The Current State of Access Control for Smart Devices in Homes

Blase Ur
Carnegie Mellon University
bur@cmu.edu

Jaeyeon Jung
Microsoft Research
jjung@microsoft.com

Stuart Schechter
Microsoft Research
stus@microsoft.com

ABSTRACT

Although connected devices and smart homes are now marketed to average consumers, little is known about how access-control systems for these devices fare in the real world. In this paper, we conduct three case studies that evaluate the extent to which commercial smart devices provide affordances related to access control. In particular, we examine an Internet-connected lighting system, bathroom scale, and door lock. We find that each device has its own siloed access-control system and that each approach fails to provide seemingly essential affordances. Furthermore, no system fully supports user understanding of access control for the home. We discuss future directions for usable access control in the home.

Categories and Subject Descriptors

K.6.5 [**Management of Computing and Information Systems**]: Security and Protection

General Terms

Security

Keywords

Smart home, access control, connected devices, audit, Internet of Things, security policy, home automation

1. INTRODUCTION

We present case studies of the access-control systems of three home-automation devices: a wireless LED lighting system, a bathroom scale, and an electronic door lock. All three devices offer remote access via the Internet and are currently marketed to average consumers. Furthermore, these devices offer a range of capabilities and potential security and privacy concerns.

The promise of home automation is a familiar feature of science fiction now within reach of current technology. However, homes in which devices communicate with each other and provide remote monitoring and control features have yet to reach the mainstream. This promise may soon be realized, however, as Internet-connected household devices are increasingly being marketed to the general public. In the last few years, these devices have become more affordable, and the ubiquity of smart phones and ease of application development have offered new opportunities for remotely managing them. In just the past year, Belkin released the WeMo line of switches, motion sensors, and baby monitors that can be controlled by an iPhone [3]; Apple's retail stores began to stock light bulbs that can be controlled from a smart phone [24]; and the SmartThings project to build a unified home-automation controller raised over one million dollars on the crowdfunding site Kickstarter [25].

While the interactive features of connected devices can benefit users, they can also introduce opportunities for abuse. Pranksters might cause lights to turn on or off, robbers might disable automated doorlocks, and pedophiles might snoop on child-monitoring cameras (as posited by Denning et al. [9]). The access-control mechanisms familiar from decades of use in computing systems may not be appropriate for home environments and have not fared well when access-control systems designed for environments with professional administrators have been blindly copied into home applications. Researchers have only begun to explore the requirements of access control for home devices, using qualitative interviews exploring hypothetical situations [10,13] and the experiences of early adopters who might not be representative of the overall market [6, 19, 26].

We come at the problem from a different direction, looking at devices currently available to mainstream consumers. We examine how their designers have addressed, and in some cases failed to address, the design challenges of controlling access to capabilities that could be abused.

2. DEVICES STUDIED

We studied three types of home-automation devices that provide mechanisms for remote monitoring and control. These capabilities can be abused if they fall into the wrong hands. The devices have access-control requirements around remote monitoring of their state (the lock and light) and the readings they take from their environment (the scale). While the lighting system and door lock can be controlled remotely, necessitating access control for these capabilities, the wireless scale is controlled locally.

2.1 Variable-Color Lighting System
Philips Hue

The Philips Hue lighting system offers LED light bulbs that not only can be switched on and off and dimmed, but can also be instructed to produce colors throughout the RGB spectrum. They can be controlled via a website or smartphone application, empowering users to schedule future changes in lighting for both practical (e.g., turning on the lights in the morning) and aesthetic purposes.

Workshop on Home Usable Privacy and Security (HUPS) 2013, July 24–26, 2013, Newcastle, UK.

