UCL DEPARTMENT OF
COMPUTER SCIENCE

Research Note
RN/12/06

How Users Bypass Access Control and Why: The Impact of Authorization Problems on Individuals and the Organization

24/05/2012

Steffen Bartsch

M. Angela Sasse

Abstract

Many organizations struggle with ineffective and/or inefficient access control, but these problems and their consequences often remain invisible to security decision-makers. Prior research has focused on improving the policy-authoring part of authorization and does not show the full range of problems, their impact on organizations, and underlying causes. We present a study of 118 individual's experiences of authorization measures in a multi-national company and their self-reported subsequent behavior. We follow the recent advances in applying economic models to security usability and analyze the interrelations of authorization issues with individuals' behaviors and organizational goals. Our results indicate that authorization problems significantly impact the productivity and effective security of organizations. From the data, we derive authorization Personas and their daily problems, which are to a large extent caused by the procedures for policy changes and the decision-making, and lead to the circumvention of the measure. As one research contribution, we develop a holistic model of authorization problems. More practically, we recommend to monitor non-compliance, such as password-sharing, for indications of authorization problems, and to establish light-weight procedures for policy changes with adequate degrees of centralization and formalization, and support for decision-making.

1 Introduction

Authorization is a core aspect in organizations to enforce security policies in information systems. While problems with authorization are frequently reported in form of anecdotes, organizations so far seem reluctant to conduct a comprehensive review of the problems, or consider their impact on individual employees' and organizational productivity. One reason is that the problems are only visible to security decision-makers, such as CISOs, as individual cases. Moreover, the problems are often reduced to security problems, which are abstract and difficult to turn into a case for addressing the problems [20]. A number of studies have analyzed the usability of authorization and found that crafting authorization policies[1] is difficult, both in laboratory experiments [23, 6] and in organizational practice [3, 18, 21].

However, the problems with authorization cannot be reduced to only the usability of management tools and the authoring of policies. Models of security economics that include the impact on productivity from security usability, such as the Compliance Budget [4], predict, for example, that when requesting a change in the policy is perceived as too much effort, employees may rather share their password as a cheaper way of solving the problem. To understand the problems with authorization thoroughly, we have to consider how authorization affects both the behavior of employees, and the organizational security and productivity.

The aim of this paper is to foster a broad understanding of usability challenges surrounding existing authorization mechanisms, their interdependence, and their impact on organizational goals. We apply economic models to security usability and the organization of information security to motivate our study. We conducted 118 in-depth interviews on security compliance at a large infrastructure company with a variety of authorization contexts.

Based on the interviews, we developed Personas [8] to draw a vivid picture of the daily issues surrounding the user of existing authorization mechanisms. Systematically analyzing causes and effects of the issues, we identify how they impact organizational goals and what the root causes for the problems are. We also compare two different authorization contexts within the organization, and show that the procedures for changing authorization policies and the policy decision-making are particularly important. This includes the degree of formality and centralization of the procedures, the interactions of stakeholders from different perspectives, and their levels of expertise and awareness. Based on our findings, we discuss approaches to mitigate the problems.

2 Related work

2.1 Policy authoring

To a large extent, studies in the area of authorization usability focus on the usability of policy authoring interfaces. Zurko and Simon formulated requirements for a usable policy authoring interface from their study on usable security [23]. Zurko et al. then developed a policy editor for policies similar to RBAC based on usability testing and user-centered design that allowed novice users to produce meaningful results [22].

Rode et al. also studied the challenges in authoring policies [15]. They find that policy authors need to comprehend consequences of the changes and suggest the integration of tasks, monitoring, and configuration. Reeder et al. add to these findings by showing that mistakes in policy authoring can originate from isolated authorization rules in lists that do not convey their interrelation [14]. Vaniea et al. similarly identified the cognitive load of conflict detection as a major challenge [19].

Focusing instead on the mental model of policy authors, Brostoff et al. found that the primary challenges lie in understanding the policy structure and the overall authorization paradigm [6]. To

[1] The term *authorization policy* is used for the restrictions or permissions enforced by information systems. In contrast, *security policies* denote the general rules of conduct with respect to security in an organization.

Study	Study design	Environment	Focus/scope	Findings	Recommendations
Sikkel [16]	Subjective: interviews	Private and public organizations	How users specify policies	Policies are stated as grants/denials, refined by exceptions, e.g. scopes	Provide expressive model: object grouping, scope, delegation
Whalen [21]	Subjective: survey, interviews	Medium-sized research laboratory	Individuals' problems from mechanisms	Users manage policies, but struggle with it; authorization interferes with primary tasks	Integrate with workflows, support social controls, visualize policies, and simplify management
Bauer [3]	Subjective: interviews	Diverse organizations	Challenges for policy professionals	Problems from stakeholder interactions and inadequate models	Support communication of policy authors, improve authorization models
Smetters [18]	Objective: historical policy data	Medium-sized corporation	Usage of authorization features and models	Complex, rarely changed policies, management errors	Simpler models, patterns, better management tools

Table 1: Prior studies on authorization in organizations

overcome the conceptual mismatches between the authorization model and the mental model of the security engineer, Inglesant et al. employed iterative development of policies using a controlled natural language [11].

