Challenges faced in working with users to design access-control systems for domestic environments

Manya Sleeper
Carnegie Mellon Unversity
Pittsburgh, PA
msleeper@cmu.edu

Michelle L. Mazurek
Carnegie Mellon University
Pittsburgh, PA
mmazurek@cmu.edu

Lujo Bauer
Carnegie Mellon University
Pittsburgh, PA
lbauer@cmu.edu

Abstract
Users share large amounts of personal content. It is important to develop usable access control systems tailored to domestic environments. However, working with users to study their access control preferences in the home presents a number of unique challenges including: ethical considerations, the difficulty of observing actual and hypothetical access-control preferences, and the impact of the presence of the researcher. We describe our experience addressing these issues for file system access control and call for discussion of best practices.

Author Keywords
Usability, access control, user study, home

ACM Classification Keywords
H.5.m [Information interfaces and presentation (e.g., HCI)]: Miscellaneous.

Introduction and background
Users share large amounts of content in domestic environments through shared devices, cloud-based systems like Dropbox or Google Docs, email, or on social networking services, like Facebook. This personal data sharing is widespread and increasing - for example, each day, 350 million photos are posted to Facebook [13].

In general, it is important to help users control access to their shared content; however, these needs are complex. It is, therefore, difficult to develop usable systems that allow users to accurately express such access control needs [6]. Additionally, while research has explored access-control system design challenges, the majority of such work focuses on organizational users' access-control needs (e.g., [9, 12]), with only more limited work on domestic environments or non-expert users (e.g., [6, 10, 2]).

Distinct from organizational users' needs, access-control systems for domestic environments must address the unique set of challenges presented by content sharing in homes or within households. Domestic environments lack formal file-sharing access-control structures found in organizations, users range in technical expertise and motivation, and relationship and household dynamics may impact access-control motivations and abilities (e.g., a household with children may differ from a household made up of roommates, which may both differ from a couple living with an elderly parent) [2]. Also, while home users often have complex access-control needs, they may have a low levels of willingness or ability to address these needs [6]. Thus, it is important to work with users in home environments to understand their file-sharing access-control needs, across a range of scenarios, when developing usable access-control tools.

As part of this effort, we are developing Penumbra [8], a metadata-based access-control system intended for home users and designed to be usable for non-experts. We based the initial design goals on preliminary studies of access-control preferences [6, 4, 7]. Penumbra should support a range of desirable access-control functionality but should be optimized for the most common and important preferences. Thus, we need to work with home users to understand how they access and share files, current content-sharing and access-control needs, and usability and privacy issues the system should address.

While working with users in this context is important, we have found that there are several challenges, specific to working on file access control in the home environment, that must be addressed when developing such studies. These fall into three broad categories: ethical issues, the difficulty of observing real and hypothetical access-control practices, and addressing the impact of the presence of the researcher. We describe lessons learned in addressing these issue from our initial studies. These challenges would benefit from discussion with the broader domestic environment design community.

Ethical considerations

Studies that target access-control preferences often present ethical concerns. To understand the content participants want to prevent others from viewing or want to share, researchers typically need to ask participants to reveal personal or sensitive information. For example, to understand access-control behaviors, it is often necessary to ask about content a participant considers private, because this is the data for which the participant would want to control access. The sensitivity of private content and access-control preferences can be exacerbated when working with users in domestic environments. Researchers often work with interconnected participants in a household (e.g., families, roommates, etc.) with varied power dynamics (e.g., parents with children, unrelated roommates) and relationships.

It is possible to avoid some sensitivity by only working with one individual in each household or relationship (e.g., either a parent or a child, or one of two people in a

couple); however, to capture access-control preferences, researchers often want to understand the sharing dynamics within the household.

We have developed several practices during prior work for asking participants about potentially sensitive data. We ask participants for the minimum amount of necessary data at the highest level of granularity. For example, we use placeholders for actual sensitive information. We also ask participants for descriptions of people instead of actual names (e.g.,"sister" or "high school teacher") or high-level descriptions of file types (e.g., "financial files") instead of detailed descriptions of content.