Potential abuses: monitoring and control

We included the Philips Hue in our case study because it has few capabilities that could be abused to cause severe security or privacy harms. An attacker who obtains the full capabilities of the owner will be able to turn lights on and off and change their color. With the exception of epileptic users vulnerable to exposure to flashing lights, users are unlikely to be physically harmed by changes in lighting. Lighting reductions would be no worse than sudden power outages. The risk of having private activities suddenly become more visible with the introduction of unwanted light is presumably already present if those who would be in view of those private activities possess a flashlight, though admittedly less detectable. Harassment attacks are similar to those possible if an adversary has access to a victim's phone number or doorbell. Finally, the ability to monitor lighting state could allow robbers or others to determine whether a room or home is currently occupied, which could already be divined less surreptitiously by an adversary standing across the street.

2.2 Wireless Scale
Withings WS-30

The Withings WS-30 scale measures users' weight and sends the results wirelessly to Withing's servers via either the user's home wireless network or the user's smartphone. Users can visit the Withings website to produce graphs showing weight changes over time, share progress with friends via social networks, or keep their doctor informed of any changes in their weight.

Potential abuses: monitoring

Sensitivity to revealing one's body weight and its variations differs widely between individuals, and may also vary within individuals depending on how they currently feel about their weight and their recent progress (or lack thereof) in reaching weight goals. The data collected by a scale may be considered especially sensitive by children, young adults, and others who may be exposed to environments in which mocking others' body weight is either tolerated or outright encouraged and socially rewarded. Thus, while it seems implausible that access-control failures in scales could lead to direct physical harm, these devices provide an excellent case study controlling information that may be highly privacy-sensitive, particularly when this data is both granular and longitudinal.

2.3 Keypad-Enabled Door Lock
Kwikset 910 TRL ZW (lock)
Mi Casa Verde Vera 3 (controller)

We complete our case study with wireless door locks. These devices are entrusted to protect owners' homes from unwanted intrusions, as well as to provide access reliably to family members and guests. 'Smart' door locks offer features like the ability to check whether a door is locked, lock it or unlock it remotely, and issue different access codes to different users. They also allow homeowners to limit the times during which regular domestic workers (e.g., cleaners) and infrequent maintenance staff (e.g., plumbers) can enter the house, give temporary access to guests and housesitters, and track comings and goings. Furthermore, they enable homeowners to grant access in unexpected situations, such as lockouts or emergency repairs, without needing to return home.

We examined the Kwikset 910 TRL ZW, which connects to a home-automation system wirelessly using the Z-Wave protocol. Z-Wave devices are accessed via Z-Wave controllers, which may act as hubs to control any number of devices within a home. We paired the Kwikset with the popular Mi Casa Verde Vera 3 controller. As is typical of Z-Wave devices, the Kwikset lock's user interface is provided by, and therefore dependent on, the controller.

Potential abuses: monitoring and control

The most salient means to abuse a door lock is to grant an attacker physical access to the home. Access-control failures could also allow attackers to lock household members out of the home, possibly at times that could be inconvenient or even dangerous to be stuck outside. Attackers who can monitor door locks may be able to determine whether or not a home is currently occupied and, with longitudinal data, may be able to estimate how long it is likely to remain unoccupied. Threats are not limited to outside adversaries; the ability to monitor who entered a code or unlocked the door at a given time can expose activities that household members consider private and would not want to share with each other.

3. DESIGN COMPARISON

In this section, we step through different dimensions of access control, comparing the access-control affordances of each of the three devices.

3.1 Configuring ownership

Users' first experiences with a new Internet-connected device likely involve connecting that device to their home network and choosing its settings. In this section, we detail the bootstrapping processes for our three devices, focusing on how the user establishes ownership over access to each device.

The lighting system we examined (Philips Hue) comes with a base station that must be connected via Ethernet to the home's router. The user then connects either a smart phone or tablet to the home network via Wi-Fi. After downloading the Philips Hue app, currently available for Android and iOS smart phones and tablets [24], the app searches the home network for the base station. Once the app locates the base station, the user takes ownership of the base station via the app, initiating a pairing protocol and pressing a button on the base station at a time specified by the app. From that point forward, accessing the app on this device transparently authenticates the owner to the base station. The user can then optionally create a password-protected account, enabling remote access to the Philips Hue via a website or over a smartphone's data network, rather than over a local Wi-Fi network [24].

