Enabling Multi-user Controls in Smart Home Devices

William Jang, Adil Chhabra
Amherst College

Aarathi Prasad
Skidmore College

ABSTRACT

The Internet of Things (IoT) devices have expanded into many aspects of everyday life. As these smart home devices grow more popular, security concerns increase. Researchers have modeled the privacy and security threats for smart home devices, but have yet to fully address the problem of unintended user access within the home. Often, smart home devices are purchased by one of the family members and associated with the same family member's account, yet are shared by the entire home. Currently most devices implement a course-grained access control model where someone in the home either has complete access or no access. We provide scenarios that highlight the need for flexible authorization control and seamless authentication in IoT devices, especially in multi-user environments. We present design recommendations for IoT device manufacturers to provide fine-grained access control and authentication and describe the challenges to meeting the expectations of all users within a home.

CCS CONCEPTS

• **Security and privacy → Authentication**; **Access control**; **Authorization**; • **Human-centered computing → Interaction techniques**; **User interface design**; **Ubiquitous and mobile devices**;

KEYWORDS

IoT, smart home, security, authentication, authorization, access control

1 INTRODUCTION

In recent years, the Internet of Things (IoT) devices have expanded into many aspects of everyday life. In particular, IoT devices have revamped the home automation industry in the form of the *smart home*. Smart home devices are defined as "network-connected products (i.e., "smart products," connected via Wi-Fi, Bluetooth or similar protocols) for controlling, automating and optimizing functions such as temperature, lighting, security, safety or entertainment, either remotely by a phone, tablet, computer or a separate system within the home itself" [29]. Common examples include the smart thermostat (such as Ecobee [14]), refrigerator (such as the Samsung Family Hub [33]), lights (such as the Philips Hue [31]), and smart home assistants (such as the Amazon Echo [3]).

IoTS&P'17, November 3, 2017, Dallas, TX, USA

ACM ISBN 978-1-4503-5396-0/17/11…$15.00
https://doi.org/10.1145/3139937.3139941

As these smart home devices grow more popular, security concerns increase [1]. For example, the Amazon Echo provides a voice user interface through which a user can order goods, play content, or even control other smart home devices [3]; the voice user interface incorporates a microphone that is always on and continuously listening for user input. Researchers have modeled the privacy and security threats for smart home devices [9, 30, 39], but have yet to fully address the issues that arise when supporting unintended user access within the home. Often, smart home devices are purchased by one of the family members and associated with the same family member's account, yet are shared by all other residents in the home; we refer to the user whose account is associated with the device, henceforth, as the *primary* user. Furthermore, currently most devices implement a coarse-grained ("all-or-nothing") access control system where all users either have complete access or no access [9]. The Amazon Echo, for example, might schedule events or read texts of the primary user, but given the coarse-grained access control mechanisms, any family member can access this data. Also if the primary user's account has a credit card associated with it, anybody within the home, including children, guests or roommates, can make a purchase inadvertently or deliberately.

Most smart home devices have multiple users with different expectations from the same device; we highlight several such scenarios in Section 2. One potential solution could be for devices to support multiple profiles with different privileges and customizable settings, ensuring that multiple users within a home can expect secure, personalized access to the same device. However, it is not sufficient to just provide support for multiple users, but the smart devices also need to provide flexible and usable authentication mechanisms that allow users to switch profiles effortlessly.

In this paper, we make the following contributions.

- We provide scenarios that highlight the need for fine-grained access control and seamless authentication mechanisms in IoT devices, especially in multi-user environments such as the smart home.
- We identify the device goals and the challenges to meeting the expectations of all users within a home.
- Finally, we present design recommendations for IoT device manufacturers to provide fine-grained access control and seamless authentication.

2 SCENARIOS

In this section, we provide scenarios that highlight the challenges that arise with smart devices in multi-user environments; the first two scenarios highlight authentication issues and the latter two highlight authorization issues.

