Exploring Reactive Access Control

Richard Shay
Carnegie Mellon University
Pittsburgh, PA USA
rshay@cmu.edu

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

Peter F. Klemperer
Carnegie Mellon University
Pittsburgh, PA USA
pklemper@andrew.cmu.edu

Hassan Takabi
University of Pittsburgh
Pittsburgh, PA USA
hatakabi@sis.pitt.edu

CHI 2010, April 10–15, 2010. Atlanta, Georgia, USA.
ACM 978-1-60558-930-5/10/04.

Abstract

As users store and share more digital content at home, effective access control becomes increasingly important. One promising mechanism for helping non-expert users create accurate access policies is *reactive policy creation*, in which users can update their policy dynamically in response to access requests that cannot otherwise succeed. An earlier study [4] suggested that reactive policy creation may be a good fit for file access control at home. To test this theory, we designed and piloted an experience sampling study in which participants used a simulated reactive access control system for a week. Preliminary results suggest a neutral to positive response to using this kind of system and indicate that reactive policy creation may help meet users' need for dynamic, contextual policy decisions.

Keywords

Access Control, Home Computing, Human Factors, Privacy.

ACM Classification Keywords

D.4.6 Security and Protection, Access Controls

General Terms

Experimentation, Human Factors, Security

Introduction

Users without technical expertise accumulate more and more digital content on their home devices. This increases the risk of unauthorized information disclosure. One promising mechanism for helping these users more easily manage their policies is *reactive policy creation*. In a reactive model, if a user tries to access a resource for which she does not have sufficient permission, she can use the access control system to send a request to the resource owner, who can elect to update her policy and allow the access.

In prior work, users showed interest in reactive policy creation [4]. To examine the depth of this interest, we designed and piloted an experience sampling study to simulate the experience of using a reactive system. For a week, participants received and responded to simulated access requests drawn at random from lists of people and files they provided. Then, we asked each participant about the positive and negative aspects of her experience.

Methodology

Our study included nine adults from the Pittsburgh area without backgrounds in computer science, recruited using craigslist. Unintentionally, we recruited only female participants; we plan to include males in the future. Participants were paid about $45 each depending on participation level.

We modeled our work on a location-sharing experience-sampling study by Consolvo et al. [3]. Our study consisted of an initial briefing interview, a request phase, and a final debriefing interview for each participant. In the briefing, we obtained lists of 8-12 people with whom the participant might share files (*askers*) and 20-30 files the participant has. Asker lists included all household members, a romantic partner if applicable, at least two additional family members and friends, a boss or supervisor, and at least two work or school colleagues. File lists included photos, music, videos, financial files, work or school files, email and text messages, address book information, resumes, and journal files.

For 6-7 days, participants were sent 5-15 emails a day indicating a particular asker requesting a particular file. Askers, files, and message timing were randomly selected using a uniform distribution; asker-file combinations were not allowed to repeat. Participants could ignore, allow, or deny each request. We also asked them to explain their reasoning. Figure 1 shows the response interface.

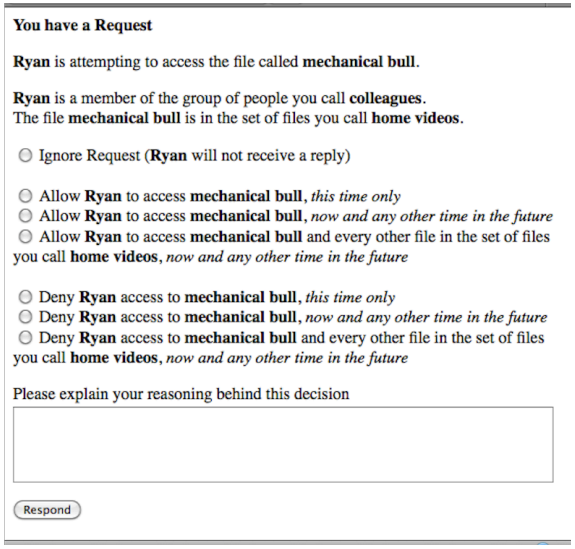

Figure 1: Sample response form. Participants could choose from seven possible response options.

In the debriefing, we gave participants a seven-question Likert survey about their satisfaction with the system and whether or not they would use such a system in real life. We also asked open-ended questions about their overall experience and discussed 8-12 particularly interesting individual responses in detail.

In addition to responding to requests, participants indicated their file sharing preferences using a grid loosely based on Expandable Grids [7]. In the grid, participants labeled each asker-file combination with *yes*, *no*, or *maybe* depending on whether they would be willing to share that file with that asker. Participants were divided into two conditions: five filled out the grid in the briefing, and four in the debriefing.