The scale we examined (Withings WS-30) initially pairs itself with an owner's iPhone or Android app, doing so via the Bluetooth protocol. Whereas the designers of the lighting system opted to require that users connect the base station to the home network via Ethernet, the designers of the scale opted to require that users perform a Bluetooth pairing with a smartphone or tablet, on which they enter credentials for the home network. Only then does the scale establish a wireless connection to the home network. To perform the Bluetooth pairing, the user first presses a button on the bottom of the scale and then transitions to the phone to click "Withings WS30" on a Bluetooth device listing. The Bluetooth connection provides the necessary means to enter the credentials necessary for the scale to connect to the home network over Wi-Fi.[1]

In addition to pairing the scale with a smartphone or tablet app, users of the scale are also expected to create a password-protected account with the Withings web service, which will store all readings from the scale alongside user profiles that include height and body-type data. Users who cannot send this data over Wi-Fi can

[1]The scale does not support WPA Enterprise security, precluding us from connecting the scale to the Wi-Fi network during testing.

upload it indirectly via Bluetooth and the app, which then uses the smartphone or tablet's data connection to upload data to the Withings web service.

The door lock we examined (Kwikset 910 TRL ZW deadbolt), like the lighting system, communicates with a central controller that interfaces with the home network. In contrast to the lighting system, which has a specialized controller, the door lock connects to a general-purpose home-automation controller. The device and controller communicate over the Z-Wave wireless protocol, a non-proprietary wireless protocol designed primarily with home-automation systems in mind. Z-Wave controllers have full control (ownership) of devices that are paired with them. Pairing a door lock or other Z-Wave device with a controller requires the user to press a button on the Z-Wave device. The lock we examined provides a special button inside the interior-facing side of the device for pairing. The lack of additional barriers to pairing is somewhat concerning; someone allowed into the home temporarily could conceivably take ownership of the device by pressing the button and re-pairing the lock with a different Z-Wave controller.

By default, anyone on the same home network as the Z-Wave controller can control the user's home-automation system, though this setting can be changed to require a password [20]. Users can optionally also access the Z-Wave controller remotely by creating an account on the manufacturer's website during the setup process. The owner has complete control of all connected devices. In the case of the door lock, the username and password credentials grant the ability to query the status of the lock, lock or unlock the door, and add or delete access codes. Furthermore, independent developers have created apps for iOS and Android devices that enable remote operation of the Vera controller using these credentials.

3.2 Roles and Delegation

The home is a heterogeneous environment. Access-control policies must account for guests [12], children [4], and all manner of temporary workers and visitors [14]. As a result, we expected the devices we examined to provide rich and intuitive mechanisms for delegating different types of access to different people, yet our three case studies revealed a number of potentially conflicting paradigms.

The lighting system we examined offers only one role: ownership. As a result, delegating full access to other users necessitates either giving them the owner's username and password, or entering these credentials into an app running on the delegate's device. While remote access to a lighting system might initially seem superfluous, guests without remote access cannot control the lights over a smartphone's data connection or using the Hue website, even if they are physically present in the same room as the device. In this sense, access by any means other than the Hue app running on a device connected to the home's Wi-Fi network is considered remote.

Guests can, however, control the Hue without credentials if they already have both physical access to the Hue base station and access to the home's Wi-Fi network. After downloading the Hue app, a guest simply needs to press a button on the base station to pair that instance of the app with the Hue system permanently. Furthermore, if an individual Hue light bulb is plugged into a socket controlled by a light switch, individuals with physical access to the light switch can turn each bulb on to a solid white color by cutting and restoring power to the bulb, yet cannot control the bulb's color.