Scenario 1: Malicious access from family members. Charlie recently purchased an Amazon Echo for his family. He links the device to his Amazon account; to prevent accidental purchases, he

sets up a voice purchasing PIN. His son, Evan, overhears the pin and orders a new gaming console using Amazon Echo, without Charlie's knowledge. Charlie is surprised to find a brand new Nintendo Switch two days later, as he missed the purchase confirmation e-mail from Amazon.

Scenario 2: Inadvertent access by guests. Mallory visits David and Betty's home. During dinner, Mallory wants to make a phone call, but since her phone ran out of battery, she borrows Betty's phone instead. During her call, Mallory walks past the bedroom door; the smart lock on David and Betty's bedroom recognizes Betty's phone and unlocks the door.

Scenario 3: Frustration with coarse-grained authorization among roommates. Alice and Eve are first-year college students who are assigned to the same room; Alice offers to share her gaming device with Eve but sets up a guest account rather than a primary account for Eve whenever they play together; a guest account gets deleted on logout, requires a primary user to play, and cannot edit saved data. Alice wants to be able to restrict Eve's ability to edit saved data, while still allowing Eve to play games and other content. Because she does not trust Eve enough yet to give her a primary user account, Eve is forced to continually use the guest account with limited access.

Scenario 4: Frustration with authorization and precedence among home sharers. Bob lends his home to travelers for extended periods of time through a home sharing service. As Charlotte will be staying with Bob for over a month, Bob decides to create a separate account for Charlotte on all of his smart home devices. Much to his displeasure, Bob finds Charlotte changed Bob's settings in a manner that even Bob could not use his own devices; Bob had given Charlotte administrator privileges since she was also a resident in the house.

As described in the scenarios, inefficient authentication techniques and a lack of flexible access controls may provide unauthorized users privileged access to the primary account.

3 RELATED WORK

Prior research shows that users are willing to share their smartphones and we expect similar behavior with smart home devices. Hang et al. discovered that smartphone sharing was usually impromptu and that users were more willing to share if it were easier and subtler to change into a guest profile that had restricted access to the phone [19]. We propose that IoT devices should implement a guest profile with least privilege access, similar to xShare, which creates a virtual environment with limited functionality through which a guest can interact [23].

Matthews et al. and Karlson et al. found that trust and convenience factored most heavily in the decision to share a device [22, 25]. Jacobs et al. discovered that couples tend to trust one another more than other residents in the home; however, they also found instances where a partner would withhold information from the other or would snoop on the other, causing conflict [21]. We propose IoT devices need separate profiles for all residents in the smart home.

Researchers have looked at how different users weighed the cost of locking or switching profiles when sharing a device, and found that usually, current solutions require too much effort on the user's part [6, 8, 15, 16, 32]. We expect users will have similar concerns with their smart home devices and hence, require an effortless way to switch profiles in IoT devices.

Devices that implement the SmartThings API support multiple users within a home; however, all users are granted the same privileges as the primary owner [36]; our scenarios clearly show the need for different privileges. Prior research also observes the negative impact of the coarse-grained access control mechanism on device or account sharing [9, 13, 19, 22, 32]. Researchers have proposed attribute-based access control mechanisms for mitigating the trust and convenience issues [23, 28]; we expect attribute-based mechanisms will be useful even in smart home devices where primary users can assign certain attributes or roles to other users [2, 7, 10, 18, 20, 35].

4 USER PROFILES

In this paper, we primarily focus on the issues that arise due to multiple users using the same device in the same house. If the device does not behave according to their expectations, the users may be frustrated. We classify the device goals as follows.

Device goals.

Functionality: The user expects the device to cater to their functional needs. For example, a smart lock lets them enter their house or room, a smart coffee maker makes coffee according to their preference, and a smart home assistant allows them to control other smart devices, respond to queries or make purchases. The user should be able to easily specify their functional needs on the device. For current devices, this step is done via a smartphone application on the primary user's phone.

