
User Experiences with Sharing and Access Control

Tara Whalen

Faculty of Computer Science
Dalhousie University
Halifax, NS B3H1W5 Canada
whalen@cs.dal.ca

Diana Smetters

Palo Alto Research Center
3333 Coyote Hill Road
Palo Alto, CA 94304 USA
smetters@parc.com

Elizabeth F. Churchill

Palo Alto Research Center
3333 Coyote Hill Road
Palo Alto, CA 94304 USA
elizabeth.churchill@parc.com

Abstract

The sharing of network-based information is a key component of recreational and professional interaction, from email attachments to P2P networks. However, people need to accommodate technical challenges in successful and *secure* content sharing. In particular, people have to manage access control policies that are both social and technical: deciding what to share and who to share it with, and how to technically effect their decisions. In this paper, we focus on the usability of access control: how people manage file sharing among various groups, organizations, and tasks. We present survey and interview data regarding content sharing and content protection, and discuss the implications for the design of networked collaboration tools.

Keywords

Security, access control, sharing, collaboration.

ACM Classification Keywords

H.5.3: Computer-supported cooperative work; D.4.6: Access controls

Introduction

Information and resource sharing through networked technologies has become a central part of many people's lives. They share digital photos with their families, and project proposals with their colleagues. However, people often need to set limits on who can

Copyright is held by the author/owner(s).

CHI 2006, April 22–27, 2006, Montreal, Québec, Canada.

ACM 1-59593-298-4/06/0004.

(or cannot) see or use a shared resource. This is traditionally the job of an access control system, such as those implemented by file permissions or access control lists.

One active and growing area of research concerns people's problems with setting restrictions on who can and who cannot access digital content. Evidence suggests that configuring file permissions in access control systems difficulties is hard for users who often don't fully understand the underlying access model(s). Similarly, setting (or encountering) restrictions on file access can interrupt or interfere with the primary task at hand [2].

However, while a few studies have attempted to design better interfaces for existing access control systems [1, 3, 4], there have been no systematic user studies of the basic access control models deployed in the vast majority of current systems – or, for that matter, the social control models that people are tacitly trying to apply in their particular activity contexts when they use these security mechanisms. In systems, the implemented models generally have tremendous expressive power, potentially leaving users awash in a sea of very fine-grained access control settings. Further, current systems often require users to manage these settings in isolation from any helpful application context. Finally, file permissions are often invisible once set, and default permission settings may be unknown.

Our goal is to offer recommendations for design that will lead to improved usability for access control mechanisms. We would like to support a wide variety of new types of sharing, using whatever security technology will best support users. In this paper we

consider the problems users routinely face from technical issues in access control. We report results from a survey and a number of in-depth field interviews. Our studies took place within a medium-sized (~200 employees) industrial research laboratory in the United States, which is involved in establishing and maintaining contracts with external collaborators and customers. There is a high level of technical competence within the organization; employees use a variety of applications and systems.

Surveying users' experiences and ideas

To address the issue of users' experience of file sharing and access control, we first conducted an online survey to gather information on how and why people share digital files; the types of information shared; and how, when and why people limit access to those files. We received 56 responses from people working in diverse areas within the organization.

Unsurprisingly, our survey results indicated that file sharing is a common practice amongst our survey respondents. Email attachments were overwhelmingly the most frequently used method for sharing with work colleagues (55 respondents, or 98% of our sample), followed by network file sharing (e.g., Windows file share; 31 respondents or 55%). Commercial content management systems (e.g., Xerox's DocuShare) were used by 14 respondents (25%), and portable devices (e.g., USB tokens) by 14 respondents (25%).

Thirty-seven respondents indicated explicitly in comments that they took measures to protect files from colleagues and friends. Free-form responses revealed several methods for restricting access: Passwords (includes user account login; trust/social conventions;

permissions/access control lists; physical controls (e.g., safeguard in office or on person); encryption: obscurity (e.g., giving files innocuous names, hidden directories); and deleting/relocating sensitive files. Unsurprisingly, passwords dominated the list; users generally have password protection for their work accounts, and often for their personal accounts as well. We were particularly interested in the reliance on trust, or social convention, to protect information from unwanted access; there is an expectation that people will not pry into personal files. People made comments like:

"I trust the insiders not to be evil"

"...mostly just trust that other people won't snoop into my personal items."