Given that the set of users for the Hue is likely to be a small group of people already resident or welcomed into the owners' home or onto the home network, this simple access-control model may be sufficient for many users. Users with existing access to a home or home network are likely capable of causing far more harm than is possible via changes to lighting. The biggest risk might come from

Figure 1: The scale is paired with a website that offers myriad options for sharing data. Some of these options, such as allowing a doctor to access data, confer ongoing access to data.

individuals who use a common password for the lighting system and for more sensitive accounts unwittingly sharing that password with guests who want to change the color of the lights.

The scale we examined can similarly be accessed via a shared account. However, it also offers support for users within the household to create separate password-protected accounts on the server, keeping their weight data private from each other [27]. Weights that fit that user's profile will only be available from that user's account, and historical weight data is not accessible on the scale itself.

In addition to offering user roles, the Withings website provides mechanisms for one-time sharing, such as posting status updates on social networking sites. It also supports sharing data on an ongoing basis, either via delegation of monitoring privileges to another Withings account or via a special link encoded in an email.[2] Figure 1 depicts the many options available to a user.

The door lock we examined is accessed via a Z-Wave controller, and the Z-Wave controller we tested offers three roles. Owners ("administrators") can control, monitor, and configure the door lock, as well as any other device accessed via the Z-Wave controller. A "guest" can control and monitor the lock and all other devices associated with the Z-Wave controller, but cannot save any new configuration settings. A "notification-only" user, as the name implies, can receive notifications selected by the owner, yet cannot control or configure the system [21]. Our tests with the Vera 3 revealed the implementation of these roles to be buggy in practice. For instance, the guest accounts and notification-only accounts we created were able to add and remove access codes for the lock's keypad, as well as to delete entries from the audit log. These limited accounts could not, however, link additional accounts to the controller.

Beyond these implementation issues, the theoretical model of access control adopted by this controller can lead to misalignments between users' mental models and the real world. Given the limited types of roles offered by the Vera interface, much of the delegation to guests occurs via the creation of codes for individual guests, or even multiple guests ostensibly filling the same role. The door lock

[2]Our attempts to test the latter option were unsuccessful; we always received an "account unknown" message, even though we chose the option for sharing with doctors without a Withings account.

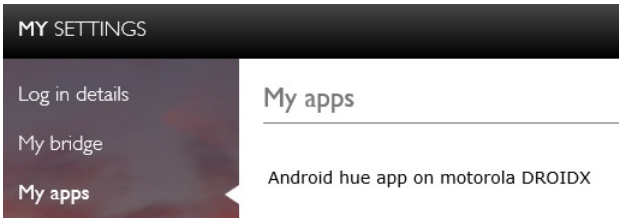

Figure 2: The Philips Hue authorization page, which lists associations between a particular Hue system and instances of the Hue app running on different models of smartphones.

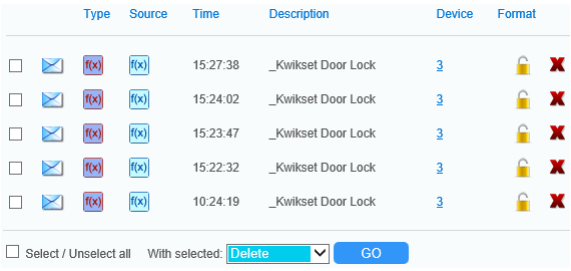

Figure 3: The lock's controller shows a log of past accesses.

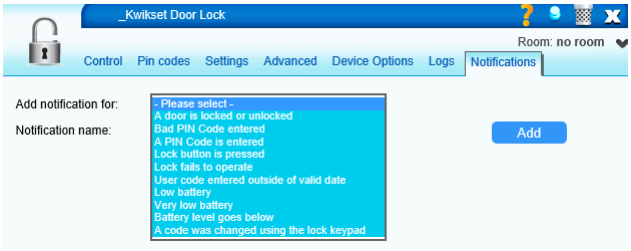

Figure 4: The lock's owner can request notifications for events including when the lock is actuated or has a low battery.

can be configured to limit the days of the week and hours of the day that codes can be used, and codes can be revoked. Notably missing is the ability for non-owners to delegate access to others. One could imagine household members who do not have ownership-level access, such as children, sharing their own entry codes with others because they are unable to create new ones for their friends.