Preliminary Results

Because this was a pilot study, our results are only preliminary; in addition, our simulated experience does not entirely capture the advantages and disadvantages of using a real reactive system. Nevertheless, our results are encouraging. We have identified two preliminary trends: 1) Participants' ideal policies are often complex, dynamic, and context- dependent. This implies that a reactive model, which can potentially handle changing policy needs more effectively than a traditional proactive model alone, may be a good fit. 2) Participants' opinions of the system were neutral to positive. Most participants identified strong benefits to using a reactive model, at least in some situations. Several had reservations about less attractive aspects of the system, but for the most part these reservations did not outweigh their interest in using it.

Policy Preferences are Complex and Dynamic

Our findings indicate users often have complex, dynamic policy preferences for sharing their files. Among 75 askers for whom participants correctly filled out their grids, only six received uniform access (all *yes* or all *no*). Among 184 completely specified files, 66 were marked uniformly.

Participants also expressed complex policies in their responses to access requests. P11 denied one request for Christmas music, which she was usually willing to share, because the asker "doesn't celebrate Christmas and might be offended." In response to a request from her teenage daughter for tax files, participant P2 said she would want to ask why her daughter wanted to see them before responding. Other participants also said their responses would depend on why the request was made, indicating that people often need more information than just a person and a file to make an access-control decision. Participant P8 sometimes wanted to share files in person rather than through the system, saying "I would rather just show it [an academic file] to her sometime myself on my laptop." In response to a request for contact information, P4 said, "If my stepmother wants my friend's contact information, she needs to personally talk to me." This interest in physical presence or direct contact for sharing echoes a finding from our prior work [4].

In many cases, differences between static (gridded) and reactive policy specification indicate changing policy preferences. P6 approved a file for an asker on her grid, but refused the same combination as a request because "today he's on my blacklist." P2 refused a request for a work document in progress, but marked yes in her grid because the document had since been completed. Overall, about 13% of reactive responses conflicted with gridded responses.

Some participants also used the *ignore* response to avoid difficult policy decisions. P7 ignored a request from her father for a video of her 21st birthday party, assuming he would soon forget about it .

Do People Like Reactive Policy Creation?

Reaction to our simulated system for reactive access control was encouraging, if not definitive. Preliminary results indicate that adding reactive policy creation to the access control mix is a promising research direction. We found that participants enjoyed the system, found it convenient, and would consider using something like it in real life. We found several aspects that participants didn't like as much, but on the whole these aspects did not outweigh the participants' overall positive impression.

In response to a Likert question about whether they enjoyed using the request system, the average response was 5.1 out of 7 (standard deviation 0.78), which shows a strong positive response to using the system. Participants also agreed (mean 5.3 out of 7; standard deviation 1.41) that the system was convenient for them. Most said they would consider using such a system.

We also asked participants whether they would prefer reactive policy specification (represented by requests), proactive policy specification (represented by the grid), or a combination. Three preferred reactive and six preferred the combination; none preferred proactive policy only. One of the most popular reasons to prefer reactive was "because things change." When the interviewer pointed out that proactive policy could be updated as needed, several participants said they would be too "lazy," busy, or forgetful to change their policies. This accords with findings in Bauer et al.'s study of physical access control policy showing that outdated policies often remain operable long after they become obsolete [1]. Other popular reasons for preferring reactive policy included the ability to make case by case decisions and an interest in knowing each time someone wants to access a file.

We also asked participants about potential disadvantages of a reactive system, including social discomfort caused by denying requests, information disclosure via listing available files, and the annoyance of receiving requests. Most participants said they weren't bothered by saying no, as people who sent inappropriate requests should expect to be denied. Participants were more concerned about making file names available, but having the option to exclude some files partially assuaged this concern. Most participants said they received more requests than preferable, but not enough to really bother them; many said they would expect to receive fewer messages in real life. Overall, however, our ability to evaluate these disadvantages realistically was limited.

Related Work

Bauer et al. implemented and tested the Grey system, in which mobile phones are used like keys to open doors [2]. Grey users can delegate authority to others, either proactively or in response to requests; this system demonstrates reactive policy creation can be effective.

Razavi et al. found file-sharing preferences are not sufficiently expressed by static access policies [6]. Instead, access policies can be related to the status of the document within a lifecycle from draft to complete. This result, consistent with our own findings, indicates users have dynamic access-policy preferences.

We modeled our experience-sampling study on work by Consolvo et al. evaluating users' location-sharing policy preferences. This study also found that disclosure decisions can be affected by current feelings toward the requester and that users want to understand why requests are made.

Olson et al. used a grid format to explore people's willingness to share a variety of personal and professional information with different types of people [5]. The authors found that policy preferences could be clustered into sets of similarly-treated people and information.

Limitations and Future Work

We conducted a small pilot study including only nine participants. Our preliminary results are encouraging, and we believe that a continued effort with more subjects will yield valuable information about the potential for a reactive model to improve access policy management.

