Authentication in the Home

Elizabeth Stobert
School of Computer Science
Carleton University
Ottawa, Canada
elizabeth_stobert@carleton.ca

Robert Biddle
School of Computer Science
Carleton University
Ottawa, Canada
robert_biddle@carleton.ca

ABSTRACT

Smart homes are distinguished not by the technology used in them, but by the relationships between the people using those technologies. These relationships may be social, cultural, or legal, and can affect how people choose to share their homes. One implication of this sharing is the need for authentication. This may involve sharing passwords or accounts. In this paper, we consider the issues of authentication and shared passwords in the home. We conducted a card-sorting study to examine how users think about their accounts and passwords. We found that users consider many aspects when categorizing their accounts, including social, financial, and pragmatic factors.

1. INTRODUCTION

As smart home technology becomes more possible, we must examine what it means to be a smart home, and the security challenges that accompany smart homes. Homes are distinguished from workplaces not only by the activities that take place, but by the differing relationships between the people in the home. Technology in a smart home must support families and personal relationships, and should allow users to interact in a way that supports these relationships.

Although traditional password wisdom tells us never to share our passwords, the home presents numerous contexts in which this advice becomes unrealistic and undesirable. Sharing a home involves social, cultural, and legal relationships that can all have a bearing on how we share information and resources. These relationships and the context of home use present new situations for authentication. We need to make distinctions among our many accounts about whether and how to share access to those accounts. We need to understand how people think about such issues: what do accounts and passwords mean in the home?

In this paper, we explore pressures that may encourage users to share their passwords in the home or in their personal life. We discuss issues that need to be considered in the design of authentication systems for shared smart homes, and we present the results of a study that asked users to categorize their password accounts and discuss the links between various accounts.

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

2. BACKGROUND

In the context of the home, different trust relationships affect the ways that people choose to share their lives, and their passwords. These relationships may include romantic partners (either long or short-term). In 2012, the New York Times reported on a password-sharing trend among teenagers [11]. Teenagers sometimes choose to share the passwords for their Facebook or email accounts with their boyfriends and girlfriends as an expression of trust and love [11]. Boyd [1] speculates that this behaviour is learned from parents who insist on knowing their childrens' passwords. Adult partners also choose to share passwords. Singh et al. [12] examined how people manage money and banking, particularly in the context of relationships, and found that many couples share banking passwords. This sharing had to do with convenience, shared circumstances and trust. Although the practices broke terms-of-service requirements, the personal and social imperatives were seen as more important.

Another relationship that can affect password-sharing habits is the relationship between guardians and their dependents, whether parents and underage children, or between adult children and aging parents. These relationships are sometimes casual and based on trust and convenience, but they may also have legal significance, such as a power of attorney. Kaye [8] shares evidence that some parents insist on knowing their children's passwords, and Boyd [1] describes techniques that families use to moderate the trust relationship, such as having the child put their passwords in a piggy bank that the parent may break in the case of an emergency. Families may also share passwords for services that are used by all family members. Egelman, Brush and Inkpen [3] studied how families share computer user accounts, and found that some families used individual accounts while others shared a single account.

Changing contexts can also affect password sharing – there are situations in which a user may wish to begin sharing their passwords (e.g., in the case of personal injury, or end of life) or stop sharing their passwords (e.g., in the case of divorce). Locasto, Massimi, and dePasquale [9] describe issues that may affect the management of information at the end of life, including the sharing of passwords and account information. Google recently introduced their *Inactive Account Manager* which lets users set up an emergency contact

for accounts that have been inactive for a given period of time. Other changing contexts that occur in the home are the decreases in parental responsibility for the information of children and teens. Parents and children may initially share passwords and account information, but eventually, the child will assume full responsibility for their own accounts. Joint custody of children after a divorce also brings changes to the technological landscape and may affect existing arrangements [10].

Other factors may also influence password sharing. Singh et al. [12] interviewed users with disabilities who reported sharing their banking information with various people in caretaking roles because of accessibility issues. These users reported that they were enthusiastic about online banking because of the improved accessibility.

Culture may also affect the way that people choose to share their passwords. Hofstede [7] identified four major dimensions of cultural differences, which affect peoples' choices and interactions. Other more recent studies differ in their identification of dimensions, but the most consistent through all studies is the dimension that describes differences from individualism to collectivism [5]. The individualism/collectivism dimension describes the extent to which people place importance on belonging to groups (notably, family groups). Individualist societies place high importance on individual rights, while collectivist societies place larger emphasis on the interests of the group. Most computer infrastructure is designed in the United States, which has a highly individualistic culture [7], and the assumptions made regarding computer security likely reflect the values of the American individual. These values may differ from those of other users, particularly in the context of the home and family group (rather than the workplace).