These laboratory studies focus exclusively on the individual task of authoring policies and further the usability of this aspect of authorization. However, crafting adequate policies depends to a large extent on the policy author being in a position to judge which permissions to grant. We thus need to consider a broader perspective to fundamentally solve authorization challenges in organizations and incorporate the problems in day-to-day operation of authorization and how stakeholders interact to mitigate them.

2.2 Challenges in organizations

A small number of broader studies have analyzed how challenges in authorization actually materialize in organizations, summarized in Table 1. Three of the four identified studies exclusively focus on the challenges in policy authoring. Sikkel and Stiemerling [16], Bauer et al. [3], and Smetters and Good [18] examine how the expressiveness of authorization models affect policy management and suggest model improvements. In addition, Bauer also analyzes the interactions of policy authors with different roles. In contrast, Whalen not only explores the problems of managing authorization, but also how authorization interferes with the primary tasks of functional users.

These studies still mostly focus on authorization usability issues on an individual level, primarily with respect to policy authoring. The consequences of the identified challenges remain implicit. However, since most problems rarely become visible for management and then only as anecdotal individual cases, the authorization issues are still largely ignored in organizations. One reason is that the scale and the actual impacts on organizational goals are unknown. To make a case for fundamentally addressing the problems that functional users are faced with every day, the full breadth of authorization challenges needs to be explored with their complex interrelations and, particularly, their impact on organizational goals.

2.3 Economic perspective

It is common to consider the impact that usability problems with security mechanisms have – usually focusing on how users' mistakes reduce security. In authorization, it has been observed, for example, that entitlements are not adjusted to reflect organizational changes, resulting in over-entitlement and secondary risks, such as more severe consequences in case of a security breach [17]. However, the

potential additional security risk created by users making mistakes is only one of several consequences and is often too intangible and abstract to measure and difficult to use as a clear case to argue for changes [20].

In a novel and promising approach, security researchers have in the last years argued increasingly on the basis of economic impact on organizations and individuals [2]. Beautement et al. described the Compliance Budget [4] and Herley analyzed the externalities of security measures [10]. They argue that we need to take a comprehensive perspective of the costs and benefits of security measures, particularly from the individuals' point of view, demonstrating that users often do behave rationally when not complying with security advice. Their examples include the insecure use of USB sticks and the effects of password policies. This line of research can be applied to authorization as well. As already noted above, authorization has been found to impact the primary tasks of employees [21]. An example of the cost of compliance is the effort expended on following the prescribed procedures to change the policy. More convenient alternatives to compliance could be found, such as sharing passwords. If the costs of compliance are perceived to be too high and alternatives are perceived as cheaper, even considering potential consequences, users are likely not comply. We use this model to examine usability issues with authorization measures.

In a parallel research strand with a focus on the *organizational* economics, Pallas [12] analyzes motivation and coordination costs for security measures, comparing hierarchical organizations with centrally made decisions with market forms with delegation to local decision-makers. Pallas shows that the extend of coordination and motivation costs depend on the form of organization. Principal–agent theories predict that centrally made decisions often suffer from information asymmetries and interfere with primary tasks. Extending this line of research, we analyze authorization usability challenges for their impact on the organization.

3 Study design

To derive insights about the interrelations of the multitude of authorization challenges and their impacts in practice, we studied the security compliance of employees at a large organization, a European, multinational company. The organization operates systems and maintains information at several levels of criticality and sensitivity, involving, amongst others, market regulation as well as the sensitive personal data of employees and customers.

3.1 Research methodology and sampling

We conducted semi-structured in-depth interviews with 118 employees from management and staff in two countries between January and September 2010. The interviewees were recruited via the company newsletter, inviting volunteers to take part in an "IT Security Research Study" on their experience with the security policy for a gift voucher. From the about 400 responses within two days, we selected the participants primarily on a "first come, first served" basis, with additional later responses added for gender balance and an increased breadth of work environments. The interviews lasted approximately 45 minutes, with 40 conducted via telephone and 78 face-to-face. The interview questions covered the interviewee background, experiences with the security policy, and how it affects the primary tasks.

3.2 Analysis

We focused on the authorization-related segments in the interview transcripts, coding for authorization usability issues and their causes and effects. Almost two-thirds of the interviewees (75 of 118) mentioned authorization issues in one of the organizational information systems, including, amongst others, file sharing, administrative systems, and restrictions to Web access. Since authorization segments are

sparsely distributed over the interviews, we coded in a two-stage process. In the first pass, we assigned broad categories of challenges, for example "policy change issue" to this quote:

> *"they may need temporary access... and a lot of the IS setup takes so long that a lot of these are work arounds to solve a temporary problem... problems tend to bounce around... for quite a long while"*

In the second pass, we then applied open and axial coding to the identified quotes for finer granularity and to establish relationships between the codes through causal coding. We assigned three types of codes to quotes: the issue (the specific challenge, "Change lead time" in the above example) as well as causes ("Multi-level procedure") and effects of the issue ("Social circumvention: Password sharing"). Employing our analysis tool, described below, the coding allowed us to generate causal diagrams of the authorization challenges.