Access: The user expects the device to allow authorized users differing levels of privileges, based on their role. Most existing IoT devices lack the controls for users to specify privileges for other users and the techniques to correctly identify and authenticate or deauthenticate them.

An IoT device in a smart home should be able to support multiple users by providing them ways to customize the device to meet their functional needs and control access privileges of certain users. The primary user might want to identify the different users and restrict the tasks other users can perform with the device, i.e., grant them certain privileges. Traditionally, role-based access control models are used for managing privileges and we expect similar models should suffice even in the case of smart IoT devices in the home.

Challenges. Before we describe the different profiles for smart home devices, we refer to the scenarios to understand what challenges multi-user environments face.

Role of the smartphone: Typically, users rely on the smartphone to specify their functional preferences. Smartphones can provide additional hardware for authentication as well

as convenience for some users, but they can also complicate the situation as some devices are completely dependent on the smartphone application. This means users might not be able to switch profiles without having access to their smartphone. What role should the smartphone play? What design challenges will device manufacturers face if they attempt to add profile switching directly to the device? We discuss this in Section 5.

Auto-login to primary account: For convenience, devices allow the primary user to easily authenticate to their account. However, this makes it easier for non-primary users to use the same account, even without the knowledge of the primary user. For example, in Scenario 1, 3 and 2, other users were easily authenticated as the primary user. How can we make it effortless for the primary user to authenticate, but also make it difficult for others to authenticate as the primary user?

Authentication with regards to the environment: How do we choose an authentication technique that is effortless, and yet, difficult to mimic? An adversary may steal the password by eavesdropping when the primary user is saying the password aloud (Scenario 1) or observe the device screen when a primary user is typing a password (Scenario 3). Alternately, a non-primary user may also obtain the token that is used to authenticate to the device, such as the smartphone of the primary user in Scenario 2. Clearly, authentication methods should be chosen after understanding the environment in which the device must be used.

Lack of flexible access controls: The primary user may want to limit the privileges given to other users, but most existing devices do not have flexible controls to support multi-user access.

Evaluating roles. Based on usage scenarios, we identify four different roles for IoT devices; the roles are described in Table 1.

Primary user: The primary user's account is set up with the device. The user should have all the privileges to the device.

Alternate primary users: In certain scenarios, there may be more than one primary user, because they are granted the same privileges as the primary user. Typically, a significant other or a trustworthy roommate can be an alternate primary user. For example, Bob was the primary user in Scenario 4 and Charlotte was an alternate primary user.

Secondary users : The secondary users have restricted privileges; their interactions of the device are limited by one of the primary users. Extended guests, such as Charlotte in Scenario 4, could be given secondary user status. Children, or untrustworthy roommates may be secondary users. Primary users who are parents, may also want to use parental controls (if available) to filter the tasks that children may perform with the device. Primary users may also grant on-demand privilege requests, if a secondary user needs temporary privilege access.

Guests : Guests, i.e., people who visit but do not reside in the home may want to use certain devices to a minimal extent. For example, they may want to interact with Alexa on the Amazon Dot and ask about the weather or play a song. This role is similar to the guest accounts already available on laptops.

Role	Description
Primary User	Main user whose account linked with device
Alternate primary users	Significant other
Secondary users	Children, roommate, renter
Guests	Visitors, other unauthorized users

Table 1: Roles for IoT devices

Privilege	Description
High	purchases, access sensitive information
Medium	change settings
Low	public information

Table 2: Various actions by IoT device users classified as privileges

Evaluating privileges. Next, we identify the different privileges associated with IoT devices that may be granted to the different roles and group them as high, medium and low risk; the privileges are identified in Table 2.

High risk: Functionality that may lead to an unwanted, irreversible situation is classified as high risk (i.e. an attacker looking at emails, ordering goods, revoking access for users). Users granted these privileges may be able to perform sensitive actions such as making purchases, accessing private information and assigning roles and privileges to other users.