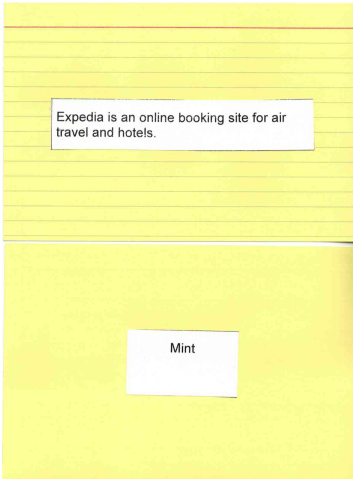
Most password studies have focused on users in individualistic western cultures. Singh et al. [12] studied banking practices among aboriginal Australian users and reported that PIN-sharing within family groups was the norm. This was clearly tied to culture in statements such as "I know that key cards and the members should be confidential, but that's not [our] ... way" (cited by Singh et al. [12]).

3. STUDY

To explore this space, we decided to study how people feel about their existing online accounts. We conducted a card-sorting study to investigate how people think about and organize their accounts. The smart home is not yet a reality, but most people already do have a range of accounts, and we felt we might learn useful information that would inform our understanding of how accounts might work in a smart home. In the context of shared home life, people will need to account for different pressures when managing their accounts and online life. Our study took a high level look at how people go about organizing their accounts, and how they categorize and identify common features among accounts.

In this study, participants sorted a set of accounts into categories of their choice. The accounts were meant to represent a real-life set of website accounts, and each account was printed on an index card. Participants were given the set of accounts and asked to sort them into five categories according to the password used for each account. We chose five as a number of passwords people might reasonably remember, and to influence them to group accounts together. We asked participants to think aloud and describe their decision-making process as they completed the task.

Figure 1: Examples of the account cards used in the study.



The study used a set of 80 cards, each of which had an account name printed on one side and a brief description of the account on the other. We recruited participants from our university community, and chose accounts that seemed plausible for members of that community. They did not correspond to a particular persona, but were chosen to represent a diverse set of users and common accounts. We used 80 accounts to represent a plausible number of accounts for a user to have in real life, based on our examination of our own online accounts. The account names on the cards included university services, common email accounts, e-commerce sites, online services, social networking websites, and others. Figure 1 shows two (different) cards used in the study.

Participants in the study were given the shuffled stack of cards and told to divide them into at most five categories based on a password that would be shared between all of the accounts in the same category. Participants were instructed to physically sort the cards, and were told to "think aloud" to describe their thoughts and decision-making processes as they sorted the cards. Participants were also provided with post-it notes and a pen to make any notes or help them distinguish their categories. After participants had finished their categorization, they were asked to provide a label that described the contents of each category.

The study took approximately 30 minutes, and participants were paid a $5 honourarium for their time. The study was approved by the Carleton University Research Ethics Board.

3.1 Results

Six participants recruited from our campus took part in the card-sorting study. None of them approached the task the same way, and they displayed a variety of categorization techniques and strategies. All participants told us that they currently reused and shared passwords across multiple accounts.

Three participants chose to use all five available categories, while two participants used four categories and one participant divided her accounts into three categories. Some

participants created a large number of categories and later combined them to make fewer categories. The participant who ended up with three categories initially created five categories, but she quickly realized that she did not need the granularity of five categories, and abandoned two empty categories. Another participant initially sorted her cards into the number of categories she found intuitive (eight categories), then combined those categories to fit the requirement of five categories.

In addition to variation in the number of categories, participants also varied in the strategies that they used to categorize their data.

Most participants began with a semantic strategy, linking together accounts that dealt with similar purposes (such as travel, email, or school). However, some participants drew their semantic links too narrowly, causing them to create many specific categories. Most participants noticed this problem early, and adjusted their strategy as they went, either by broadening their semantic categories (e.g., enlarging a "travel" category to include daily transportation accounts) or by changing strategies.

One common semantic grouping seen in the study was to group accounts that dealt with financial issues or money. Participants conveyed this strategy in a number of ways, grouping together bill payments, banking sites, and online marketplaces. Interestingly, participants did not seem to want to distinguish different levels of risk that accompanied various money-related activities. They consistently grouped bank accounts with e-commerce sites (even those where credit card information is not stored), although the potential loss resulting from an attack on an online store is less than that from a bank account.

