Challenges in Access Right Assignment for Secure Home Networks*

Tiffany Hyun-Jin Kim[§] Lujo Bauer[§] James Newsome[§] Adrian Perrig[§] Jesse Walker[†]

[§] Carnegie Mellon University
{hyunjin1, lbauer, jnewsome, adrian}@ece.cmu.edu

[†] Intel Research
jesse.walker@intel.com

Abstract

The proliferation of advanced technologies has been altering our lifestyle and social interactions – the next frontier is the digital home. Although the future of smart homes is promising, many technical challenges must be addressed to achieve convenience and security. In this paper, we delineate the unique combination of security challenges specifically for access control and consider the challenges of how to simply and securely assign access control policies to visitors for home devices and resources. As an initial approach, we present a set of intuitive access control policies and suggest four access control settings based on our in-person interview results. We anticipate that future research can build on our proposed mechanisms to provide confidence to non-expert home owners for letting visitors use their home network.

1 Introduction

The following technology trends for 21st Century home are already well under way: connected devices and appliances, demand/response systems for electricity and other connections to the "smart grid", digital media ranging from books to music, Internet-connected security systems, wireless medical devices like pacemakers, location systems, and smart phones. These technologies will fundamentally impact our home environment, offering transformational new features ranging from remote management to digital troubleshooting to neighborhood interaction among various devices. Indeed, there already is a cross-industry organization of leading consumer electronics, computing and mobile device companies called Digital Living Network Alliance that enables digital content (e.g., photos, music) to be shared among devices that belong to the same network (e.g., laptops, mobile phones).[1] For many new technologies, new features drive adoption, and unfortunately, security and privacy issues are often left to be addressed later.

Technology Trends. The future smart home that we envision is enabled by a number of technology trends:

- **User Interfaces (UIs) for "everything."** As in Mark Weiser's vision, "invisible" computers and interfaces (i.e., ease of use is so effective that one does not notice the computer) will transcend most objects we interact with [15], and appliances will have built-in computers, UIs (display, keyboard), and/or RFID tags.
- **Network communication.** Objects with computing capabilities will also connect to the home network and the Internet. Network communication will enable remote device operation and management.
- **Digital media.** Media will continue transitioning from physical to purely digital. Examples include MP3 files, Netflix movies, Kindle eBooks, and photos on Flickr.
- **Smart phones.** Smart phones will become universal UIs to control devices in a smart home. In Q2 2009, 28% of all phone sales in the US were for smart phones.[2] In the foreseeable future the majority of phones will be smart phones, and users are already developing home control applications on smart phones.
- **Smart meters & grids.** Smart meters and grids reduce costs by enabling power companies to use demand-response mechanisms. This makes it possible to manage electricity consumption in response to supply conditions (e.g., market prices).
- **Wireless medical devices.** Many health-care devices are becoming portable and wireless to enable real-time monitoring by doctors.

These trends will fundamentally alter our living style

*This research was supported in part by CyLab at Carnegie Mellon under grant DAAD19-02-1-0389 from the Army Research Office, grant CNS-0627357 from the National Science Foundation, and by gifts from Bosch and Intel. The views and conclusions contained here are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either express or implied, of ARO, Bosch, CMU, Intel, NSF, or the U.S. Government or any of its agencies.

[1] http://www.dlna.org

[2] http://www.npd.com/press/releases/press_090819.html

and the way we interact with our home. However, a challenge is to build smart homes that are both convenient and secure. In this paper, we consider how to address the security issues of access control management in such an environment when sharing resources while minimizing user involvement.

Security Issues. Consider, for example, that the home will have a plethora of microphones and cameras that can be remotely activated; sensitive data such as health information and financial information will be accessible from anywhere; records of viewing and reading habits, personal photos, videos, and diaries will all be available digitally; implanted medical devices can be remotely controlled by health care providers and interact with medical databases. In this context, computer security breaches will not only compromise individuals' and families' privacy to an even greater degree than ever before, but can also easily cause direct physical harm, all in the "comfort" of one's own home.

