Laissez-faire file sharing

Access control designed for individuals at the endpoints

Maritza L. Johnson
Columbia University
maritzaj@cs.columbia.edu

Steven M. Bellovin
Columbia University
smb@cs.columbia.edu

Robert W. Reeder
Microsoft
roreeder@microsoft.com

Stuart E. Schechter
Microsoft Research
stus@microsoft.com

ABSTRACT

When organizations deploy file systems with access control mechanisms that prevent users from reliably sharing files with others, these users will inevitably find alternative means to share. Alas, these alternatives rarely provide the same level of confidentiality, integrity, or auditability provided by the prescribed file systems. Thus, the imposition of restrictive mechanisms and policies by system designers and administrators may actually reduce the system's security.

We observe that the failure modes of file systems that enforce centrally-imposed access control policies are similar to the failure modes of centrally-planned economies: individuals either learn to circumvent these restrictions as matters of necessity or desert the system entirely, subverting the goals behind the central policy.

We formalize requirements for *laissez-faire* sharing, which parallel the requirements of free market economies, to better address the file sharing needs of information workers. Because individuals are less likely to feel compelled to circumvent systems that meet these laissez-faire requirements, such systems have the potential to increase both productivity *and* security.

Categories and Subject Descriptors

K.6 [**Management of Computing and Information Systems**]: System Management, Security and Protection, Economics; H.1.2 [**Models and Principles**]: User/Machine Systems—*Human Factors*

General Terms

Security, Human Factors, Economics, Management

Keywords

File sharing, access control management

NSPW'09, September 8–11, 2009, Oxford, United Kingdom

1. INTRODUCTION

Despite decades of research into shared file systems, email remains an enormously popular way to share files. Prior research has shown that email is used more frequently than other sharing mechanisms [5, 29] and that many users choose email as their primary sharing mechanism [31]. Our anecdotal experiences at Microsoft align with these findings; even those individuals and groups we work with that primarily use shared file systems (shared folders or SharePoint) inevitably resort to email attachments when access controls interfere with sharing.

Like many before us, we set out to enumerate the user requirements that lead users to circumvent the file sharing systems prescribed by their organizations. This effort was part of a larger effort to retrofit an existing file sharing system to better meet the needs of *individual* knowledge workers; our goal was to make Windows shared folders as easy to use as it is to attach files to email. As we enumerated the needs of individual knowledge workers we discovered surprising resemblances to the economic freedoms and other requirements that are essential to empowering individual workers in market economies. These economic parallels provide theoretical grounding not only to explain recent survey and interview results, but also to show that this circumvention of centrally-managed access control is inevitable.

Indeed, both centrally-planned command economies and file sharing systems with centralized access control share similar failure modes. Centrally-managed policies hinder individual productivity and give individuals less incentive to participate in the system. As a result many individuals either flee the system or subvert central planners as a matter of necessity. In centrally-planned economies the consequences of failures include lost productivity, emigration, and the loss of goods to underground markets.

When users opt for alternatives to organizations' prescribed systems for storing and sharing files, the organization will no longer be able to audit who has accessed the files, ensure these files are stored in a secure manner, back up files, or otherwise protect their integrity. Thus, overly restrictive access control policies may negatively impact not only productivity, but security as well.

For example, restrictions on where shared data can be accessed often lead users to a dangerous circumvention of these policies: storage of data on laptops. Of the 570 data breaches reported to the Open Security Foundations DATALOSSdb in 2008, 116 (20%) were attributed to information

stored on laptops that were stolen, resulting in an aggregate loss of 2.6 million individual records [18].[1]

USB sticks are another example of a mechanism for sharing and transporting data that is attractive for its flexibility when compared to overly-restrictive file sharing systems. Alas, USB memory sticks are easily lost and pose a growing malware threat [27], yet when Beautement *et al.* interviewed 17 employees of both HP Labs and Merrill Lynch about their use of USB memory sticks, all reported using them [2]. The participants from Merrill Lynch reported using these sticks for the purpose of transporting information.

A particularly dangerous workaround for access control restrictions is to share a password or other credential for an authorized account (e.g., your own) with the intended delegate. In interviews with students and technology workers by Weirich and Sasse, participants reported sharing passwords when they deemed it necessary to complete their work [30].

The temptation to circumvent policy that overly restricts productivity can also be seen in the U.S. nuclear weapons complex. Tober and Hoffman's book on the Wen Ho Lee case [28, p. 294] quotes a weapons physicist explaining ways "to circumvent some laws we thought were too restrictive, to get some work done."

Even when secrets of national security are at risk, the costs of access controls that fail to meet the needs of knowledge workers may outweigh the benefits. The fundamental assumption of many security practitioners, "that the risk of inadvertent disclosure outweighs the benefits of wider sharing" was faulted by the National Commission on Terrorist Attacks Upon the United States (a.k.a. The 9-11 Commission) in its investigation of why the U.S. intelligence community failed to discover the 9/11 plot [17]. It concluded that these "Cold War assumptions are no longer appropriate."