Another common semantic grouping was social media. This included online social networks (such as Facebook), but most participants also included websites that pertained to activities they might share with a friend (e.g., music, or movie websites), or leisure activities (e.g., online gaming). The "social" label was not taken literally, but interpreted as a broader and more associative category.

Several participants took an affective approach to categorization, distinguishing account categories based on the emotional reactions to the accounts in the category. Some participants created categories of accounts that were linked by the level of pleasure or duty they perceived in a set of items. One participant distinguished a category of "fun money", or accounts where money was spent for pleasure, rather than by necessity. Another participant created a category called "fun stuff", which combined accounts that she deemed entertainment-related or social media. Another affective strategy employed by participants was to categorize accounts by the amount of desired privacy or emotional risk associated with them. One participant separated the three email accounts from all of the other accounts because of the importance of the personal data contained in those accounts. Other participants made similar decisions about the private data and potential for embarrassment in their social media accounts.

Another categorization approach seen in the study was to group accounts by the frequency of logins, i.e., grouping accounts with temporal similarity. Participants distinguished categories for "sites I use often", "occasional use", and "use daily".

Participants varied widely in how they addressed and acknowledged security concerns. One participant did not mention security at all, and when queried, said that she was unconcerned. The majority of participants regarded security as a post-hoc consideration in their classification. After they had created their categories, they then assessed a level of security for that category. Although they did not explicitly discuss security in the formation of their categories, it appeared that they had grouped together accounts with similar levels of concern. One participant used security as her only explicit categorization criterion. She began by assigning a spectrum of five levels of security concern, and sorted the accounts based on the level of security she wished the accounts to have. Interestingly, this participant ended up with only three categories, because her security concerns did not need the granularity of five accounts. She also discussed the kinds of passwords that she would assign to each category, and acknowledged accessibility concerns in her descriptions. She said that she would use more kinds of characters in her most secure password, and that this would be convenient, because she was likely to only log into those accounts from her home computer (where she has a full keyboard). In contrast, she said she was less concerned about the security of her social networking websites, and that because those were websites she was likely to log into from other locations (such as her phone), she would opt for a less secure password with fewer character sets. For very low-priority accounts, she said that she would only use lower-case letters and "just a name", indicating some understanding that dictionary words are more vulnerable to attack.

4. DISCUSSION

The results of the card-sorting study showed that users draw boundaries around their online accounts and identities in different ways. It is clear, however, that users consider social implications alongside security and practicality in the way that they manage their passwords.

In practice, most participants used a combination of strategies to create their account categories. A few strategies were consistently used together: affective strategies were often discussed alongside security concerns, and most participants used semantic strategies alongside another categorization technique. In general, broad themes of categorization seemed to be money-related accounts (with high security concern), accounts with embarrassment potential (i.e., social media) and a general catch-all category for "everything else".

In general, we realized that the considered accounts related to our participants as individuals, first and foremost. We can think of several reasons that things worked out this way. One is that our participants were students, and mainly single young people. This demographic is typically focused on developing their individual identity. We also realized that the selected accounts, while they included home-related accounts, did not strongly situate the study in the home. On the other hand, most accounts situated in the home (such as utilities and services) are typically associated in one person's name. We begin to wonder whether the entire online world is structured around individuals, and this influences the way that users consider these accounts. Even the rise of online social networks (e.g., Facebook) has the individual and their relationships as the primary focus. No wonder that the people reported on by Singh et al. and Richtel [12, 11] stepped outside the capabilities of the systems to create

the structures they felt they needed.

Other, more established, domains have addressed similar issues, at least in limited ways. In banking, for example, joint accounts are a common way of managing home finances. Even roommates might have a shared "kitty" to manage shared expenses. In legal systems, business ventures can be organized as partnerships or corporations, but provisions also exist for shared legal responsibilities in the home. These might include shared ownership of a house or car, shared guardianship of children, or shared powers-of-attorney. On a simpler level, it is commonplace to have shared (or multiple) keys for houses, cars, post office boxes, etc. Homes will typically share one phone number, or internet service account. It seems that there are many existing precedents for letting families share services.