For interviews in the home, it's also necessary to consider which questions can be asked as part of a group interview and which should be asked one-on-one. In one study (Mazurek et al. [6]) we interviewed households one-on-one and in groups about access-control preferences. Questions about data household members might want to hide from one another, or about how one member would react to the discovery that another member was hiding something, were restricted to the one-on-one interviews in an effort to elicit more honest answers.

Difficulty of observing access-control practices

Although it is important to understand access-control preferences in the home, many people do not currently use technical access-control mechanisms offered by the devices and software they use, because the mechanisms are either too obscure or require too much time and effort. Instead, people tend to use ad-hoc, self-developed approaches to control access to content, such as physically hiding an external hard drive to protect it from roommates or giving important files semi-random obfuscated names [6, 10]. New, more usable systems are also often intended to enable new functionality that would, in turn, cause new behaviors.

Thus, to inform development of usable access-control systems, researchers often want to understand ideal access-control preferences that systems should support, not just ad-hoc practices users have developed. There are a variety of techniques that studies have used to try to discover home users' actual access-control preferences absent current, widely-used, usable systems.

One technique is to use interviews to ask participants about their different file types, who should be allowed to access which content, and how they keep content safe (both on- and off-line). Paired with asking about current use of access-control system, this can help develop an idea of users' mental models of access control [6]. Another technique is to approximate access-control preferences by asking participants for a representative set of content and a set of people who represent a range of access-control preferences (e.g., close friends, family members, enemies, etc.), create a grid of access-control preferences, and ask the participant to indicate their willingness to share (used in Klemperer et al. [4]).

Experience sampling can also be used. Several studies of access-control preferences have, with prior participant knowledge, sent participants mock requests for access from a range of people to gauge hypothetical reactions [7, 3]. Some studies have also specifically instrumented access-control settings in a participant's tool to study their preferences [5]. Similar methods could be used in a specifically domestic environment.

Choice of technique depends on the focus of the study. Ideally, as no technique will provide a perfect

representation of participants' preferences, a combination should be used to provide the best approximation.

Impact of the presence of the researcher

In general, the presence of the researcher can impact a study and can change the dynamic in a home. This can be especially important for studies that address access control because participants may be reluctant to admit private content or behaviors to a researcher or carry out such behaviors when observed.

This reluctance can be addressed in several ways. First, typical best practices for user research should be used. Researchers should behave professionally, emphasize in recruitment materials and preliminary scripts their ties to a research organization and the purpose of the project, and build trust with participants. However, it may also be necessary to supplement the rich data supplied by in-person work with participants in the home with an anonymous survey (with the same participants or others) or other forms of aggregate data collection that preserve privacy while also allowing more openness.

Additionally, participants in user studies often describe a high level of concern about privacy that is not reflected in behavior with an actual system [14]. This may reflect the fact that using access-control tools in practice requires more effort than talking about preferences, or it may reflect a desire to tell the researcher what the participant thinks they want to hear. To more accurately reflect the access-control preference level of the participants, it may be necessary to simulate a similar level of effort when testing a prototype as would be required in an actual system. Or, when asking a participant about the strength of their preference, it may be necessary to ask them about the preference framed in terms of its cost/benefits. For example, in a survey on Facebook and privacy Acquisti and Gross asked participants to rate privacy relative to other, major social issues [1].

Conclusions

Content sharing is becoming increasingly prevalent, and is moving increasingly into the home, across household devices (phones, computers, tablets, TVs, etc.) and family members. Outside organizational structure for access control there is a need for usable access-control tools for such content. However, incorporating an understanding of home users into the design of usable access-control systems for domestic environments creates several challenges.

Although our work has addressed file-system access control, as smart devices become more common in homes access control for such devices will become more important, creating additional challenges for such work. Research has already begun to address the need to design usable access-control systems for smart devices ranging from door locks and lighting systems to energy consumption monitors [11, 15]. The challenges seen in file-system access-control systems will continue to increase in scope with the need to design studies to inform such system designs.