We are not the first to observe the connection between central planning in economies and in information sharing systems. Jimmy Wales, co-founder of Wikipedia, reports being influenced by Nobel Economics Laureate Friedrich Hayek's classic essay *The Use of Knowledge in Society* [8], in which Hayek argues that centrally-planned economies were inherently inefficient because only individuals "on the spot" (or at the "endpoints", in the networking parlance used by Wales) maintained the local knowledge necessary to make decisions [13, 23]. Hayek's arguments have made Wales wary of attempts to change Wikipedia in ways that would "centralize something that can be left decentralized" [23], including access control.

We argue that Hayek's arguments for moving control to the endpoints is not only applicable to open systems like Wikipedia, but can be applied more generally to include closed systems as well. Given the negative impact on both security and productivity when file sharing systems impose access control mechanisms that undermine individual information workers, we develop a set of requirements for *laissez-faire* access control: access control that will let individuals do what they need to do get their jobs done.[2] These requirements are ownership, freedom of delegation, transparency, dependability, and minimization of friction.

[1]Numerous examples of USB drives containing information are also detailed, but are less easy to quantify as they are not explicitly separated from media stolen from secured locations.

[2]Laissez-faire is French for "let do".

We formalize each of the requirements that define laissez-faire sharing in Section 2, presenting each requirement with its economic analog. As we present each requirement we describe how email-based file sharing fares in meeting it. In Section 3 we detail an ongoing effort to layer laissez-faire email-based sharing on top of Windows folder sharing. We explain how the underlying architecture and deployment choices of desktop/workstation file systems impose barriers that interfere with our attempts to overlay a laissez-faire model. In Section 4 we discuss how users' circumvention of file sharing technologies that fail to meet these laissez-faire requirements drives an evolutionary process away from centralized access control. We discuss further related work in Section 5 and conclude in Section 6.

2. DEFINING LAISSEZ-FAIRE SHARING

Laissez-faire sharing is defined by five properties – ownership, freedom of delegation, transparency, dependability, and minimization of friction – which we will now define in detail. After introducing the definition of each property we will discuss its analog in economics and work an example, examining how email-based file sharing fares in achieving the desired property.

Ownership

> *The owner of a document, initially the individual who creates it or first introduces it into a sharing system, must not be required to sacrifice rights in order to add the file into the system.*

In a market economy, private property rights provide an incentive for *production*: the introduction of goods into the economic system through labor. When individuals do not enjoy the fruits of their labor underground markets inevitably emerge to compete with those that are officially sanctioned. In file systems, similar competition exists among prescribed file sharing mechanisms and unsanctioned mechanisms. Information workers may have the opportunity to store their work on a file system local to their device, a portable storage device, the shared file system provided by their organization, or even systems external to the organization for which they are working. These individuals are less likely to choose to introduce a document into a prescribed file sharing system if doing so necessitates forfeiting rights, such as the right to easily access the file from the location or device of their choosing. For example, if the owner of a file cannot access a file share from home, or if remote access is especially burdensome, he or she may instead store the file on a USB drive, send it by email, or place it on a cloud storage website.

Strong ownership may have something to do with the popularity of email attachments, as email provides as much ownership as is possible within a file sharing system. By attaching a file to an email one may sacrifice the ability to permanently delete the data, prevent readers from forwarding it to others, or prevent others from editing their own copy. However, these sacrifices are all but unavoidable for any mechanism of sharing information; the perpetual failures of technologies designed to prevent sharing of software, music, and movies (digital rights management technologies) illustrate just how hard it is to prevent those granted access to read a file from duplicating, modifying, or redistributing copies if they are intent on doing so.

Freedom of delegation

The owners of a document may grant (delegate) or deny any or all rights – including the right to further delegation or even full ownership – to whomever they so choose, regardless of organizational or administrative boundaries.

In a market economy, the freedom to contract guarantees a good's owner the right to share or sell the good to anyone she chooses under any mutually agreeable terms. Free trade seeks to extend these rights beyond local, state, or national boundaries. When rules or laws interfere with the freedom to contract, artificially limiting the value that the owner of a good can legitimately obtain for it, he or she will be tempted to subvert these rules and exchange the good via an underground economy.

Similarly, an owner of a document who is prevented from sharing it with collaborators by the security policies of the prescribed sharing system (e.g. a Windows share) may subvert these rules by using an alternate sharing mechanism (e.g. email attachments). The freedom of delegation requirement goes beyond discretionary access control (as defined by Landwehr [11] or Ferraiolo [6]) in that the right to delegate must be guaranteed for all owned files and not constrained by organizational boundaries. Furthermore, when expressing a delegation policy in terms of groups that may be owned or controlled by others, it must be possible to define the terms of the policy as pertaining to the current membership of a group. If one cannot, the group-owner may retain greater control over policy than is desired by the file's owner.

While the freedom to restrict access or further delegation may initially seem counter to a laissez-faire philosophy, such restrictions are the foundation of intellectual property law designed to spur innovation.

Freedom of delegation is one of the most attractive properties of email attachments, as files can be shared with anyone (or any group) with an email address.

Transparency

The owners of (and ideally all contributors to) a document must be able to quickly and easily find and comprehend the rights associated with it, including such meta-rights as delegation. All changes to the document or its rights must be attributable to the individual who made the change.

In a market economy, transparency of ownership rights is essential in enabling investors to contract those rights. Transfers of rights in market economies are made explicit via deeds and licenses issued by states and contracts made among individuals or organizations. Without the rule of law to enforce these contracts and provide accountability, participants in market economies may be afraid to form agreements that would otherwise be profitable.

