Poster: Exploring Reactive Access Control

Michelle L. Mazurek*
mmazurek@andrew.cmu.edu

Peter F. Klemperer*
pklemper@andrew.cmu.edu

Richard Shay*
rshay@cmu.edu

Hassan Takabi†
hatakabi@sis.pitt.edu

Lujo Bauer*
lbauer@cmu.edu

Lorrie Faith Cranor*
lorrie@cs.cmu.edu

*Carnegie Mellon University
Pittsburgh, PA

†University of Pittsburgh
Pittsburgh, PA

1. INTRODUCTION

As users store and share more digital content at home, effective access control becomes increasingly important. One promising approach to 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 [8] suggested that reactive policy creation might be a good fit for file access control at home. To examine this theory in more depth, we conducted an experience-sampling study in which participants used a simulated reactive-access-control system for a week.

Our results bolster the case for using reactive policy creation as one of the modes by which home users specify access-control policy for files. We found both quantitative and qualitative evidence of dynamic, situational access-control policies that are hard to implement using traditional models but that reactive policy creation can facilitate. Our study showed that the reactive model supports many of our participants' policy creation needs, including the desire for more control and interactivity. While we found some clear disadvantages to the reactive model, they do not seem insurmountable. In fact, we found that some seemingly obvious disadvantages had only a minor impact on the usability of our simulated system and on user satisfaction. Based on these results, we believe that reactive policy creation has considerable potential as one component of a usable access-control system. The design of our simulated system also helps pave the way for the design of future, more realistic, reactive-policy-creation mechanisms.

2. METHODOLOGY

Our study included 24 adults from the Pittsburgh area without backgrounds in computer science, recruited using craigslist. Participants were compensated $10 for the briefing interview, $15 for the debriefing interview, and 25 cents per response to a reactive request.

We modeled our work on a location-sharing experience-sampling study by Consolvo et al. [4]. Our study consisted of a briefing interview, a request phase, and a 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 diverse files the participant has.

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. Participants could ignore, allow, or deny each request, as well as modify or fine-tune policy that would affect other users and files. We also asked them to explain their reasoning. Participants were aware that our requests were simulated, and that no files were actually being shared.

In the debriefing, we gave participants a seven-question Likert survey about their experience 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 some individual responses in detail.

Participants also indicated their file sharing preferences using a grid. 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. This corresponds to traditional proactive access control. About half of our participants filled out the grid before responding to requests, and about half after.

Participants filled in a total of 4481 grid entries. Of these, 2518 were *yes*, 1518 were *no*, and 445 were *maybe*. Individual choices ranged from 100% *yes* to 72% *no*. Responses to requests showed a similar distribution, with 913 *allow*, 406 *deny*, and 41 *ignore* out of 1360 total responses.

3. RESULTS

Our results—both qualitative and quantitative—show that reactive policy creation is a promising access-control mechanism that supports people's changing policy needs.

Policies are dynamic and situational. Many access policies that users wish to enforce cannot easily be supported by traditional approaches to policy configuration. File-sharing policies can and do change relatively often, in response to a wide variety of factors. Participants demonstrated this dynamism by setting *maybe* policies, selecting one-time-only responses to requests, and commonly evincing policy changes during the study. Participants used *maybe* for 10% of grid policies, while 29% of responses were one-time-only. 12% of responses differed from the corresponding grid entry, demonstrating policy shifts over time. Most participants said they considered why a request was made before responding. For example, one participant denied a friend's request, but said, "if she has a good reason to see it then I might allow her." In fact, despite knowing our requests were simulated, some participants fabricated reasons for the requests and then responded in the context of those reasons. We believe reactive policy creation is a good fit for these dynamic policy needs.

Reactive policy creation is popular. Participants enjoyed using our system (Likert mean 4.9 of 7), found it convenient (Likert mean 5.3 of 7), and would consider using something like it in real life (20 of 24 people). Most said the system was quick and easy to use; many also said it could be used to share files more easily or conveniently than currently available mechanisms, including current ad-hoc reactive processes. Participants cited flexibility for dynamic policy needs and added control over their files as benefits.