In the course of designing studies in the file-system access-control space we have developed several solutions to address the challenges presented by ethical considerations, the difficulty of observing access-control practices, and the impact of the presence of the researcher. However, these issues would benefit from discussion in the broader domestic design community and the potential development of best practices for varied types of studies in the home. This is an important and

challenging research area, and the need to work with users on access-control issues in varied domestic environments will only increase going forward.

Acknowledgements

This material is based upon work supported by the National Science Foundation under Grants No. 0946825, CNS-0831407, and DGE-0903659, by CyLab at Carnegie Mellon under grants DAAD19-02-1-0389 and W911NF-09-1-0273 from the Army Research Office, by gifts from Cisco Systems Inc. and Intel, and by Facebook and the ARCS Foundation.

References

[1] Acquisti, A., and Gross, R. Imagined communities: Awareness, information sharing, and privacy on the Facebook. In *Privacy Enhancing Technologies*, Springer (2006), 36–58.

[2] Brush, A. B., and Inkpen, K. M. Yours, mine and ours? Sharing and use of technology in domestic environments. In *UbiComp*. Springer, 2007, 109–126.

[3] Consolvo, S., Smith, I. E., Matthews, T., LaMarca, A., Tabert, J., and Powledge, P. Location disclosure to social relations: Why, when, & what people want to share. In *Proc. CHI*, ACM (2005), 81–90.

[4] Klemperer, P., Liang, Y., Mazurek, M., Sleeper, M., Ur, B., Bauer, L., Cranor, L. F., Gupta, N., and Reiter, M. Tag, you can see it!: Using tags for access control in photo sharing. In *Proc. CHI*, ACM (2012), 377–386.

[5] Madejski, M., Johnson, M. L., and Bellovin, S. M. The failure of online social network privacy settings.

[6] Mazurek, M. L., Arsenault, J., Bresee, J., Gupta, N., Ion, I., Johns, C., Lee, D., Liang, Y., Olsen, J., Salmon, B., et al. Access control for home data sharing: Attitudes, needs and practices. In *Proc. CHI*, ACM (2010), 645–654.

[7] Mazurek, M. L., Klemperer, P. F., Shay, R., Takabi, H., Bauer, L., and Cranor, L. F. Exploring reactive access control. In *Proc. CHI*, ACM (2011), 2085–2094.

[8] Mazurek, M. L., Liang, Y., Melicher, W., Sleeper, M., Bauer, L., Ganger, G. R., Gupta, N., and Reiter, M. K. Toward strong, usable access control for shared distributed data. In *FAST*, USENIX (2014).

[9] Olson, J. S., Grudin, J., and Horvitz, E. A study of preferences for sharing and privacy. In *CHI Ext. Abs.*, ACM (2005), 1985–1988.

[10] Salmon, B., Schlosser, S. W., Cranor, L. F., and Ganger, G. R. Perspective: Semantic data management for the home. In *FAST*, vol. 9 (2009), 167–182.

[11] Schwartz, T., Stevens, G., Ramirez, L., and Wulf, V. Uncovering practices of making energy consumption accountable: A phenomenological inquiry. *Transactions on Computer-Human Interaction 20*, 2 (2013), 12.

[12] Smetters, D. K., and Good, N. How users use access control. In *Proc. SOUPS*, ACM (2009), 15.

[13] Smith, C. (May 2013 update) by the numbers: 32 amazing Facebook stats. *Digital Market Ramblings* (May 2013).

[14] Spiekermann, S., Grossklags, J., and Berendt, B. E-privacy in 2nd generation e-commerce: Privacy preferences versus actual behavior. In *Proc. EC*, ACM (2001), 38–47.

[15] Ur, B., Jung, J., and Schechter, S. The current state of access control for smart devices in homes. In *HUPS* (2013).