Another potential hazard can result from the collision of two access control models: the roles built into the Z-Wave controller and the PIN codes built into locks. Codes do not represent a true user role, but exist solely to allow the lock to be opened from directly outside the door. Knowing a code does not endow an individual with the ability to access a device via Z-Wave, monitor the lock's state or past use, or access doors remotely. However, a user acting in the Z-Wave "guest" role should be allowed to control and monitor the device, but not change its configuration. That is, guests should be able to control and monitor the lock, but not make changes that would give them long-term access. Alas, disregarding implementation issues, the guest role would likely be able to view, but not change, the access codes of all existing users by examining access logs—hardly a capability most users would expect to grant to "guests."

3.3 Monitoring

As household devices are connected to the Internet, their control mechanisms are no longer purely physical. As a result, a light can turn on without anyone being present in the room, or a door could be unlocked remotely by an adversary without leaving visible signs of forced entry. Monitoring and audit mechanisms can give users transparency about what actions have occurred in the past, what the current state of the house is, and who can control which devices in the future. These mechanisms, however, go further in allowing individuals to track actions that have occurred in a house to an extent that was not previously possible.

The lighting system we examined can be monitored by the owner using the Hue website, as well as using a tertiary screen on the mobile app. Using the Hue website, the owner can view whether each light bulb is currently turned on or off, but not its color, intensity, or prior states. A screen three levels deep in the mobile app provides access to each bulb's current color and intensity, yet not any of its prior states, nor even how or when it was set to its current state. The Hue website, but not the mobile app, allows the owner to see a list of devices that have been granted access to the Hue, yet only lists the device model, as shown in Figure 2. Furthermore, in our tests, the Hue website only appeared to list devices into which a user had entered his or her account credentials to enable remote access. A guest could have paired his or her device with the Hue base station, gaining access to the Hue from within the same Wi-Fi network, yet not appearing in the audit interface.

The scale we examined, as a core function of its design, logs weigh-ins by sending them to its corresponding web service. However, like the lighting system, the overall system does not keep track of when these data are being monitored or analyzed. Users cannot determine whether their doctors are actually monitoring the data they are sharing, nor if the data they shared with a friend for support are now receiving hundreds of views.

The lock and controller we examined empower owners to monitor the comings and goings of their household by maintaining a log of accesses. However, the log does not indicate whether the door was locked or unlocked, which access code was used, nor whether the change in lock state was triggered in person via an access code or remotely via an app/website. Confusingly, lock icons appear in the log display, shown Figure 3, but are unrelated to physical locks. Instead, the lock icon 'locks' a particular entry to the display so that it will not scroll away.

A dashboard on the Vera web interface shows whether the lock is currently locked or unlocked, providing assurance that commands have been faithfully executed and that a home is safely locked. The lock can also be configured to blink an LED on the inside of the door red (locked) or green (unlocked) every five seconds so that individuals inside the home know the state of the lock. Furthermore, as shown in Figure 4, the owner can configure notifications to be sent via email or text message when any number of different events, ranging from successful entry to a low battery, occur. Thus, owners' email accounts could provide more detailed logs of recent activity than are available via the web service.[3] The owner can also view which access codes are currently active, as well as the days and times they are valid, via the web interface (Figure 5).

4. RELATED WORK

Internet-connected devices in smart homes present both benefits and risks for users. On the one hand, researchers have found in qualitative interviews that smart homes can be used to demonstrate success and power [17], help family members with special needs [8], ease the control of climate and irrigation systems [26],

[3]Unfortunately, we were unable to get the notification feature to work reliably during our tests.