"...on work machines...using protection mechanisms available though I realize that many people can defeat them here so I consider it to be something of an advisory/accident prevention that works in polite company"

Thirty-seven out of 51 people (67%) indicated they performed some management of permissions on files. Broadly, reasons given for restricting access were:

- controlling access so a only limited group (or organization) can access files: 14 responses
- prevent modifying/deleting files: 12 responses
- keeping files private to only me: 7 responses
- resetting system defaults: 3 responses

Eight people mentioned the need to allow temporary access to files, either within the organization or when working with external partners. Of the 37 respondents who reported resetting permissions, these people broadened and narrowed access in fairly equal amounts. These results demonstrate that access control is about

more than just locking files down: people also reset permissions in order to be more open in their sharing. We also asked about the cases in which people stopped sharing files, either by removing them or by resetting permissions to prohibit sharing. The main reasons cited for prohibiting sharing were: changes in work team; changes in content required stricter control; changes in organization (e.g., parts of company should no longer have access to certain files); and temporary usage.

Our results suggest strongly that permissions are not set once and left alone: changes in the work environment, as well as the need for short-term sharing, will require people to repeatedly interact with access control settings over time.

When asked for details about file permission management, some people discussed problems they encountered. Many of these involved heterogeneous systems or technical complexity:

"Previously, ACLs on windows filesystems would get munged when trying to recursively set access rights to files in directory trees from a different OS than running on the filesystem."

"Cross platform issues, where users were not recognized the same from their Mac and their PC. Hassle of going through a terminal window to reset permissions on a Unix server."

People also described how access permission problems interfered with work. Forty-one people reported problems (73%), a few of which were very minor or infrequent, while others (7 respondents) expressed a great deal of frustration. The level of irritation rises sharply when access control problems recur:

"This is a constant problem for me. I am a web developer, but I am not an administrator on the production server. This means creating a new web application, or adjustments to permissions often take days."

Summary observations from the survey

The survey results indicate that even in a highly technically competent group, with good technical support, problems arise regularly, leading to frustration and difficulty. We found little correlation between skill level and experience, although it was clear that technical competence led to improved understanding of the issues at large. This undermines the myth that only users with little skill are stymied by issues of file access and restriction. Further, we note that users are well aware of the periodic need to access and to "keep tabs" on files, but this management and monitoring must be carried out in addition to the focused work that is taking place. Finally, we note that the workplace supports many different systems as a necessity – trying to force a single solution would severely affect the work.

Follow-up interviews on access control

In order to gather more in-depth, personalized information, we gave survey respondents the option of being contacted for a follow-up interview. Thirty-eight of the 56 respondents agreed to be interviewed, from whom we selected 12 individuals. The people in this subgroup are a representative sample of roles in the organization, amount of career and technical experience, and the attitudes and behaviors around security described in survey responses. Interviews took place in people's place of work (typically but not always their offices), were semi-structured and conversational and took approximately one hour. Questions were tailored to the interviewee's occupation and role in the

organization, while focusing on common job tasks; handling of sensitive data; sharing data over email; file management; and security concerns and annoyances. Interview transcripts were analyzed using grounded theory methodology.

Accessing access control

Access control is often discussed in terms of operating-system level methods: specifying rights on objects, such as file permissions. Some people (11/12) did set explicit file permissions, but said that this was an infrequent practice. Generally the people who manage direct file permissions have technical jobs that also involved handling of confidential data:

"Sometimes I have confidential files that are customer data...we maintain our own file servers, we put appropriate permissions on it – which says only our group can get at it"

Many applications provide mechanisms for controlling access to content. Three people in our study protected documents by converting them to a read-only format such as PDF, or using document locking or encryption, available in such programs as Adobe Acrobat. There are two distinct advantages to this approach: ease of use, and portability. The reasons for "locking" a document, or making it read-only, varied. In some cases, locking prevented undesirable changes to something they created, ensured proper attribution, and prevented modification of official documents:

"I like to do PDFs...so people can't change it...if you want changes, let me know and I'll make them for you...since I have a graphic design background...I want it to look the way I intended it to look."

"I'll send a PowerPoint [presentation] to somebody, and it'll be locked, and they can use it. It'll have my name on it,

that's fine, use it – but it has my name on it and you can't take my name off of it."

"If it's a letter, I'll always do a locked PDF. Any letters that I write and sign, I'll make a PDF and I'll lock it, and send it. [Or] if my boss signs it or anything like that."

Our survey results supported the notion that email attachments were the preferred method for file sharing. Interviewees mentioned the convenience of email made it a good choice for sharing:

"Email's the easiest...it's fast, and you get it right away. You don't have to go look for it on the server, you don't have to tell somebody some path...instant gratification"

Despite the ease of use, there are some drawbacks to this method: files may be too large for the system, version control becomes a problem, or documents may even be sent to the wrong recipient:

"I get emails for [person with similar username] all the time. And I get confidential data sometimes."