The fundamental challenge that we focus on is how to control access in this environment – essentially, how to enable home users to manage access-control policies for everyone who visits their homes, including family members, friends, visitors (e.g., repairman, housekeeper, accountant), as well as emergency-related personnel (e.g., first responder, doctor). The central issues in this space revolve around the complexity and diversity of the resources, the diversity of the subjects, the low sophistication of the administrators, and the social context.

Contributions. With this paper, we want to raise awareness of the important problem of access control in future home networks, and we pursue two objectives. First, we enumerate the series of challenges that makes the access control management of the digital home a unique and particularly difficult task. Although some of the individual challenges may appear in other contexts, the home environment presents a unique combination of challenges. Second, we lay out a high-level approach for defining access-control policies in the home environment. Our approach is motivated by a preliminary user study, which we briefly describe.

2 Problem Definition & Threat Model

Establishing a home network is easy, but a core challenge is how to enable non-expert users to safely set home access control policies. In this section, we present a problem definition and threat model.

2.1 Problem Definition

Our central goal is to protect the resources in a home network environment against unauthorized use. More specifically, we intend to protect against misuse by visitors, as we assume that current security mechanisms can protect against malicious outsiders (e.g., we do not address key management). In particular, we aim to provide a mechanism to assist home owners in giving their visitors access to particular devices or resources within their homes. Such mechanism should be as easy to use as possible so as to be accessible to non-experts and to generally place minimal burden on users.

An access control management mechanism should provide the following security properties:

- secrecy and privacy of personal information (protect against undesired disclosure of data),
- integrity of personal information (protect against undesired alteration or loss of data),
- availability of resources (prevent Denial-of-Service (DoS) attacks against resources),
- allow only permitted accesses (prevent against misuse of devices to cause annoyance, disturbance, physical damage, or economic harm).

2.2 Threat Model

Our adversary model is a visitor who receives unintended access privileges from some principal in the system and misuses them. More specifically, we try to guard against a visitor who receives more permissive access rights than what the home owner wishes to grant.For example, an honest but curious visitor could attempt to read sensitive information, perform unwanted alterations to existing data, or overuse devices beyond reasonable limit (i.e., printing an entire photo album on the owner's color printer). Also, the visitor could perform disturbing operations on the home network after he leaves, for example by playing loud music at night or shutting off the home security system.

Although other attacks such as external attacks on the communication channel [4] or device compromise are important, we focus in this work solely on access control, given the limited amount of space available.

3 Unique Combination of Challenges

Despite the plethora of research in access control, we believe that no existing solution adequately addresses the unique set of challenges posed by home environments. Discretionary access-control mechanisms do not usably scale to the complexity of homes; it would be impractical to set access rights to hundreds of resources for each visitor. Access-control systems used in corporate environments require professional administrators. While some researchers have created tools to help users create access-control policies (i.e., SPARCLE Policy Workbench [5], Expandable Grid [13]), these tools target more constrained environments and more skilled (though still non-expert) users than will characterize the future digital home. In this section, we elaborate on specific challenges that secure home access assignment systems encounter.

No Dedicated Expert Administrator. The typical

home user lacks both the patience and the expertise required of an administrator in a corporate access control system. For example, even technologically savvy Firefox 2 users ignore an expired certificate warning from their banking websites [14]. A typical home user is unlikely to spend much time learning complex interfaces or performing tasks such as assigning access rights, auditing current policies, or auditing the access logs.

Mixed Ownership. In many homes, no single person owns all devices, but each household member owns a subset of devices. Also, many shared devices exist without a single clear owner. Consequently, some devices may lack an access policy, while others have inconsistent policies.

Complexity of Home Environments. The number and diversity of devices and resources in homes causes tremendous complexity for access control mechanisms. For example, homes have typical appliances (washer, fridge), storage devices (for music, videos, photos, files), network-related devices (wireless router, femto cell), safety devices (smoke/gas detectors, alarms), etc. Home environments are further complicated by the high dimensional types of resources that each device supports. For instance, a portable music player is no longer used just to store and listen to music – it is also used as a storage device (contact information, videos, photos, documents) and as a scheduler. Furthermore, data adds one more layer of complexity. On a storage device (i.e., desktop computer) that is shared by house members, for example, users may store sensitive personal data along with non-sensitive data that they may want to share with others.