Rights transparency ensures that individual contributors know who will and will not have rights to access their contributions. Individuals are less likely to contribute information into the system if they are afraid that those whom they would not want to access a document will be able to do so, or that those who should have access will be unable to obtain it. The need for rights transparency was observed as early as 1974, when Jerome Saltzer called for "better understanding the nature of the typical user's mental description of protection intent" to devise "interfaces which permit more direct specification of that protection intent" [24].

One barrier inhibiting users from sharing editing rights (write permissions) on documents is the risk to the integrity of their documents: undesirable changes may go undetected, it may not be possible to identify the individual who made the change, and the value of the document before the change may not be recoverable. Systems that provide *transactional transparency* – allowing contributors to identify, attribute, and roll back changes – reduce these risks, increase the likelihood of sharing, and thus increase the potential value attainable through the use of a file sharing system.

Email sharing is extremely transparent. The recipients box in the composition window of most email clients provides a clear, comprehensible interface for specifying the set of individuals (delegates) who will receive (be permitted to read) an attached document. The sender of a message is identified as the source of the most recent changes to the document and the list of other recipients appear next to the *to* and *cc* headers. Changes are made explicit through the creation of a new email. Forwarding and use of the *bcc* field enable delegates to further delegate the ability to read a file to others, and do so without attribution. However, such losses of transparency are unavoidable in any sharing system. If those authorized to read a file want to subvert access controls designed to keep others from reading a file or track who has read it, they will always be able to photograph, record, or even manually copy the information to an unprotected medium. Thus, it can be argued that email provides the greatest level of transparency that is possible to achieve.

Dependability

Users must be able to rely on the sharing system to both store and transmit their information both reliably and securely, enforcing their chosen sharing (access control) policies.

Investors are more likely to invest in a stable economic system than an unstable one when all other factors are equal. Witness, for example, the capital available to the U.S. treasury at low cost as a result of its high perceived stability. Policy stability is also important to investors wary of the risks of investing in economies in which firms may be nationalized at the whim of government officials. Users of a file system require similar assurances that their data will be safe and that their policies will be enforced correctly.

While many users find email dependable enough to rely on for many of their communications needs, email systems are not without failures. Email may be incorrectly marked as spam, dropped due to attachment size, intercepted, or forged. However, these failures are relatively rare and since email is already in wide use its users have developed user-layer protocols to detect and recover from many failures when an email is of sufficient importance. For example, it is not unusual for important emails to be accompanied by phone calls or requests for confirmation of receipt. While unencrypted email is subject to interception at the network level (man-in-the-middle attacks), such attacks are exceedingly rare and so the great majority of users still consider email sufficiently secure and thus dependable. One advantage of email-based sharing is that the dependability of the file transfer is linked to the dependability of the email used to notify the recipient of its existence; if the email arrives, so too will the attachment.

Minimal friction

A sharing system should be free of barriers that unnecessarily or excessively inhibit sharing.

In market economies, the term *friction* refers to barriers that inhibit transactions that would otherwise increase the common good. Such barriers include tax policies and information asymmetries, though in some ways friction serves as a catch-all for barriers to the efficient use of the system not explicitly detailed in the previous set of requirements.

The management of access control policies and the imposition posed by incorrectly formed policies introduce significant friction into file sharing systems. For example, the designers of the Multics access control mechanisms recognized that it was too complex; accordingly, it was simplified [10] as the system evolved. In one example, per-ring ACLs were removed, since no one used them. In another, a feature known as "common access control lists" – per-directory permission specifications that applied to all files within it, in addition to specific ACLs for individual files [19] – was deleted by 1972 because it led to "frequent mistakes and confusion, in violation of the design principle that calls for naturalness and ease of use" [24].

Email-based sharing, on the other hand, piggybacks on users' existing process of notifying collaborators that new content is available. Email clients already help users manage individual contacts and groups (mailing lists). The contact management tools that help users specify the recipients of an email (those with access to read it) are leveraged to control access to the attachment as well.

On the other hand, using email attachments for collaboratively editing documents introduces friction, as user-level protocols are required to lock documents for editing, resolve conflicts, and send updates—problems that traditional file sharing systems seek to address.

What laissez-faire sharing is not

We have encountered a number of misconceived assumptions about laissez-faire sharing among those exposed to early versions of this work and our presentation to the New Security Paradigms Workshop. We thus feel compelled to put some of these to rest.

The adoption of laissez-faire sharing systems does not necessarily imply the adoption of looser or more open policies that grant more users access to files. Rather, it only implies that the owner will make the decision of who has access to the file. In fact, file owners may become more comfortable using defaults that grant few others access if the friction to grant access to additional users is sufficiently reduced. This was part of the motivation for the Slackcess Control system discussed in 3.

The adoption of laissez-faire sharing does not require one to assume that their users are more trustworthy than those of systems with centrally-administered access-control policies do. If some users aren't trustworthy, no mechanism will be able to protect the resources that they have been given access to from being compromised.