Medium risk: Functionality that pertains to managing one's own account and settings is classified as medium risk (i.e. creating playlists, changing coffee brew settings). Users granted these privileges may be able to access the functional control settings and specify their functional expectations via a mobile application.

Low risk: Functionality that features public information or has little consequence is classified as low risk (i.e. listening to music, providing the weather). Users granted these privileges may only be able to access minimal information from the device, such as information that is available to anyone who visits the house.

Access to information could be high or medium risk depending on the device and the role. The risk differs also based on the *sensitivity* of information that can be obtained by a user via the device, as perceived by the primary user. Several factors affect the sensitivity of information, for example, who uses the device, where the device is located in the house, what accounts the device is linked to, what information it collects, and what it stores. For example, the information collected by a smart home assistant may be much more sensitive than that collected by a smart thermostat; the primary user may want to allow a guest to obtain the current temperature, which they may know even without accessing the thermostat, but the primary user may not want the guest to access her credit card account linked to the smart home assistant.

Defining profiles. A profile is defined by the user's role, the user's functional settings and the set of privileges assigned to the user. Typically primary and alternate primary roles will be assigned

high-risk privileges, secondary roles will be assigned medium-risk privileges and guest roles will be assigned low-risk privileges.

Several existing systems could be used in providing the hierarchical access control necessary for fine-grained authorization. Specifically, systems developed by Goyal et al. and Bethencourt et al. provide fine-grained attribute based encryption systems that would authorize users based on the attributes defined in their respective profiles [7, 18]. Both of these ciphertext policy (CP-ABE) and key policy attribute-based encryption (KP-ABE) cryptosystems are very resistant to collusion.

Other CP-ABE and KP-ABE systems could be extended to incorporate existing access control languages similar to XACML and OAuth [34]. This combination would allow primary users to specify which users could use which functions. Furthermore, uses of XACML and OAuth would allow for primary users to authenticate other roles based on time or request from another user.

This type of functionality would be best suited for the smartphone. Users could define their profile on their smartphone, as well as manage other profiles in the household.

We next explore ways to support profile switching in the device so users can easily authenticate to their profiles. Even if the devices allow users to define profiles and provide flexible access control mechanisms, users may disable security options and find workarounds if the users cannot authenticate to their profile effortlessly. How can we improve the design of IoT devices so users can easily authenticate to their profiles?

5 DESIGN

Typically, IoT device users use a mobile application on their smartphone to control their device and manage accounts. If a device is used by multiple users, often the mobile application will support multiple accounts. When Alice wants to use the device, she has to login to her account on the application in order to use the device as Alice.

While smartphones are well suited for managing and defining smart home device profiles, switching can become a hassle, particularly for users who, for whatever reason, do not have access to their smartphone. If Alice's smartphone is unavailable when she wants to use the device, she may have to borrow a family member's smartphone or log into her computer, all the while keeping track of several different login combinations for her smart home device accounts. For a device that boasts convenience, having to rely on a smartphone to use it may make the user experience less desirable.

Instead, we explore different ways to leverage input modalities on devices for enabling effortless multi-user authentication. We chose these modalities based upon what we have seen in existing literature and industry.

Passwords/PIN: The user can switch profiles by entering a user-specific PIN or password on the device.

Touch: A user can press a button on the device or on a screen to switch profiles quickly. Alternately, fingerprint readers could be incorporated in devices, such as the controllers in Scenario 3; when Eve holds the controller, the device obtains Eve's fingerprint and tries to match his fingerprint with that of the authorized user Alice; when the fingerprint does not match, the device logs him into his guest profile.