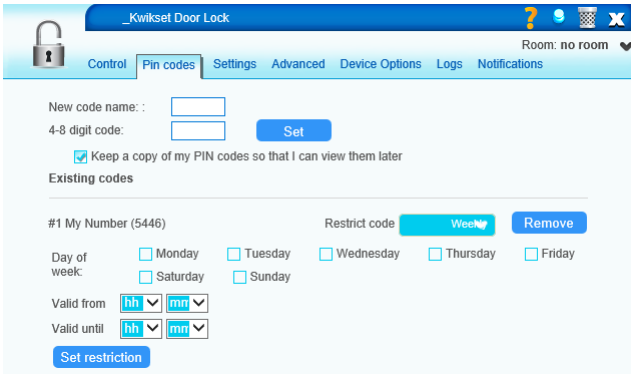

Figure 5: The lock's controller allows the owner to create access codes for in-person locking and unlocking of the door. The owner can limit the day of week and time of day that codes can be used, as well as revoke codes when necessary.

and save energy [19]. On the other hand, Internet-connected devices can create potential risks, allowing adversaries to capture users' private moments [7], disable security systems, or simply prevent users from accessing their devices [9].

In general, capturing access-control preferences in a usable manner is a complex task. Existing access-control systems in the real world handle exceptions and unexpected events poorly [2], and the distribution of tokens, such as physical keys, can be problematic [1]. Introducing access control to the home adds even more challenges, including the need to maintain a reliable system in the absence of a system administrator [11]. Even for systems focused on sharing or replicating data in the home, users' mental models of access control are often misaligned with actual systems, and users have complex policies that they try to implement through ad-hoc mechanisms [18]. Implied trust relationships and the diversity of data in the home make domestic access-control decisions particularly complex [16], and differing trust relationships with neighbors can impede the sharing of sensors with nearby houses even when sharing is potentially beneficial [5]. Many home users wish they had greater visibility into what is happening on the home network, yet this affordance can introduce subtle privacy concerns [23].

A handful of researchers have conducted formative studies investigating what access-control affordances might be necessary for smart homes. Based on interviews with 14 households that already use home automation, Brush et al. identified the difficulty of achieving security as a primary barrier to the adoption of home automation [6]. Their participants identified temporary access and access based on presence as important affordances. Although participants also desired remote access, this particular affordance raised many concerns. Kim et al. explored access control for smart homes by interviewing 20 individuals without smart homes [13, 14]. They proposed physical presence, logging, and the ability to ask for permission as useful dimensions of access-control policy.

A handful of additional affordances appear potentially useful for smart homes. Users would want to set access-control rules based on time, as well as limit applications' access to particular devices [10]. Allowing guests to access certain devices in a smart home is both important and potentially complex [12], as is specifying policies for shared devices [15]. Giving users feedback about the data monitored by household sensors could allay users' privacy concerns, yet also be onerous [22]. Compared with the more hypothetical approaches taken in past work, we focus on the access-control affordances popular smart devices actually provide to consumers.

5. CONCLUSIONS

Across our three case studies, we noticed a number of challenges and opportunities for supporting access control. First of all, the three devices differed in their mechanism for users to establish ownership of the device. While the Withings scale required a bluetooth connection, the Philips Hue required connecting a hub to a router and pressing a button, and the Kwikset lock involved opening a compartment on the lock and pressing a pairing button after initiating a pairing process on the home's Z-Wave controller. Most alarmingly, the lock did not prevent anyone with physical access to that button to pair the lock with their own Z-Wave controller, creating a security risk. To improve usability, each device could have the same mechanism for establishing ownership.

Each device also provides different mechanisms and modalities for access control, and this gallimaufry of models can cause confusion for users, potentially leading to configurations that are misaligned with mental models. Access is sometimes available by default to everyone on the same network (lock), and sometimes to everyone on the same network who has paired with the device (lighting system). However, sometimes being on the same network is irrelevant to access control (scale).

All three devices permit the owner to create an account, comprising a username and password, to control access to the device. However, the lighting system also allows anyone with physical access to a bulb to turn it on and off, and anyone on the same wireless network and with physical access to the base station can control the lights without appearing in an audit log of devices associated with the system. The lock instead allows individuals to use PIN codes to open the lock, yet does not appear to distinguish between PIN codes and remote access in audit logs.