Diversity of Visiting Parties. The types people who visit homes and need access to home resources is diverse, ranging from family members and relatives, friends and neighbors to service workers, utility company, first responders (law enforcement, fire fighters), health care providers, and elderly care providers. Each party requires different access to home resources, yet generating a specific access control policy for each party under all circumstances is cumbersome.

Multiple Uncoordinated Administrators. In homes with multiple members, a single master administrator for the home network is not sufficient for maintenance. In case the one and only administrator is away from home, there must be an alternative administrator who knows how to manage and update the access control policies; for example, an electrician needs to access the master light control system when the master administrator, who can only change the access policies for the light control system, is on business travel. Hence, it is necessary that more than one (if not all) members of the household should be able to manage access control mechanisms.

On the other hand, only trusted people should be able to change the access control configuration. For example, small children should not be able to control the access control functions for the main security system such that they cannot grant burglars (who may approach children in a friendly manner) access to home devices.

Differences in Administrator Preferences. Some owners want a high level of security and privacy and do not mind high management overhead while others may be trusting and prefer low administration overhead. The level of convenience desired or disturbance tolerated can also vary. Balancing the security, privacy, and the level of convenience for different users is a significant challenge.

Social Context: Distrust Revelation Problem. Users may not want to admit that a visitor is untrusted. As a result, the usually invisible aspect of trustworthiness becomes visible through the home access control policy. A visitor who considers himself as a close friend to the home owner may become upset to learn that he is only granted the minimum access level. Such situations may put social pressure on the home owner to provide looser access controls to avoid revealing his distrust.

4 Preliminary Policy Assignment

A significant aspect of the problem of securing the digital home is providing users with convenient yet trustworthy mechanisms for specifying and managing access-control policy. Studies have suggested that users have varied and complex access-control needs (e.g., [12]). At the same time, experience teaches us that complex policies typically cannot be adequately managed by end users, especially by non-expert users. We conducted a small user study to preliminarily determine the specific access-control needs of users with respect to the future digital home (Section 4.1). We found that home users wish to restrict access to resources within their home via a small set of high-level constraints (Section 4.2). Based on the results of the study, we propose that creating several sets of policies and assigning users to these sets may meet the needs of most home users (Section 4.3).

4.1 User Study

We conducted a small-scale interview study to learn about users' access-control concerns and desired policies. We recruited 20 people (8 males and 12 females) within the age range of 20 to 60 years old through Craigslist and personal contacts. We asked each participant to list 8 people with whom they interact on an at least semi-regular basis. We also asked each participant to consider electronics and appliances in their future home. We then sought information about the access policies that they would set on those devices to restrict their use by the 8 contacts. More specifically, we asked various questions related to how much participants would allow each contact to access home appliances and how much they would be concerned if they violate specified access rights. To prepare participants, we mentioned various instances of the poli-

cies we describe in Section 4.2, and asked them to suggest new policies when our initial ones didn't meet their needs. For example, we asked questions about how the participant would assign access-control policies for the main entrance, such as "would you allow Person X to unlock your door and enter the house?", "would you feel comfortable to let Person X unlock the door when you are not present?", or "if the door lock keeps a record of who has operated it and you can check the record, would you allow Person X to unlock the door?"

While conducting this user study, we were able to validate some of the challenges as mentioned in Section 3. We observed that the participants (mostly the heads of their households) were not technical experts. Also, the participants listed diverse devices when we asked for a list of all devices for their future home, and provided various types of people as potential visitors. The participants responded that they would be concerned if the access policy assignments were revealed to the visitors.

Among the observations we make based on the data gathered in our study are the following two. First, the three types of policies that we presented users with (Section 4.2) were sufficient to capture users' desired policies. Users made use of all three, and did not propose any others when given the opportunity to do so. Second, we observe that users tend to create fixed sets of access-control policies, and assign a particular set to visitors based on the duration of their relationship and the level of trust (Section 4.3).

4.2 Policy Constraints

To mimic access-control policies in current homes, the future digital home will need to support richer policies than simply allowing or denying access to specific resources. We propose three orthogonal dimensions for naturally constraining access-control policies: presence, logging, and asking for permission.