Concerns can be mitigated. Despite our worry that requests would be annoying, most participants were not particularly bothered by receiving five to 15 requests per day (Likert mean 3.3 of 7). Over the course of our study, participants generally responded to requests in a timely manner, despite the fact that our scheme for compensating participants did not encourage such behavior. We therefore expect that annoyance and latency in real-life scenario will not be an unsurmountable problem.

Other interesting results. Reactive policy creation provided an added sense of control. Six participants said the model allowed them to keep track of who was accessing which files. Others liked the idea of being asked permission. Moreover, some participants said the reactive model helped them make better decisions.

Some participants used the *ignore* response option to circumvent making a direct response to certain requests, for example avoiding socially awkward *deny* responses.

About a quarter of participants expressed concern regarding our hypothetical system's security, such as worrying that a request might be from someone impersonating the indicated asker. This is despite our explicitly stating that "no one can access [your files] without your permission," and despite the requests being simulated. This suggests people may have trouble trusting new access-control systems.

4. LIMITATIONS

We believe the following limitations are important to note, but we don't think they undermine our overall results.

Our methodology asked participants to use their imagination. When a subject opted to share his or her data using our design, he or she knew that no data is actually being shared. However, based on their reasons for responses, and based on our interview results, we believe participants took their responses seriously.

In another limitation, we paid a quarter per response, which could have led participants to continue responding even after becoming annoyed with the system. We attempted to mitigate this by asking participants their opinion of the system. The favorable responses provide evidence they were not so annoyed that they would discontinue use of the system without payment. Further, in real life, while there is no direct payment generally involved in a request for a file, there is a genuine social incentive to respond to such requests. If we removed our incentive to respond, then there may have been less motivation than would exist in reality.

Finally, the files in our study were selected by the participants. It is possible they may own files that they did not feel comfortable mentioning to researchers. We tried to mitigate this by asking about a diverse variety of files.

5. RELATED WORK

Egelman et al. designed a new model for home computer accounts [6]. Their design takes advantage of the fact that home users may not need controls as strict as those required in traditional corporate environments. Ahern et al. examined how users managed privacy settings related to online photo sharing; they found that users' decisions are driven by concerns about security, social disclosure and convenience [1].

Bauer et al. implemented the Grey system, which allows mobile phone users to delegate reactively authority to open locked doors [3]. A subsequent study verified that Grey helps users implement their ideal policies more accurately than they could with keys, in part because of its near-real-time reactive features [2]. In an earlier study, we found the idea of reactive policy creation resonated with home users' desire to align digital access control with the social norm of asking permission [8]; that finding inspired this paper.

Our use of experience-sampling methodology was inspired by Consolvo et al.'s work examining location-sharing preferences [4]. The experience sampling method was developed by Csikszentmihalyi and Larson [5]. Our study asks participants to imagine a system where files are easily shared among personal computing devices; distributed file systems like HomeViews [7], and Perspective [9] aim to make this paradigm accessible to consumers.

6. REFERENCES

[1] S. Ahern, D. Eckles, N. S. Good, S. King, M. Naaman, and R. Nair. Over-exposed? Privacy patterns and considerations in online and mobile photo sharing. In *Proc. CHI*, 2007.

[2] L. Bauer, L. Cranor, R. W. Reeder, M. K. Reiter, and K. Vaniea. A user study of policy creation in a flexible access-control system. In *Proc. CHI*, 2008.

[3] L. Bauer, L. F. Cranor, M. K. Reiter, and K. Vaniea. Lessons learned from the deployment of a smartphone-based access-control system. In *Proc. SOUPS*, 2007.

[4] 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 *Proc. CHI*, 2005.

[5] M. Csikszentmihalyi and R. Larson. Validity and reliability of the experience-sampling method. *J Nerv Ment Dis*, 1987.

[6] S. Egelman, A. Brush, and K. Inkpen. Family accounts: A new paradigm for user accounts within the home environment. In *Proc. CSCW*, 2008.

[7] R. Geambasu, M. Balazinska, S. D. Gribble, and H. M. Levy. HomeViews: Peer-to-peer middleware for personal data sharing applications. In *Proc. SIGMOD*, 2007.

[8] M. L. Mazurek, J. P. 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. In *Proc. CHI*, 2010.

[9] B. Salmon, S. W. Schlosser, L. F. Cranor, and G. R. Ganger. Perspective: semantic data management for the home. In *Proc. FAST*, 2009.