The adoption of laissez-faire sharing does not prevent central administrators from providing policy guidance. System administrators may still set the default policy for new users to the system, and defaults hold great power. Furthermore, system administrators may still provide low-friction warnings to indicate if a policy is about to be violated and the consequences of doing so. These are of value as users are more likely to violate a security policy if they are not aware of it and convinced of its importance. A laissez-faire sharing system will allow owners to override the central policy guidance if he or she is not convinced it applies to his or her situation, but this may not make the system less secure: motivated users will be able to override any attempts to restrict information from being copied regardless of technical obstacles. While the consequences imposed for departing from a prescribed policy are external to the system, it is important to note that administrators will only be alerted to such departures if users can override the policies within the system, rather than by circumventing it entirely.

Finally, laissez-faire sharing systems are not dismissive of the rights of readers or editors with whom files are shared but who do not, themselves, have ownership rights. While owners can restrict others from delegating read access, they are as powerless as central system administrators in preventing re-sharing. For example, a reader could be asked (but not forced) to request permission before granting others read access. Those who can only read a file, but wish to edit it, will inevitably be able to copy the file's contents into a new version that they own, even if they must do so manually. The owner of the original version will not see the updates, but the owners of new branches can edit and share them with whomever they wish. Again, the consequences of unauthorized re-sharing and branching are outside the bounds of the system and depend on the social contract between the file owners and those they share with. Like system administrators, owners who allow their preferred policies to be overridden are more likely to know when overrides occur. Thus, owners who choose to may apply laissez-faire principles by issuing recommendations, rather than restrictions, on how their delegates may access and re-delegate their permissions.

3. PROBLEMS RETROFITTING WINDOWS TO SUPPORT LAISSEZ-FAIRE SHARING

Traditional file sharing mechanisms do have advantages over email-based sharing. Windows shared folders (the built-in file sharing system in Windows) provide users access to the most recently saved copy of a file without requiring manual updates be sent by the most recent contributor. Windows shared folders also provide synchronization mechanisms to prevent simultaneous editing that could result in conflicting versions. Furthermore, Windows shared folders are space-efficient in that only a single copy of a document need be stored for all those with access to it, whereas each email server must store its own copy of an attached document (and many store one copy per recipient). Alas, permissioning of Windows shared folders introduces significant friction; users are forced to interrupt their application task flow to interact with OS-provided access control interfaces. These interfaces have been shown to be tedious and difficult to understand [22]. We sought to minimize the friction that access-control mechanisms impose on Windows shared folders by making them work more like email-based sharing. This goal of reducing the effort required to successfully permission and share files inspired us to name the project *Slackcess Control*.

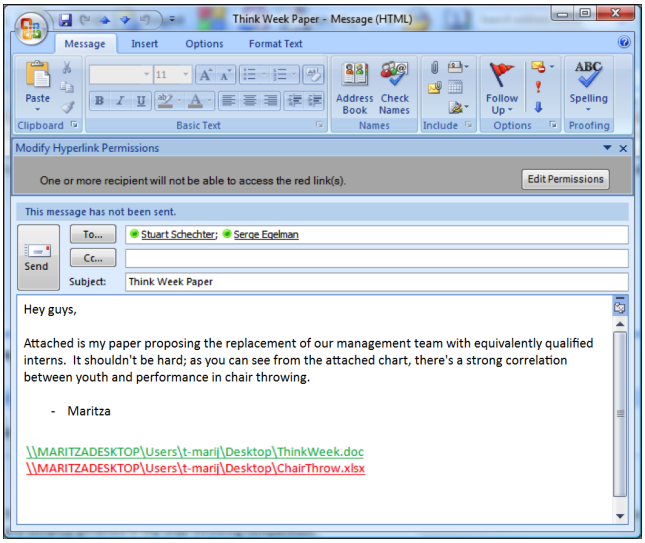

Figure 1: Slackcess Control adds a pane to the message composition window to warn the user a recipient does not have access.

3.1 Design and goals

We developed Slackcess Control as an extension to Microsoft's Outlook email client. When a user composes a message containing a link to a file stored in a Windows shared folder, this extension queries the access control interfaces in Windows to determine whether any of the message's recipients lack the ability to read (or edit) the document. When one or more recipients lack the permissions required to access the linked file, Slackcess Control alerts the user – via a ribbon at the top of the message composition window – and offers to update the access control settings to grant the missing permissions. Figure 1 illustrates an example of a message composition window containing such a warning.

We hoped that Slackcess Control would reduce the occurrence of a common annoyance in our work lives: receiving email with links to files that we could not access. We also hoped that making it easier to grant permissions at the file level would result in a net increase in security, as users could now set safe (e.g. owner-only) default permissions and trust that additional permissions would be effortlessly granted as needed. Finally, we hoped that the highly developed group management (mailing list) capabilities in email clients would make it easy for users to reason about the groups they were sharing with.

3.2 Windows sharing–ce n'est pas laissez-faire

Our attempt to layer Slackcess Control on top of Windows shared folders led to numerous problems that, in retrospect, could have been anticipated by examining support for laissez-faire sharing in Windows. Windows shared folders use access control lists to specify who may read, write, delete, and modify the permissions to folders (directories) in a hierarchy.