Even the roles available for accounts differ across devices. The lighting system can have only one account associated with it, potentially leading users to share passwords that they reuse elsewhere. The scale allows multiple users of a single device to have their own accounts. While these accounts can be configured to share data with each other, this sharing is smartly turned off by default. The scale also claims to grant access to users without accounts via email links, although we could not get this feature to work during our tests. The lock and associated controller allow administrator, guest, and notification-only accounts to be made, yet subtleties about the exact functionality given to guests can derail the entire access-control system.

Sharing access to smart devices with other users and with guests can be complicated, yet guests [12], children [4], and temporary workers [14] are not new problems. In comparing the sensitivity of the devices from our case studies with the mechanisms they provide for sharing access, a series of tiers becomes clear. For low sensitivity devices with high availability requirements, such as lighting or heating systems, providing physical buttons that let anyone in close proximity control the device likely solves the problem. For instance, the Philips Hue's affordances for turning the lights on by cutting power to the device, or by joining a home network, seem reasonable. Once sensitive data, such as the output from a security camera, or sensitive actions, such as turning off the water to a home, come into play, the problem of access control becomes much more nuanced. We did not observe an easy-to-use way to delegate access to a device across any of our three case studies.

A major shortcoming we observed across all three devices was a lack of mechanisms for monitoring access. Neither the Philips Hue nor the Withings scale provide user-facing audit mechanisms, making it impossible for users to understand who has accessed their devices. While one could argue that these two devices are not sufficiently sensitive to require access to a log, audit functionality ap-

pears particularly desirable for wireless door locks. Alarmingly, the availability of an audit mechanism for the door lock we tested depends on the Z-Wave controller used with it, and we encountered numerous usability flaws with the controller we tested. We find this issue problematic as audit mechanisms are crucial for understanding both past accesses and the potential for future accesses.

Furthermore, each of the three devices in our case study operates within its own silo. To control the Philips Hue, the Withings scale, and the Kwikset lock currently requires separate accounts with Philips, Withings, and the home's Z-wave controller. While having a separate system for each device enables differing access-control affordances that align directly with each device's sensitivity and use cases, the tasks we have discussed in the preceding paragraphs become much more difficult. A handful of groups are working to develop universal hubs for smart homes, such as HomeOS [10] and Smart Things [25], and these hubs have the potential to present a single access-control regime. However, given the paucity of usability research into access control for smart homes, the ideal design for such a unified access-control system remains to be determined.

6. REFERENCES

[1] L. Bauer, L. Cranor, R. W. Reeder, M. K. Reiter, and K. Vaniea. A user study of policy creation in a flexible access-control system. In *Proc. CHI*, pages 543–552, 2008.

[2] L. Bauer, L. F. Cranor, R. W. Reeder, M. K. Reiter, and K. Vaniea. Real life challenges in access-control management. In *Proc. CHI*, pages 899–908, 2009.

[3] Belkin. Belkin expands WeMo family... `http://www.belkin.com/us/pressreleases/8798223729724`, Accessed 5/24/13.

[4] A. B. Brush. It's use by us: family friendly access control. In *Technology for Today's Family Workshop at CHI*, 2012.

[5] A. B. Brush, J. Jung, R. Mahajan, and F. Martinez. Digital neighborhood watch: investigating the sharing of camera data amongst neighbors. In *Proc. CSCW*, pages 693–700, 2013.

[6] A. B. Brush, B. Lee, R. Mahajan, S. Agarwal, S. Saroiu, and C. Dixon. Home automation in the wild: challenges and opportunities. In *Proc. CHI*, pages 2115–2124, 2011.

[7] E. K. Choe, S. Consolvo, J. Jung, B. Harrison, and J. A. Kientz. Living in a glass house: a survey of private moments in the home. In *Proc. UbiComp*, pages 41–44, 2011.