Microphone: Devices can record a user's voice using a microphone and identify the user using voice recognition algorithms, or custom voice commands. A voice command would provide a quick, and hands-free way to switch profiles, which would be especially helpful if the user does not have access to smartphones. The devices in Scenarios 1, 3,and 2 all currently contain microphones, so voice recognition algorithms can be easily incorporated without any hardware change. Google Home has implemented voice recognition, but it can be fooled with recordings [12, 17]. Amazon Echo allows users within a household to switch between multiple profiles using voice, but offers no voice recognition authentication; any user can switch into any profile by simply saying "switch accounts" [4].

Camera: A camera on the device can allow automatic face recognition or support custom hand gestures to allow quick profile switch. Certain smart locks already have camera support; users may want smart locks to record every visitor to the home. Facial recognition would maintain the same hands-free access for a smart lock, but also prevent accidental access like that in Scenario 2. Smart locks, doorbells, and DIY security systems can use facial recognition to maintain separate profiles for household members as well as allow guests into the home at certain time periods [11, 27, 37].

Proximity: Devices can leverage Bluetooth scans to identify users nearby by detecting their smartphone or wearable device and immediately switch to their profile. In a controversial move, a company based in Wisconsin implanted RFID-enabled chips into volunteers' hands, enabling them to authenticate with smart devices through proximity [5]. BLE wearables can also make authentication easier without the need for biometric hardware or smartphones in Scenario 2.

Combination: Devices can also use a combination of two or more different modalities to authenticate. For instance, Momo, a smart home assistant, has a camera to provide facial recognition and a microphone for voice commands [26]. Other systems might combine different modalities to provide multi-factor authentication for stronger security. For instance, in Scenario 1 and 2, the devices could implement a two-step authentication technique using both a PIN and voice recognition.

Smartphone: Although these input modalities are supposed to be added to the device itself to provide profile switching functionality without dependence on the smartphone, the smartphone, if available, could extend the combination section to provide multi-factor authentication. The new iPhone X will feature an A11 chip that will facilitate artificial intelligence software that could be used for biometric authentication [38]. This solution would decrease the strain put on the processor and battery as well.

Caveats. It may be tempting to add the above input methods to IoT devices given the possibilities they offer in terms of effortless authentication, but we also need to weigh the potential disadvantages of incorporating these modalities.

Privacy: Users may be concerned about a microphone or camera that is constantly recording and feeding information to

the cloud, even though the devices may be using the microphone and camera feed only for voice and face recognition respectively. Also, the feed is typically sent to the cloud, so an external adversary could obtain the recordings when they are sent to the cloud or from the user's account in the cloud.

Additional Hardware: Adding input modalities to the device can make the device bulky and also increase its cost, which could lead to fewer sales.

Resource Consumption: Microphones, cameras, and proximity sensors increase the processing load and power consumption on the device since it has to not only support complex sensing algorithms but also support voice, facial, and spatial recognition algorithms respectively. This could be especially problematic as many smart home devices are constantly on, listening for input. Also, the developers must implement multiple complex algorithms in the resource-constrained device; however, Mathur et al. proposes ways to address the challenges that arise when implementing multiple deep learning models in IoT devices [24].

False positives: Authentication methods may not always work according to the developer's expectation. Using Bluetooth scans to sense if a user's smartphone is close by makes it convenient to unlock doors using smart locks, however, it assumes that only the authorized user will have access to the device.

Usability: Adding more controls might also affect the user experience, so device manufacturers need to conduct several usability studies before adding additional modalities to the device.

Despite the caveats, we expect device manufacturers should consider adding input modalities on the devices to provide seamless authentication for multi-user access while smartphones can be used for providing authorization privileges. But before choosing the modalities, the manufacturers need to better understand the device usage environment, such as the roles of the users, their functional needs and appropriate privileges.

6 RECOMMENDATIONS

In this section, we explore ways to improve authorization and authentication in smart home devices.