Presence. Many current home devices require physical presence to operate, i.e., a user must be *inside* the house to gain access. Light switches fall into this category. Although in future homes wireless control of resources will be pervasive, we would like to preserve this property of requiring physical presence. This can be accomplished with two kinds of constraints: *user presence* and *owner and user presence*.

For policies constrained by *user presence*, denoted as $\mathtt{P_U}$, the home owner allows the visitor to use the home electronics and appliances under one condition: the visitor must be physically present near the device. This policy may be the simplest that non-expert home owners may use for their home devices since any visitor may use devices as needed without bothering the owners; however, this type of policy is the most vulnerable in terms of secrecy and integrity properties, since a malicious visitor could potentially access secret information or alter information while they are near a storage device. This policy is ideal for physical devices such as a light switch, which can be operated while the visitor is in the room, and aren't vulnerable to secrecy or integrity violations.

For the *owner and user present* access control policy, denoted as $\mathtt{P_{OU}}$, we additionally require that the owner of the resource is physically present. For some resources, it is obvious when the resource is accessed because of noticeable artifacts of operation, e.g., the sound made by a printer. For these devices, a natural policy is to enable the access when both the owner and user are physically present. This policy is commonly used today, as visitors can usually freely use visible resources when the owner is in the same room, under the assumption that the owner would warn them if they attempt to perform an unauthorized action, either accessing unauthorized resources or overusing them beyond a reasonable limit.

Logging. We envision that future home devices will record accesses. A *permitted with logging* policy, denoted as $\mathtt{P_L}$, requires devices to maintain detailed audit logs. Rarely accessed devices may even proactively notify their owners of accesses, e.g., via a text message. This policy assumes that users are generally aware that accesses of all devices are logged. Such logging could deter visitors from making unauthorized accesses since they are likely to be discovered by the owner. The current equivalent of this policy is a security camera that watches a resource. The log entries may be prioritized based on the importance of events such that users can easily review the logs when necessary. Correctly prioritizing the entries with illegitimate accesses while preventing the entries with legitimate accesses is yet another challenge.

With logging-based policies, a user may pretend that a malicious access was inadvertent. For example, a visitor may blame an access of a tax file on a home storage server on an overly aggressive virus scanner on the visitor's mobile device. Consequently, logging-based access control should be used for resources where such inadvertent access is implausible.

Asking for Permission. Sometimes it is unclear how much access to provide to visitors. Instead of enumerating exactly all access rights, we propose that lazy evaluation is appropriate in some circumstances – the owner is contacted whenever visitors attempt to use a particular resource. We call this policy *ask for permission* and denote it with $\mathtt{P_A}$. In this manner, the owner knows exactly who is trying to use which device in her home. On the other hand, the owner may be overwhelmed with queries when several guests attempt to use resources. The current equivalent for this policy is that polite visitors would ask the owner if they are allowed to open a fancy box on a shelf, for example. The length for which access is granted may vary: the owner may grant one-time access or permit

access for a specific interval. Similarly, the number of allowed uses may vary to prevent visitors from overusing any devices/resources.

Hybrid Policies. The three orthogonal policy constraints can be combined. For example, a policy P_{UA} will require user presence and asking for permission.

We denote the *always deny* policy with P_X. For some devices or resources owners may want to deny any access by visitors. Devices containing private information, such as tax records or a personal diary, are examples.

4.3 Groups of Policies

A home owner may have a unique personal relationship with each visitor, and would hence wish to assign to that visitor a distinct set of access policies. Unfortunately, this would likely require a lot of effort.

Although studies find that categorizing all visitors into a small set of groups is unlikely, such a classification with respect to access-control settings may capture *most* visitors [8]. From our user study, we observe that participants use a fixed set of categories of access-control policies and assign each visitor to one of them. Such assignment is based on the length and closeness of the relationship. For example, home owners do not mind if people such as close family members and relatives open the main entrance from outside when the owners are not present; however, they would mind if people with whom they spend less time and trust less (e.g., neighbors) did so.

Based on the fine-grained responses, we were able to group access control policies into four common settings.