Users who are given directories in which to store files (e.g. a home directory) may not be given to change these files' permissions or read them from a remote location. Thus, both ownership and freedom of delegation in Windows shared folders are provided only at the discretion of the system administrators who set default permissions. Our experience tells us the system administrators who have this power have difficulty resisting the temptation to use it; they may do so out of fear that they will be held responsible if security failures result from access control policies deemed, after the fact, to be too lax. When run by a user without sufficient permissions to a linked file, Slackcess Control may be unable to evaluate whether a recipient of this link will be able to read it.

Even if the user has access to change the permissions for a document at the file system level (the *NTFS-level permissions*) and Slackcess Control grants the required permissions, a second set of permissions specific to the shared folder implementation (*share-level permissions*) may override these grants. Remote access to files on Windows shared folders is allowed only when access has been granted via both the file system (NTFS) permissioning infrastructure and on a per-share basis via the shared folder infrastructure. Again, individual users may not have access to read, let alone change, permissions on shares. Thus, freedom of delegation may be limited at both the NTFS and share levels.

Windows shared folders also lack rights transparency as share permissions are not visible to all users. Thus, Slackcess Control may not be able to determine who does, and does not, have access to a user's file. Slackcess Control may grant NTFS permissions to a recipient but – unable to read let alone change the share permissions – will be unable to guarantee that the recipient will actually be able to access the file as a result. Thus, in many cases Slackcess Control cannot achieve anywhere near sufficient rights transparency or perceived dependability. This is not a shortcoming of the Slackcess Control implementation but of the underlying file system. Users who employ the interfaces built into Windows to add NTFS permissions for a user and to verify – using the effective permissions interface – that a recipient can read the file may still find that the recipient is later denied access at the share-level when he or she tries to access it. This failing is a consequence of a failure to grant users who own files on a share the ability to view the share permissions, and to incorporate share level permissions as part of the calculation of effective permissions.

Even when system administrators grant ownership and provide for free delegation, Windows shared folders have not traditionally supported delegation to users who are outside the organization: domain or local accounts must be created to support external users. Even as such support is added, support for external users is often hindered by firewalls that would prevent access from outside an organization. Thus, if Slackcess Control wants to help users share documents on Windows file shares with recipients outside of their organization, the best it can do is attach the document to the email on the user's behalf.

Finally, transactional transparency is notably lacking in Windows shared folders and there is little Slackcess Control can do to address this. While changes to Windows file shares may be logged, the owners of individual documents and contributors rarely have access to these logs. Once one writer overwrites a file, previous versions are no longer available.

4. EVOLUTIONARY PRESSURE DRIVING LAISSEZ-FAIRE SHARING

Economies compete for talent, investment, business, and trade. Their ability to compete drives a process of natural selection through which laissez-faire economies have increasingly driven out centrally planned ones.

Just as free market economies place evolutionary pressure on centrally-managed ones, the ongoing selection of file sharing mechanisms by individuals places similar pressure on these mechanisms. Whenever access control policies fail to provide the flexibility users need to do their work, users will be tempted to switch to systems with a more laissez-faire approach to access control.

As with centrally-planned economies, some may argue that their limitations reflect the fact that they have yet to be properly implemented and so their potential has not yet been realized. There is no shortage of research on more expressive access control models and languages that one might deploy in hopes of reducing the frequency with which centralized access control impedes productivity. We believe that the best one can do by increasing the expressiveness of centralized policies is to reduce the rate at which users abandon centralized access control regimes.

As new sharing mechanisms better meet workers' demand for laissez-faire policies, system administrators must choose between adapting their policies to meet user needs or risk having their users circumvent the systems they support and prescribe. The less attractive an organization's sharing mechanism is in comparison to the alternatives, the more likely it is that users will choose the alternatives to store their files and that the organization will lose the ability to ensure that files are stored securely, backed up, and that accesses may be audited. As an increasing number of systems support laissez-faire sharing and information workers become increasingly familiar with their benefits, the evolutionary pressure increases against overly restrictive sharing systems.

We see this ongoing evolution in play today not just in the popularity of email and USB sticks, but in the increased adoption of wikis in corporate environments [12]. Indeed, even the U.S. national intelligence community has created their own wiki, known as "Intellipedia" [3]. One interesting development in this evolutionary process is the success of Microsoft's SharePoint, for which a single "site collection" administrator can support a single server with independently administered "sites" [14]. Thus, SharePoint pushes administration of access control policies closer to the endpoints by distributing management of sites to the center of the teams for which they are purposed. While each team may still have a central administrator, it is at least more likely that it is someone an individual user will know.

Systems like SharePoint, in turn, must now compete with cloud storage products like Google Docs and Microsoft OfficeLive. Docs and OfficeLive provide sufficient ownership and allow users to access their files from anywhere they can reach the web. Earlier research has already cited cases in which individuals use cloud storage to transfer files in order to access them outside of work [5]. Cloud storage products also allow users to delegate to anyone with an email address and maintain the ability to revoke access. Cloud storage products take transparency to new levels by allowing users to see others' changes in real time. Dependability is on par with that of web-based email, for which the rarity of security failures and outages is evidenced by the attention that these events receive when they do occur. To the chagrin of many a corporate IT department, employees who use these cloud storage systems are also delegating the management and security of their data to the operators of these services.