Authorization. When a user purchases and sets up a device in her home, she sets up an account on the device and registers herself as the primary user by accessing the application or website for the device on her smartphone or laptop. She can then specify her preferred settings for the device. She can also create roles for all the other users on the same application or website. For example, her significant other could be an alternate primary user, her children, roommates or renter could be a secondary user and everyone else could be considered to be guests. She defines different privileges for the users - alternate primary users could be assigned high-risk privileges, secondary users medium-risk privileges and guests low-risk privileges. It should also be possible for her to allow on-demand privilege escalations to secondary users or guests, under certain circumstances.

For example, consider smart home assistants. Alice purchases an Amazon Echo Dot and sets it up to work with her Amazon account. She allows her husband to also make purchases through her account. Her children can request to play songs, but not purchase songs not in the library. But suppose, her children's nanny (also a secondary user) wants to purchase a song on the children's behalf; Alice may receive a privilege escalation request on her smartphone and she can grant the nanny temporary privileges to purchase an item.

Authentication. We also need to consider authentication techniques for multiple users. If authentication is not seamless, users may get frustrated and disable the access control mechanisms.

Smartphones have replaced remotes and can be used to control most current smart home devices. However, if you do not have access to your smartphone, you may have to find the smartphone of an alternate primary user that is authorized to control the device or use the buttons on the device itself to control it. An alternate option is to improve the design of the device to allow a user to authenticate to the device. For example, voice and face recognition techniques can be ideal on devices that provide high-risk functionalities. Since users may be concerned about privacy when using these mechanisms, the device should also give some feedback for when the mechanisms are in use.

For example, in Amazon Echo, users can give voice commands and the user is aware of when the device is listening since the device shows a red light when the microphone is off. We expect providing additional feedback such as an upload icon that blinks when the device is sending data to the server will help reduce privacy concerns.

Even though we make the above suggestions, we recommend device manufacturers conduct focus groups and interviews with real users to better understand the environment in which the devices will be used, so they can weigh the pros and cons of using the different modalities in the devices, before adding them to the devices. As future work, we plan to conduct user studies to better understand the issues that arise in multi-user environments.

7 SUMMARY

In this paper, we provide scenarios that highlight the need for seamless and flexible access control and authentication in IoT devices, especially in multi-user environments. We present design recommendations for IoT device manufacturers to provide fine-grained access control and authentication and describe the challenges to consider when adding input modalities to the devices.

ACKNOWLEDGMENTS

We wish to thank the anonymous reviewers for their valuable insights and feedback.

REFERENCES

[1] ABIresearch. 2017. Smart Home. https://www.abiresearch.com/market-research/service/smart-home/. (April 2017).

[2] Joseph A. Akinyele, Matthew W. Pagano, Matthew D. Green, Christoph U. Lehmann, Zachary N.J. Peterson, and Aviel D. Rubin. 2011. Securing Electronic Medical Records Using Attribute-based Encryption on Mobile Devices. In *Proceedings of the ACM Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)*. ACM, 75–86. https://doi.org/10.1145/2046614.2046628

[3] Amazon. [n. d.]. Amazon Echo. https://www.amazon.com/Amazon-Echo-Bluetooth-Speaker-with-WiFi-Alexa/dp/B00X4WHP5E. ([n. d.]).

[4] Amazon. 2017. Household Profiles on Alexa. https://www.amazon.com/gp/help/customer/display.html?nodeId=201628040. (2017).

[5] Maggie Astor. 2017. Microchip Implants for Employees? One Company Says Yes. *New York Times* (July 2017).