- **Full Control:** A user is given complete control over and full access to all devices and resources. It may be assigned to owners, close relatives, and members of the household.
- **Restricted Control:** Users assigned to this group of policies have full access to all devices besides the entertainment system and the security system. This group of policies may be assigned to teenagers in the household.
- **Partial Control:** A user assigned to this group receives full access permissions over selected public devices that can be easily shared with others, such as a TV. This policy may be for people other than household members with whom the owner feels comfortable and whom the owner trusts.
- **Minimal Control:** This setting is the most restrictive, and is granted to acquaintances or visitors who are not close friends.

From our study we derive a set of specific policies with which each of these four groups could be instantiated; we show these in Table 1. We suggest that devices should be outfitted by the manufacturer to be able to support these suggested policies. Such pre-loading of suggested policy assignments during manufacturing time can simplify home owners' tasks; instead of assigning a specific policy for each and every device per visitor, they now only need to decide which of the four access control settings the visitor belongs to. Then the mapping from the setting to basic policies for all devices and resources is automatically configured with pre-loaded suggested policy assignments.

It is possible that home owners are not satisfied with a pre-loaded set of basic access policies, access control settings, and the suggested access policy assignments. Consequently, we suggest that devices and resources allow home owners to change policies manually; home owners can not only create new policies, new classes of users, and new policy assignments, they can also modify the pre-loaded assignments that we suggest.

Device/Resource Group	Full	Restricted	Partial	Minimal
Personal laptop computer	P_U	P_U	P_A	P_A
Personal file (tax/diary)				P_X
Internet			P_U	P_A
Home storage (photos, music)				P_{OU}
Personal file storage (USB)			P_A	P_A
Surveillance camera			P_L	P_X
Home telephone (call log)			P_U	P_A
TV/DVR/game		P_L		P_{OU}
Digital photo frame		P_U		
Smart fridge (camera inside)				P_A
Door lock			P_L	P_X
Window lock				P_A
Home security controller		P_{OU}	P_X	P_X

Table 1: Suggested basic access policy assignments for potential home devices and access control settings

5 Related Work

Johnson and Stajano have considered the problem of providing permissions to guests [7]. This paper is the most related work, but we consider the problem in more detail by considering a wider range of guests, devices, resources, and data. We also consider social aspects and perform a user study to back up our explorations. Argyroudis and O'Mahony have built a system called AETHER, which addresses the establishment of security associations between a set of access control attributes and principals for ubiquitous smart home environments [1]. Although AETHER provides a foundational architecture for managing security relationships in smart home environments, our work addresses the problem in more detail, such as suggesting a complete set of access control policies and classes of principals. Kostianinen et al. test several access control concepts and propose an access control solution for home networks that imposes minimal burden

on the user [9], but they focus on establishing a home network for family members only, and they do not address the access of visitors, which is the core challenge for an efficient and easy-to-use home access control system. Similarly, Marin et al. propose a home automation middleware for secure management of user and contextual data that gives access to services just to the authorized users and devices [11], but their system also only considers owners of devices as authorized users and does not address issues with visitors. Brush and Inkpen present results from an empirical study of 15 families, and discuss about the degree of shared ownership and use of technologies that families own [6]. Their result suggests that families trust their family members, but they maintain separate profiles on technologies only to prevent teenagers from accessing computers or to prevent malicious outsiders.

In the remainder of this section, we discuss other related work in trust-based access control and policy management for both corporate and home environments. Many researchers have worked on trust-based security establishment mechanisms. Seigneur et al. have developed the SECURE framework that has focused on allowing access rights among previously unknown principals to minimize security configuration [10]. Adjusting trust based on reputation as described in their paper has some security vulnerabilities; an unauthorized person may be able to gain high trust by stealing a security object that belongs to the home owner and mimicking the owner's biometric information such as his/her voice.

Prior work considers using portable devices to control access to physical spaces [2, 3]. Bauer et al. use mobile devices as access control tokens for physical space in an office environment [3]. They also conduct a user study and derive users' ideal access policies, which includes the 'ask for permission' policy [2]. However, their work focuses chiefly on controlling access to a single type of resource (office doors) and only in an office environment.

6 Conclusion

We observe that providing access to home resources to visitors is a very challenging research problem, mainly because of the heterogeneity and complexity of home resources, the diversity of visitors, the distrust revelation problem, and the inexperience in security of the home owner. Without sensible mechanisms, visitors could either obtain access to sensitive personal data (in the case of liberal access assignment), or not be able to use the light switch (in the case of restrictive access assignment).