As cloud storage increases in popularity, an increasingly pressing decision will face system administrators and IT departments: whether to deploy an internal system that meets all the laissez-faire requirements supported by cloud storage, to entrust data to an externally managed system that meets these requirements, or to implement strict (but inevitably ineffective) policies requiring the use of prescribed sharing mechanisms so as to protect themselves from blame. The choice to adopt laissez-faire systems is the one that maximizes the amount of data that stays within the control of the organization, where it can be stored securely, backed up, and audited.

5. RELATED WORK

Friedrich Hayek observed in *The Use of Knowledge in Society* that problems in centrally managed polices arise as the consequence of change, that such changes are first observed by the individuals "on the spot", and that these individuals at the endpoints are best equipped to manage changes [8]. We are not the first to draw parallels between these economic philosophies and access control. As we discuss in the introduction, Jimmy Wales cites Hayek's influence leading him to eschew centralized control in Wikipedia [23]. Miller *et al.* also cite Hayek's economic theories in the context of security in software engineering to advocate that security policies should be specified close to the functions they are intended to protect [15]. Cheng *et al.* cite Hayek in their proposal for Fuzzy Multi-Level Security [4]

Those frustrated that a flood of new languages, logics, and algebras for expressing and reasoning about access control policies has not resulted in systems that are comprehensible to users may take solace in Hayek's similar frustrations with economic theorists: "The character of the fundamental problem has, I am afraid, been obscured rather than illuminated by many of the recent refinements in . . . theory, particularly by many of the uses made of mathematics" [8].

Parallels with Hayek's economic theories provide the background for why *centrally-controlled policies fail* and why *more expressive policies don't help*, the first two subsections of related work that we explore. We then examine *approaches from usability researchers* to the problem of file sharing, many of which focus on addressing rights transparency and friction. Finally, we explore the emergence of systems that rely on *optimistic access control*, which meets all laissez-faire requirements with the exception of the right not to share.

5.1 Centrally-controlled policies fail

In a survey of 56 employees of a "medium-sized industrial research laboratory" by Whalen *et al.*, 55 (98%) reported that their most frequent means of file sharing was email.

In a survey of ten employees of a medium-sized research organization[3] presented in 2006, Voida *et al.* found that

[3]This study was performed at PARC, the same medium-sized research organization as Whalen *et al.*, and so these studies results may not be as independent as they would otherwise appear.

email-based sharing was used in 43% of the sharing instances reported, vs. 16% for shared folders [29], and that respondents who did use traditional file sharing systems reported falling back to email when they were unable to grant permission using those systems. They found that knowledge workers chose file-sharing mechanisms to meet the needs of a situation and identified ten features that affected decision making. Amongst the ten features were universal scope (i.e., the ability to share with anyone), which is similar to our property of freedom of delegation; visibility, logging, and versioning, which are all part of our property of transactional transparency; and specification of access control and access rights, which we include under the properties of ownership and freedom of delegation. Miltchev *et al.* demonstrated a method of allowing sharing across organizational boundaries thus partially fulfilling the freedom of delegation property [16].

Dalal *et al.*, also at PARC, conducted a field study of ten individuals from various domains to identify ad-hoc sharing practices among knowledge workers [5]. They found corporate security policies were unable to support the sharing needs of users. The inflexibility forced users to employ a number of insecure and undesirable methods in order to get their job done. They found "that people regularly bypass secure access procedures by using public web repositories, personal email, and USB drives to transfer information (insecurely)." Their results show all participants used email for sharing in some tasks, even emailing snippets of code to a personal account to allow them to work at home. They found these issues arose most often when sharing between groups within a company, granting short term access, sharing between one user's own devices, and outside consultants. The users in this study expressed requirements for what we have called ownership, freedom of delegation across domains, rights transparency, and dependability.

5.2 More expressive policies don't help

Attempts to address the limitations of centrally-managed access control go back as far as Shen and Dewan's attempt to provide a more fine-grained access-control model for collaboration in multi-user environments [25]. Role-based access control (RBAC) [26] is perhaps the most well known approach to solving problems of access control by changing how policies are expressed. By introducing roles as a level of indirection between people and the rights they have to resources, RBAC was intended to help administrators align access-control policies more closely with organizational structures and objectives.

Alas, in both economies and file systems, central planners fail to account for losses to individual productivity that result when policies are overly restrictive and the security risks that result when individuals try to work around these policies. A NIST-funded 100-plus paged report on the economic benefits of RBAC (see [7]) illustrates such disregard. The researchers quantified the time required to provision (add) employees, de-provision (remove) them, and make changes to policy for existing employees—costs borne by administrators. With the exception of time lost during provisioning, no consideration was made for user-borne costs such as the number of legitimate actions prevented by overly restrictive policies, productivity loss while employees await access, or the number of instances in which users worked around policies by circumventing prescribed systems or practices.

5.3 Approaches from usability researchers

Most sharing systems developed by usability researchers focus on increasing transparency and reducing friction.

Kapadia *et al.*'s KNOW system adds transparency; it sits within an access control system and provides feedback when access is denied to help explain why access is denied and how it might be obtained [9]. The Expandable Grid, developed by Reeder *et al.* to manage NTFS access control policies, adds transparency by enabling users to manage effective permissions rather than abstract policies [21]. Like Slackcess Control, Balfanz's ESCAPE file-sharing tool attempts to reduce friction by integrating message composition and sharing. Whereas Slackcess Control employs users' existing message composition experience for file sharing, ESCAPE moves the message composition experience into the file sharing system [1].