[6] E. Bardram. 2005. The Trouble with Login: On Usability and Computer Security in Ubiquitous Computing. *Personal and Ubiquitous Computing* 9, 6 (Nov. 2005), 357–367. https://doi.org/10.1007/s00779-005-0347-6

[7] John Bethencourt, Amit Sahai, and Brent Waters. 2007. Ciphertext-Policy Attribute-Based Encryption. In *Proceedings of the IEEE Symposium on Security and Privacy*. IEEE Computer Society, 321–334. https://doi.org/10.1109/SP.2007.11

[8] A. J. Bernheim Brush and Kori M. Inkpen. 2007. Yours, Mine and Ours? Sharing and Use of Technology in Domestic Environments. In *Proceedings of the International Conference on Ubiquitous Computing (UbiComp)*. Springer-Verlag, 109–126. https://doi.org/10.1007/978-3-540-74853-3_7

[9] Marta E. Cecchinato and Daniel Harrison. 2017. Degrees of Agency in Owners & Users of Home IoT Devices. In *ACM CHI 2017*.

[10] Melissa Chase. 2007. Multi-authority Attribute Based Encryption. In *Proceedings of the Conference on Theory of Cryptography (TCC)*. Springer-Verlag, 515–534. https://doi.org/10.1145/2914642.2914659

[11] Chui. 2014. Chui Doorbell. https://www.getchui.com. (2014).

[12] CNET. 2017. Is Google Home good at voice recognition? https://www.cnet.com/news/is-google-home-good-at-voice-recognition/. (2017).

[13] Ry Crist. 2017. Multiple users, multiple systems, multiple devices: Is this the smart home from hell? https://www.cnet.com/news/multiple-users-multiple-systems-multiple-devices-is-this-the-smart-home-from-hell/. (December 2017).

[14] Ecobee. 2017. Ecobee4 Wi-Fi Thermostat. (2017). https://www.ecobee.com/ecobee4/

[15] Serge Egelman, A.J. Bernheim Brush, and Kori M. Inkpen. 2008. Family Accounts: A New Paradigm for User Accounts Within the Home Environment. In *Proceedings of the ACM Conference on Computer Supported Cooperative Work(CSCW)*. ACM, 669–678. https://doi.org/10.1145/1460563.1460666

[16] Serge Egelman, Sakshi Jain, Rebecca S. Portnoff, Kerwell Liao, Sunny Consolvo, and David Wagner. 2014. Are You Ready to Lock?. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS)*. ACM, 750–761. https://doi.org/10.1145/2660267.2660273

[17] Google. 2017. Media and multiple users on Google Home. https://support.google.com/googlehome/answer/7342711?hl=en. (2017).

[18] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. 2006. Attribute-based Encryption for Fine-grained Access Control of Encrypted Data. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*. ACM, 89–98. https://doi.org/10.1145/1180405.1180418

[19] Alina Hang, Emanuel von Zezschwitz, Alexander De Luca, and Heinrich Hussmann. 2012. Too Much Information!: User Attitudes Towards Smartphone Sharing. In *Proceedings of the Nordic Conference on Human-Computer Interaction: Making Sense Through Design (NordiCHI)*. ACM, 284–287. https://doi.org/10.1145/2399016.2399061

[20] Luan Ibraimi, Milan Petkovic, Svetla Nikova, Pieter Hartel, and Willem Jonker. 2009. Ciphertext-Policy Attribute-Based Threshold Decryption with Flexible Delegation and Revocation of User Attributes (extended version). *Centre for Telematics and Information Technology, University of Twente* (2009).

[21] Maia Jacobs, Henriette Cramer, and Louise Barkhuus. 2016. Caring About Sharing: Couples' Practices in Single User Device Access. In *Proceedings of the 19th International Conference on Supporting Group Work (GROUP)*. ACM, 235–243. https://doi.org/10.1145/2957276.2957296

[22] Amy K. Karlson, A.J. Bernheim Brush, and Stuart Schechter. 2009. Can I Borrow Your Phone?: Understanding Concerns when Sharing Mobile Phones. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 1647–1650. https://doi.org/10.1145/1518701.1518953

[23] Yunxin Liu, Ahmad Rahmati, Yuanhe Huang, Hyukjae Jang, Lin Zhong, Yongguang Zhang, and Shensheng Zhang. 2009. xShare: Supporting Impromptu Sharing of Mobile Phones. In *Proceedings of the International Conference on Mobile Systems, Applications, and Services (MobiSys)*. ACM, 15–28. https://doi.org/10.1145/1555816.1555819