In this paper, we provide a preliminary approach to address some of these challenges by assigning visitors access rights from one of four pre-defined groups, each constructed using one of three proposed policy types. We leave as future work a full evaluation of how well these assignments work with larger set of participants. Several other challenges from Section 3 remain, particularly the ones stemming from multiple administrators.

We hope that the research community will embrace this important research challenge to make future home networks at least as secure and usable as current homes.

References

[1] ARGYROUDIS, P., AND O'MAHONY, D. Securing Communications in the Smart Home. In *Proceedings of International Conference on Embedded and Ubiquitous Computing* (August 2004).

[2] BAUER, L., CRANOR, L., REEDER, R. W., REITER, M. K., AND VANIEA, K. A User Study of Policy Creation in a Flexible Access-Control System. In *CHI: Conference on Human Factors in Computing Systems* (Apr. 2008).

[3] BAUER, L., GARRISS, S., MCCUNE, J. M., REITER, M. K., ROUSE, J., AND RUTENBAR, P. Device-Enabled Authorization in the Grey System. In *Information Security: ISC* (Sept. 2005).

[4] BERGSTROM, P., DRISCOLL, K., AND KIMBALL, J. Making Home Automation Communications Secure. *Computer 34*, 10 (2001), 50–56.

[5] BRODIE, C. A., KARAT, C.-M., AND KARAT, J. An Empirical Study of Natural Language Parsing of Privacy Policy Rules Using the SPARCLE Policy Workbench. In *Proceedings of the Usable Privacy and Security (SOUPS)* (2006).

[6] BRUSH, A. J. B., AND INKPEN, K. M. Yours, Mine and Ours? Sharing and Use of Technology in Domestic Environments. In *Proceedings of Ubicomp* (2007).

[7] JOHNSON, M., AND STAJANO, F. Usability of Security Management: Defining the Permissions of Guests. In *Proceedings of Security Protocols Workshop* (April 2006).

[8] KARLSON, A. K., BRUSH, A. B., AND SCHECHTER, S. Can I Borrow Your Phone?: Understanding Concerns When Sharing Mobile Phones. In *CHI: Conference on Human Factors in Computing Systems* (2009).

[9] KOSTIAINEN, K., RANTAPUSKA, O., MOLONEY, S., ROTO, V., HOLMSTROM, U., AND KARVONEN, K. Usable Access Control inside Home Networks. *Nokia Research Center Technical Report NRC-TR-2007-009* (2007).

[10] MARC SEIGNEUR, J., JENSEN, C. D., FARRELL, S., GRAY, E., AND CHEN, Y. Towards Security Auto-Configuration for Smart Appliances. In *Proceedings of the Smart Objects Conference* (2003).

[11] MARIN, A., MUELLER, W., SCHAEFER, R., ALMENAREZ, F., DIAZ, D., AND ZIEGLER, M. Middleware for secure home access and control. In *Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops* (2007).

[12] MAZUREK, M. L., ARSENAULT, J., BREESE, J., GUPTA, N., ION, I., JOHNS, C., LEE, D., LIANG, Y., OLSEN, J., SALMON, B., SHAY, R., VANIEA, K., BAUER, L., CRANOR, L. F., GANGER, G. R., AND REITER, M. K. Access Control for Home Data Sharing: Attitudes, Needs and Practices. In *CHI: Conference on Human Factors in Computing Systems* (2010).

[13] REEDER, R. W., BAUER, L., CRANOR, L. F., REITER, M. K., BACON, K., HOW, K., AND STRONG, H. Expandable Grids for Visualizing and Authoring Computer Security Policies. In *CHI: Proceeding of the Conference on Human Factors in Computing Systems* (2008).

[14] SUNSHINE, J., EGELMAN, S., ALMUHIMEDI, H., ATRI, N., AND CRANOR, L. F. Crying Wolf: An Empirical Study of SSL Warning Effectiveness. In *USENIX Security* (2009).

[15] WEISER, M. The Computer for the Twenty-First Century. *Scientific American 265*, 3 (Sept. 1991).