In large organizations, there have also been needs to represent complex arrangements for access to resources. For example, role-based access control (RBAC) [4] was developed to allow the efficient management of access to services and resources. In RBAC, the key concept is the *role* of the individuals, and its attendant rights and responsibilities. More conceptual models for identity management have also been established [6]. Even in a corporate setting, these models have proven challenging [2], and there will be additional challenges in the home. For example, it might be that one account is associated with multiple individuals, it might be that logging is undesirable (for privacy reasons), or balancing true role-sharing (where no user has precedence over another). There may also be complexities relating to the strictness of policy enforcement, and these policies can be more flexible in the home.

While understanding the need for flexibility within home settings, we cannot lose sight of the need for security. When computer systems do not provide the necessary flexibility, users sidestep or avoid security mechanisms to accomplish their primary goals. This is the lesson to draw from the work of Singh et al. [12]. But, while password sharing accomplished a desired flexibility, it still presented dangers. For example, we can see that these behaviours presented risks, particularly when passwords were verbally conveyed to others or conveyed to third parties. Our challenge is to allow the necessary flexibility, while promoting security.

We feel that further research in this area is needed. Research is needed to document examples of authentication, authorization, and access control in real homes, families and shared situations, and to understand how they are managed. We need a better understanding of the new technologies that are being introduced, and the security and privacy needs associated with them. For authentication in the home, needs such as equal access, temporary sharing or access, revocation, and different access models require further consideration. We must be cautious of importing security frameworks directly from business or government, as the pressures governing those models may be quite different and inappropriate in a home context.

5. CONCLUSION

In this paper, we have considered the issues surrounding authentication in the home, specifically password sharing. While this behaviour is generally discouraged, many users continue to share passwords as a way of managing the social, cultural and legal pressures existing in the home. We conducted a card-sorting study to examine how users think about their accounts and passwords, and found that users draw large boundaries around their accounts by considering pragmatic, financial, social and security factors. We discussed how other domains have accommodated similar issues relating to homes, families and shared life.

If we really mean for smart homes to incorporate authentication, we need to come up with mechanisms that support and respect relationships and their dynamic nature. Smart homes are distinguished not by the technology, but by the relationships among the people that live there. As researchers and designers of security mechanisms, we need to take these ideas into account at the design stage. If we do not, users will bypass or avoid the security mechanisms meant to protect them, thereby opening themselves to vulnerability.

6. REFERENCES

[1] D. Boyd. How Parents Normalized Teen Password Sharing. *Zephoria*, Jan. 2012.

[2] R. Dhamija and L. Dusseault. The Seven Flaws of Identity Management: Usability and Security Challenges. *IEEE Security & Privacy Magazine*, 6(2):24–29, 2008.

[3] S. Egelman, A. J. B. Brush, and K. M. Inkpen. Family accounts: a new paradigm for user accounts within the home environment. In *Computer Supported Cooperative Work (CSCW)*, page 669, New York, USA, 2008. ACM Press.

[4] D. Ferraiolo, J. Cugini, and D. R. Kuhn. Role-based access control (RBAC): Features and motivations. In *Proceedings of 11th Annual Computer Security Application Conference*, pages 241–248. sn, 1995.

[5] V. V. Gouveia and M. Ros. Hofstede and Schwartz's models for classifying individualism at the cultural level: their relation to macro-social and macro-economic variables1. *Psicothema*, 12(Suplemento):25–33, Dec. 2000.

[6] M. Hansen, A. Schwartz, and A. Cooper. Privacy and identity management. *Security & Privacy, IEEE*, 6(2):38–45, 2008.

[7] G. Hofstede. National cultures in four dimensions: a research-based theory of cultural differences among nations. *International Studies of Management & Organization*, 13(1/2):46–74, 1983.

[8] J. Kaye. Self-reported password sharing strategies. In *Human Factors in Computing Systems (CHI)*, pages 2619–2622, New York, USA, 2011. ACM.

[9] M. E. Locasto, M. Massimi, and P. J. DePasquale. Security and privacy considerations in digital death. In *Proceedings of the 2011 workshop on New security paradigms workshop*, pages 1–10, New York, USA, 2011. ACM.

[10] W. Odom, J. Zimmerman, and J. Forlizzi. Designing for dynamic family structures. In *The 8th ACM Conference on Designing Interactive Systems (DIS)*, pages 151–160, New York, USA, 2010. ACM.

[11] M. Richtel. Teenagers Sharing Passwords as Show of Affection. *The New York Times*, Jan. 2012.

[12] S. Singh, A. Cabraal, C. Demosthenous, G. Astbrink, and M. Furlong. Password sharing: implications for security design based on social practice. In *Human Factors in Computing Systems (CHI)*, pages 895–904, New York, USA, 2007. ACM Press.