Homes, Their Development, and the People Who Live in Them. In *Proceedings of Pervasive'12* (2012), 143–160.

[15] Saroiu, S., and Wolman, A. Enabling New Mobile Applications with Location Proofs. In *Proceedings of HotMobile'09* (2009), 31–36.

[16] Sastry, N., Shankar, U., and Wagner, D. Secure Verification of Location Claims. In *Proceedings of WiSe'03* (2003), 1–10.

[17] Takayama, L., Pantofaru, C., Robson, D., Soto, B., and Barry, M. Making technology homey: Finding sources of satisfaction and meaning in home automation. In *Proceedings of UbiComp'12* (2012), 511–520.

[18] Zhu, Z., and Cao, G. APPLAUS: A Privacy-Preserving Location Proof Updating System for Location-based Services. In *Proceedings of INFOCOM'11* (2011), 1889–1897.