Zurko *et al.* were amongst the first to build an access-control management system with usability in mind—but focused only on the usability needs of a central policy administrator. Their Visual Policy Builder interface to their Adage system made policies more transparent and reduced the friction to create them [34].

Zurko [35] and Yee [32, 33] provide design guidance with which Slackcess Control and laissez-faire file sharing are aligned. Zurko proposed achieving usable security by adding security into a process that is already usable; with Slackcess Control, we sought to make file sharing with email more secure. Yee argues for "security by designation", in which users grant access to resources implicitly in the course of their work when they request that a system carry out an action [33]. Slackcess Control implements security by designation for files shared via email. Our laissez-faire requirements (and the Slackcess Control system) encompass many of the general properties suggested by Yee in *User Interaction Design for Secure Systems* [32]: least resistance (our minimization of friction); explicit authorization and revocability (freedom of delegation); expected ability, expressiveness, and clarity (transparency).

5.4 Optimistic access control policies

At the 1999 New Security Paradigms Workshop, Dean Povey proposed an "optimistic" approach to access control in which users may override access control restrictions and violations are handled post-facto through rollback and attribution [20]. Thus, Povey favors transparency for achieving reduced friction at the cost of freedom of delegation–removing the right *not* to share.

Wikipedia provides an excellent example of optimistic access control, using change histories and self policing in place of access control restrictions. Heavier-weight access control mechanisms are reserved for those entries that prove controversial enough to require them.

Laissez-faire systems employ optimistic policies for actions that cannot be prevented: such as sharing a file the user already has access to with someone else. However, in laissez-faire systems access cannot be acquired optimistically without the help of someone who already has access.

Optimistic security may at first appear to pose an evolutionary threat to laissez-faire sharing—it does not. When information owners must choose where to store their information, the freedom of delegation required by laissez-faire systems guarantees that they will be able to delegate optimistically if they so choose.

6. CONCLUSION

Individual information workers circumvent prescribed file sharing systems when these systems' access controls impede their productivity or otherwise fail to meet their needs. We have introduced five requirements of laissez-faire sharing necessary (though not in all cases sufficient) to meet the needs of information workers. These requirements are ownership, freedom of delegation, transparency, dependability, and minimization of friction. Each requirement's analog from economics helps elucidate the consequent inefficiencies that result when a system fails to satisfy it.

Given individual tendencies to choose laissez-faire sharing mechanisms, system administrators must choose to either deploy and support systems that meet laissez-faire requirements or – voluntarily or not – relinquish control over the storage of workers' data. Only by adopting laissez-faire sharing can administrators hope to limit the number of systems trusted to store their organizations' data and to enforce their users' chosen access control policies. Thus, we contend, the evolutionary path to widespread adoption of laissez-faire access control is both inevitable and well underway.

Acknowledgements

Allan Friedman provided feedback and pointers to related research that were essential building blocks of this work. Paul Karger helped to provide a historical perspective on access control design. Ben Laurie and Mary Ellen Zurko helped to assemble the valuable comments of reviewers and NSPW attendees and provided additional feedback of their own. We also benefited from a careful reading and feedback from Rich Draves.

We would like to thank Jamie Eisenhart and Quinn Hawkins for their valiant efforts in continuing the development of Slackcess Control following Maritza's internship.

7. REFERENCES

[1] D. Balfanz. Usable access control for the world wide web. In *ACSAC: 19th Annual Computer Security Applications Conference*, pages 406–415, 2003.

[2] A. Beautement, R. Coles, J. Griffin, C. Ioannidis, B. Monahan, D. Pym, A. Sasse, and M. Wonham. Modelling the human and technological costs and benefits of USB memory stick security. In *The 2008 Workshop on the Economics of Information Security*, June 25–28, 2008. `http://weis2008.econinfosec.org/papers/Pym.pdf`.

[3] M. Calabresi. Wikipedia for spies: The CIA discovers Web 2.0. *Time*, 8 April 2009. `http://www.time.com/time/nation/article/0,8599,1890084,00.html?imw=Y`.

[4] P.-C. Cheng, P. Rohatgi, C. Keser, P. A. Karger, G. M. Wagner, and A. S. Reninger. Fuzzy multi-level security: An experiment on quantified risk-adaptive access control. In *SP '07: Proceedings of the 2007 IEEE Symposium on Security and Privacy*, pages 222–230, Washington, DC, USA, 2007. IEEE Computer Society.

[5] B. Dalal, L. Nelson, D. Smetters, and N. Good. Ad-hoc guesting: When exceptions are the rule. In *UPSEC '08: Usability Psychology and Security*, 2008.

[6] D. F. Ferraiolo, D. M. Gilbert, and N. Lynch. An examination of federal and commercial access control policy needs. In *Proceedings of the 16th National Computer Security Conference*, pages 107–116, Darby, PA, USA, 1993. DIANE Publishing Company.

[7] M. P. Gallaher, A. C. O'Connor, and B. Kropp. The economic impact of role-based access control, Mar. 2002. RTI Planning Report 02-1 presented to the NIST.