[24] Akhil Mathur, Nicholas D. Lane, Sourav Bhattacharya, Aidan Boran, Claudio Forlivesi, and Fahim Kawsar. 2017. DeepEye: Resource Efficient Local Execution of Multiple Deep Vision Models Using Wearable Commodity Hardware. In *Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys)*. ACM, 68–81. https://doi.org/10.1145/3081333.3081359

[25] Tara Matthews, Kerwell Liao, Anna Turner, Marianne Berkovich, Robert Reeder, and Sunny Consolvo. 2016. "She'll Just Grab Any Device That's Closer": A Study of Everyday Device; Account Sharing in Households. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, 5921–5932. https://doi.org/10.1145/2858036.2858051

[26] Momo. 2017. Momo | Your Intelligent Smart Home Assistant. https://www.kickstarter.com/projects/98269215/momo-your-intelligent-smart-home-assistant. (May 2017).

[27] Netatmo. 2015. Netatmo Welcome. https://www.netatmo.com/en-US/product/security/welcome. (2015).

[28] Xudong Ni, Zhimin Yang, Xiaole Bai, Adam C. Champion, and Dong Xuan. 2009. DiffUser: Differentiated User Access Control on Smartphones. In *Mobile Adhoc and Sensor Systems*.

[29] Diana Olick. 2016. Just what is a 'smart home' anyway? https://www.cnbc.com/2016/05/09/just-what-is-a-smart-home-anyway.html. (May 2016).

[30] Mark Patton, Eric Gross, Ryan Chinn, Samantha Forbis, Leon Walker, and Hsinchun Chen. 2014. Uninvited connections: a study of vulnerable devices on the internet of things (IoT). In *Intelligence and Security Informatics Conference (JISIC)*. IEEE, 232–235.

[31] Philips. 2017. Philips Hue. (2017). http://www2.meethue.com/en-us/

[32] Oriana Riva, Chuan Qin, Karin Strauss, and Dimitrios Lymberopoulos. 2012. Progressive Authentication: Deciding when to Authenticate on Mobile Phones. In *Proceedings of the USENIX Conference on Security Symposium*. USENIX Association, 15–15. http://dl.acm.org/citation.cfm?id=2362793.2362808

[33] Samsung. 2017. Samsung Family Hub Refrigerator. (2017). http://www.samsung.com/us/explore/family-hub-refrigerator/overview/

[34] X. Si, P. Wang, and L. Zhang. 2013. KP-ABE Based Verifiable Cloud Access Control Scheme. In *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*. 34–41. https://doi.org/10.1109/TrustCom.2013.68

[35] Nigel P. Smart. 2003. Access Control Using Pairing Based Cryptography. In *Proceedings of the RSA Conference on The Cryptographers' Track (CT-RSA)*. Springer-Verlag, 111–121. https://doi.org/10.1007/3-540-36563-X_8

[36] SmartThings. 2017. Account sharing FAQ. https://support.smartthings.com/hc/en-us/articles/206531223. (2017).

[37] A. Ben Thabet and N. Ben Amor. 2015. Enhanced smart doorbell system based on face recognition. In *2015 16th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA)*. 373–377. https://doi.org/10.1109/STA.2015.7505106

[38] Wired. 2017. APPLE'S 'NEURAL ENGINE' INFUSES THE IPHONE WITH AI SMARTS. https://www.wired.com/story/apples-neural-engine-infuses-the-iphone-with-ai-smarts/. (2017).

[39] Jan Henrik Ziegeldorf, Oscar Garcia Morchon, and Klaus Wehrle. 2014. Privacy in the Internet of Things: threats and challenges. *Security and Communication Networks* 7, 12 (2014), 2728–2742.