A recurring theme in both the survey and the interviews was the degree to which social conventions governed how access control was managed. In many cases, this was based on trust in colleagues, or in the organizational or group cultures that defined appropriate access:

"...we have a shared repository of software that we work on. We do access control on it based on 'who does what.' Your ability to write any particular directory is implicit...if I need to change something in a piece you work on, I...go down the hall and talk to you about it."

In these cases, colleagues had the technical ability to modify shared data, but did not do so. The conventions that evolved within this organizational culture permitted

social-based access control: technical barriers did not have to be put in place.

Sharing with "insiders" and "outsiders"

Collaboration among individuals, groups, and organizations poses challenges for access control. The distinction between "inside" and "outside" is not always clear-cut, particularly when working with other institutions. Our interviewees discussed their experiences with managing corporate partnerships across group and organizational boundaries:

"...we put access controls in place at times...for access from outside [our] local networks...And it's a pain to have to do that kind of stuff...Those of us...responsible for making the change did ask, 'Do we really have to do this?' It was not clear there was a need..."

Whether due to corporate security policy conflicts or technological limitations, access control can interfere with collaboration. Creating a boundary that is permeable, yet still prevents undesirable leaks, remains a challenge.

Summary observations from interviews

In keeping with related work, our respondents agreed that access control interfered with their productivity, and that they too had problems with setting permissions correctly. Furthermore, our interviews revealed a wide range of "mental models" or belief systems around digital content protection and a concomitant range of practices. We were mildly surprised about this range within the bounds of one relatively small organization. When we evaluated the interview transcripts from a design perspective, it was notable that people locked documents with the same application they used to create it, which fit quite seamlessly into workflow. It

was noted that a document moving between two separate file systems (e.g. over email) cannot carry file permissions with it, which mandates a different approach to access control. Having the permissions handled by the application sidesteps this problem. People also wanted documents to more clearly reflect the permissions they had set; document interface feedback was considered to be lacking.

Discussion and Design Implications

Our study results suggest design guidelines to improve methods for socially appropriate content protection. We note these are not solutions, but rather are guidelines for evaluating new proposals and prototypes as the design space is elaborated:

1. Fit access control management into the user's tasks: make security fit seamlessly into task at hand. Take advantage of application context to simplify and clarify security tasks.
2. Make access control decisions visible: setting access permissions can be difficult and error-prone, so make it easy to see what has been done.
3. Make the controls themselves simple to manage: make changes easy to perform (e.g., not beneath several levels of menus), even if they are infrequent. Provide controls at an appropriate level of granularity: flexible enough to accomplish common user tasks, but not confusingly complex. Granularity may be current-setting specific and requires support for customization.
4. Support, rather than replace, social controls: social conventions are a powerful, real-world tool for managing appropriate access, which can provide a simple and flexible shorthand for access policies.
5. Design for sharing across organizational and file system boundaries: an overall document management

system can handle tasks such as version control as well as prevent errors (such as sending confidential files to the wrong recipient).

6. Allow users to choose from a palette of sharing and security tools: people will choose the option that is easiest to use that still meets their needs. Make sure that choice is also secure.

Future Work

In this paper, we have presented the results of a survey and field interviews regarding people's experience with what they consider to be *appropriately* secure digital content sharing. These data have enabled us to elaborate a set of commonly occurring issues that we will use to systematically drive the design and development of secure file sharing prototypes to explore the design space further. We are developing prototypes for a file sharing application, which will go through a process of user evaluation to determine how well they support usable access control.

References

1. Brostoff, S., Sasse, M.A., Chadwick, D., Cunningham, J., Mbanaso, U., and Otenko, S. R-What?: Development of a Role-Based Access Control (RBAC) Policy-Writing Tool for e-Scientists. *Software—Practice & Experience* 35, 9 (2005), 835–856.
2. Cranor, L.F. and Garfinkel, S. *Security and Usability*. O'Reilly & Associates, Sebastopol, CA, USA, 2005.
3. Reeder, R.W. and Maxion, R.A. User interface dependability through goal-error prevention. In *Proc. Int'l Conf. on Dependable Systems*, IEEE Computer Society (2005), 60–69.
4. Zurko, M.E. and Simon, R.T. User-Centered Security. In *Proc. New Security Paradigms Workshop*, ACM Press (1996), 27–33.