[8] F. A. Hayek. The use of knowledge in society. *American Economic Review*, 35(4):519–530, Sept. 1945. Republished in Individualism and Economic Order.

[9] A. Kapadia, G. Sampemane, and R. H. Campbell. KNOW why your access was denied: Regulating feedback for usable security. In *CCS '04: Proceedings of the 11th ACM Conference on Computer and Communications Security*, pages 52–61, New York, NY, USA, 2004. ACM.

[10] P. Karger. Personal communication, Apr. 2009.

[11] C. E. Landwehr. Formal models for computer security. *ACM Computing Surveys*, 13(3):247–278, 1981.

[12] A. Majchrzak, C. Wagner, and D. Yates. Corporate wiki users: results of a survey. In *WikiSym '06: Proceedings of the 2006 international symposium on Wikis*, pages 99–104, New York, NY, USA, 2006. ACM.

[13] K. Mangu-Ward. Wikipedia and beyond, June 2007. `http://reason.com/news/show/119689.html`.

[14] Microsoft Corporation. About security features of Windows SharePoint Services 3.0. `http://office.microsoft.com/en-us/sharepointtechnology/HA100215781033.aspx`.

[15] M. S. Miller, B. Tulloh, and J. S. Shapiro. The structure of authority: Why security is not a separable concern. In *LNCS 3389: Multiparadigm Programming in Mozart/OZ*, pages 2–20. Springer Berlin / Heidelberg, Feb. 22, 2005.

[16] S. Miltchev, J. M. Smith, V. Prevelakis, A. Keromytis, and S. Ioannidis. Decentralized access control in distributed file systems. *ACM Comput. Surv.*, 40(3):1–30, 2008.

[17] National Commission on Terrorist Attacks Upon the United States. *the 9/11 Commission Report*. United States Government Printing Office, July 22, 2004.

[18] Open Security Foundation. DATALOSSdb. `http://datalossdb.org/`.

[19] E. I. Organick. *The Multics System: An Examinatio of Its Struture*. The MIT Press, Cambridge, MA, and London, 1972.

[20] D. Povey. Optimistic security: A new access control paradigm. In *NSPW '99: Proceedings of the 1999 Workshop on New Security Paradigms*, pages 40–45, New York, NY, 1999. ACM.

[21] 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, NY, NY, USA, 2008. ACM.

[22] R. W. Reeder and R. A. Maxion. User interface dependability through goal-error prevention.

Dependable Systems and Networks, International Conference on, pages 60–69, 2005.

[23] R. Roberts and J. Wales. Wales on wikipedia, Mar. 9, 2009. Library of Economics and Liberty. `http://www.econtalk.org/archives/2009/03/wales_on_wikipe.html`.

[24] J. H. Saltzer. Protection and the control of information sharing in Multics. *Commun. ACM*, 17(7):388–402, 1974.

[25] H. Shen and P. Dewan. Access control for collaborative environments. In *CSCW '92: Proceedings of the 1992 ACM Conference on Computer-supported Cooperative Work*, pages 51–58, NY, NY, USA, 1992. ACM.

[26] R. S.Sandhu and E. J. Coyne. Role-based access control models. *IEEE Computer*, 29(2):38–47, 1996.

[27] Symantec Security Intel Analysis Team. Increase in usb-based malware attacks. `https://forums2.symantec.com/t5/blogs/blogarticlepage/blog-id/malicious_code/article-id/220`, Nov. 19, 2008.

[28] D. Tober and I. Hoffman. *A Convenient Spy: Wen Ho Lee and the Politics of Nuclear Espionage*. Simon & Schuster, New York, 2001.

[29] S. Voida, K. W. Edwards, M. W. Newman, R. E. Grinter, and N. Ducheneaut. Share and share alike: exploring the user interface affordances of file sharing. In *CHI '06: Proceedings of the SIGCHI conference on Human Factors in computing systems*, pages 221–230, New York, NY, USA, 2006. ACM.

[30] D. Weirich and M. A. Sasse. Pretty good persuasion: a first step towards effective password security in the real world. In *NSPW '01: Proceedings of the 2001 workshop on New security paradigms*, pages 137–143, New York, NY, USA, 2001. ACM.

[31] T. Whalen, D. Smetters, and E. F. Churchill. User experiences with sharing and access control. In *CHI '06: CHI '06 extended abstracts on Human factors in computing systems*, pages 1517–1522, New York, NY, USA, 2006. ACM.

[32] K.-P. Yee. User interaction design for secure systems. In *ICICS '02: Proceedings of the 4th International Conference on Information and Communications Security*, pages 278–290, London, UK, 2002. Springer-Verlag.

[33] K.-P. Yee. Aligning security and usability. *IEEE Security and Privacy*, 2(5):48–55, September 2004.

[34] M. E. Zurko and T. Sanfilippo. A user-centered, modular authorization service built on an RBAC foundation. In *Proceedings of the 1999 IEEE Symposium on Security and Privacy*, pages 57–71, Los Alamitos, CA, USA, 1999. IEEE Computer Society Press.

[35] M. E. Zurko and R. T. Simon. User-centered security. In *NSPW '96: Proceedings of the 1996 workshop on New security paradigms*, pages 27–33, NY, NY, USA, 1996. ACM.