[8] E. K. Choe, S. Consolvo, J. Jung, B. Harrison, S. N. Patel, and J. A. Kientz. Investigating receptiveness to sensing and inference in the home using sensor proxies. In *Proc. UbiComp*, pages 61–70, 2012.

[9] T. Denning, T. Kohno, and H. M. Levy. Computer security and the modern home. *Commun. ACM*, 56(1):94–103, Jan. 2013.

[10] C. Dixon, R. Mahajan, S. Agarwal, A. J. Brush, B. Lee, S. Saroiu, and P. Bahl. An operating system for the home. In *Proc. NSDI*, 2012.

[11] W. K. Edwards and R. E. Grinter. At home with ubiquitous computing: seven challenges. In *Proc. UbiComp*, pages 256–272, 2001.

[12] M. Johnson and F. Stajano. Usability of security management: Defining the permissions of guests. In *Proc. Security Protocols Workshop*, 2006.

[13] T. H.-J. Kim, L. Bauer, J. Newsome, A. Perrig, and J. Walker. Challenges in access right assignment for secure home networks. In *Proc. HotSec*, 2010.

[14] T. H.-J. Kim, L. Bauer, J. Newsome, A. Perrig, and J. Walker. Access right assignment mechanisms for secure home networks. *Journal of Communications and Networks*, 13(2):175–186, April 2011.

[15] K. Kostiainen, O. Rantapuska, S. Moloney, V. Roto, U. Holmström, and K. Karvonen. Usable access control inside home networks. Technical Report NRC-TR-2007-009, Nokia Research Center, April 2007.

[16] V. Lekakis, Y. Basagalar, and P. Keleher. Don't trust your roommate or access control and replication protocols in "home" environments. In *Proc. HotStorage*, 2012.

[17] A. B. Lynggaard, M. G. Petersen, and S. Hepworth. "I had a dream and I built it": power and self-staging in ubiquitous high-end homes. In *CHI Extended Abstracts*, pages 201–210, 2012.

[18] M. L. Mazurek, J. P. Arsenault, J. Bresee, N. Gupta, I. Ion, C. Johns, D. Lee, Y. Liang, J. Olsen, B. Salmon, R. Shay, K. Vaniea, L. Bauer, L. F. Cranor, G. R. Ganger, and M. K. Reiter. Access control for home data sharing: Attitudes, needs and practices. In *Proc. CHI*, pages 645–654, 2010.

[19] S. Mennicken and E. M. Huang. Hacking the natural habitat: an in-the-wild study of smart homes, their development, and the people who live in them. In *Proc. Pervasive*, pages 143–160, 2012.

[20] Mi Casa Verde. Security. `http://docs2.mios.com/doc.php?platform=0&language=1&manual=1&page=security`, Accessed 5/24/13.

[21] Mi Casa Verde. MiOS. `http://docs5.mios.com/doc.php`, 2013.

[22] S. Moncrieff, S. Venkatesh, and G. West. Privacy and the access of information in a smart house environment. In *Proc. MM*, pages 671–680, 2007.

[23] R. Mortier, T. Rodden, P. Tolmie, T. Lodge, R. Spencer, A. crabtree, J. Sventek, and A. Koliousis. Homework: putting interaction into the infrastructure. In *Proc. UIST*, pages 197–206, 2012.

[24] Philips. Hue. `https://www.meethue.com`, Accessed 5/23/13.

[25] SmartThings. Make your world smarter. `http://www.kickstarter.com/projects/smartthings/smartthings-make-your-world-smarter`, Accessed 5/24/13.

[26] L. Takayama, C. Pantofaru, D. Robson, B. Soto, and M. Barry. Making technology homey: finding sources of satisfaction and meaning in home automation. In *Proc. UbiComp*, pages 511–520, 2012.

[27] Withings. About the scale. `http://www.withings.com/en/wirelessscale/faq`, Accessed 5/28/13.