Inherent Methodology Limitations

Our study design creates some inherent limitations in our ability to draw conclusions. First, we are limited by the fact that no data is actually shared and no real social interactions take place. We ask participants to imagine receiving requests and sharing their files, but they are aware no data is actually at risk. One consequence of this is that a participant may refuse a request in our study, when in real life she might accept it in order to avoid an awkward social situation. On the other hand, participants may casually accept simulated requests, when in real life they might be more careful with their files. Based on our debriefing interviews, we believe our participants took the requests they received seriously and answered carefully, but there is no substitute for reality.

This problem is compounded by our inability to tell participants why a given request was made. Several participants said they might accept requests they found unusual or inappropriate if the asker had a good reason, which we were unable to supply. This may have reduced participants' ability to imagine the system to be real.

Our payment system, in which participants received 25¢ per response, creates another potential limitation. We paid participants this way to replicate partially social incentives to respond promptly to requests received from friends, family, and colleagues. The payment, however, may induce participants to respond to requests even if they find the system annoying, or may reduce their annoyance at receiving requests. We attempted to mitigate this by asking participants about it during the debriefing; our results provide at least some evidence that the annoyance factor did not overwhelm interest in using the system.

Finally, the files in our study were selected by the participants. Because participants selected only a small subset of their files, it is likely they chose not to mention the most sensitive or private items. We tried to mitigate this by asking about a diverse range of files, but we cannot entirely solve the problem.

Beyond a Pilot Study

Running the study at a larger scale will allow us to confirm our preliminary results and perform additional quantitative analysis. For a full-scale study, we will make sure to recruit a more balanced population including men and women, as well as more people with children and more people over 40.

We would like to examine quantitatively whether using reactive policy creation affects people's access-policy decisions, which files and askers a reactive system would be most useful for, and how often policies change. We would also like to test whether participants' general privacy orientation or tech-savviness affects their policy decisions or their interest in a reactive system.

We would also like to examine the time lapse between when a request is sent and when a response is received. Do responses take longer during work hours or on weekends? Would using text messages instead of email to send requests affect the lag in response time?

Another interesting direction might be whether we can make predictions about access decisions based on information about the asker's relationship to the participant and the type of file being requested.

Finally, we would like to include a longer request phase. In the pilot, we sent participants many messages per day for a week; fewer requests over a longer time period might be a more realistic scenario.

Acknowledgments

The authors wish to thank the entire Home Storage Project team, of which this effort is a part; and CyLab. Thanks to Meghana Koushik for her contribution to our study. Thanks to Microsoft Research and the National Science Foundation for funding assistance. Special thanks to Lorrie Faith Cranor; this project began as a student project in her Usable Privacy and Security class, and she has provided guidance throughout the process.

References

[1] L. Bauer, L. Cranor, R. W. Reeder, M. K. Reiter, and K. Vaniea. Real life challenges in access-control management. In *CHI 2009: Conference on Human Factors in Computing Systems*, pages 899–908, Apr. 2009.

[2] L. Bauer, L. F. Cranor, M. K. Reiter, and K. Vaniea. Lessons learned from the deployment of a smartphone-based access-control system. In *SOUPS '07: Proceedings of the 3rd Symposium on Usable Privacy and Security*, pages 64–75, July 2007.

[3] S. Consolvo, I. E. Smith, T. Matthews, A. LaMarca, J. Tabert, and P. Powledge. Location disclosure to social relations: why, when, & what people want to share. In *CHI '05: Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 81–90, New York, NY, USA, 2005. ACM.

[4] M. L. Mazurek, J. Arsenault, J. Bresee, N. Gupta, I. Ion, C. Johns, D. Lee, Y. Liang, J. Olsen, B. Salmon, R. Shay, K. Vaniea, L. Bauer, L. F. Cranor, G. R. Ganger, and M. K. Reiter. Access control for home data sharing: Attitudes, needs and practices. Technical Report CMU-CyLab-09-013, CyLab, Carnegie Mellon University, Oct. 2009.

[5] J. S. Olson, J. Grudin, and E. Horvitz. A study of preferences for sharing and privacy. In *CHI '05: CHI '05 extended abstracts on Human factors in computing systems*, pages 1985–1988, New York, NY, USA, 2005. ACM.

[6] M. N. Razavi and L. Iverson. A grounded theory of information sharing behavior in a personal learning space. In *CSCW '06: Proceedings of the 2006 20th anniversary conference on Computer supported cooperative work*, pages 459–468, New York, NY, USA, 2006. ACM.

[7] R. W. Reeder, L. Bauer, L. F. Cranor, M. K. Reiter, K. Bacon, K. How, and H. Strong. Expandable grids for visualizing and authoring computer security policies. In *CHI '08: Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems*, pages 1473–1482, New York, NY, USA, 2008. ACM.