We were particularly interested in relating the diverse challenges to organizational goals and identified the following underlying organizational goals that are affected:

- The *effectiveness of the security measure*: the degree to which the authorization measure increases the overall security as intended,
- The *efficiency of the security measure*: the effort expended by employees in operation to achieve effective security,
- The *regulatory compliance* of the organization with laws and market regulation,
- The *functional effectiveness*: the ability of employees to complete their primary tasks despite authorization restrictions,
- The *functional efficiency*: the effort expended by employees to complete functional tasks, particularly additional efforts caused by security measures,
- The employee *satisfaction*: effects on the motivation of employees, such as frustration.

3.3 Challenges analysis tool

We coded 540 quotes in the interview transcripts, associating issues with the system context as well as causes and effects as tuples or triples in a spreadsheet. We explored the data with a challenge analysis tool that derives relationships from the coded quotes and generates diagrams using the Graphviz tool suite[2]. An example of the diagrams is shown as part of the findings in Figure 1: causal edges connect causes with challenges, until reaching impacts on organizational goals at the bottom. The example above results in the edge from "Policy change issue" to "Circumvention". Since our coding is significantly more detailed, we implemented three levels of details. At the most detailed level, all identified issues are shown with their causal and is-a relationships ("Password sharing" is-a "Social circumvention"). In a more abstract representation, all is-a relationships are flattened and the edges of the detailed level lifted to their parent nodes. The most abstract form is shown in Figure 1 and only displays challenge categories. The different levels of abstraction allow us to both draw high-level conclusions and analyze the interrelations in detail. The diagrams also convey meaning through their structure, the node connectedness, and their relative position.

The tool further supported us by filtering the diagrams in two ways: First, by system context, allowing us to analyze individual authorization contexts. Second, limiting the diagrams to root-cause/ultimate-impact graphs, only showing those causes and effects that directly or indirectly relate to given challenges.

[2] `http://www.graphviz.org/`

Persona/Role	Motivation	Activities	Challenges
Amber Functional staff	Personal, organizational, society risks; productivity	Share/access data, request changes, circumvent measure	Restrictive policies, degraded productivity, change lead time and effort, unclear/ineffective/inefficient procedures, non-transparent decisions and policies
Emily Technically-informed staff	Recognition, (see Amber)	Develop, mitigate issues, make decisions	Non-transparent policies, coarse-grained permissions, lack of usability and functionality, unclear permissions, lack of high-level policy, missing expertise, emotional costs of decisions, informal procedures
Brandon PA	(see Amber)	Make decisions	Non-transparent policies
Lauren Functional manager	Personal risks and gains, organizational/society risks, productivity	Motivate compliance, make/delegate decisions, review policy	Retained permissions, non-transparent policy, inadequate model, lack of usability, decision complexity, required expertise, inefficient procedure, inefficient/ineffective reviews
Nicole Administrator, developer	Personal and organizational and society risks, risk awareness	Administer/develop applications, make decisions, support requests	Lack of high-level policy, cumbersome permissions, conflict of authority

Table 2: Personas related to authorization measures

4 Authorization Personas

Interviewees were affected differently by authorization measures depending on their roles within the organization. A common approach would thus be to identify the roles and relate the personal challenges to the roles. However, roles have the drawback of abstracting detail that is necessary to understand the behavior of a person. As an alternative to roles, usability engineers employ the Persona methodology to preserve concrete characteristics, such as motivations and activities, of typical users [8]. Faily and Flechais successfully used security Personas in security engineering [9].

We followed the approach of Cooper et al. [8] and identified behavioral variables, such as attitudes, motivations, and activities, related to authorization in the interview transcripts. We found 11 categories of behavioral variables with a total of 53 variables. From common combinations of behavior variable assignments, we derived behavioral patterns and formed five Personas, listed in Table 2. We then assigned personal authorization challenges to the individual Personas. Since Personas are originally a design methodology, it is difficult to validate them outside of design endeavors. However, the breadth of the study should provide a good initial hypothesis of the Personas and allow for a vivid picture of how employees are personally affected by authorization.

4.1 Functional staff

Amber is a business analyst in a technical department of the organization. She uses a number of company IT systems, for example, to share documents with co-workers and access data for analyses. Her main motivation concerning the use of the systems are her personal productivity, but also the general organizational efficiency and effectiveness, in that the necessary tasks are completed. Authorization measures affect her most directly through the operational aspects of *restrictive policies* that hinder her work or reduce her productivity, for instance, when she cannot access a document that was sent as a link to her. In some cases she is forced to circumvent the authorization measures and, for example, use the password of a co-worker to access data in the system. However, she feels uneasy about not complying with the organization's security policy that forbids the sharing of passwords.

Amber cares about the security of the sensitive data that she is handling, both for the risks that the organization faces, for example, from a disclosure, but also because of the consequences to her personally

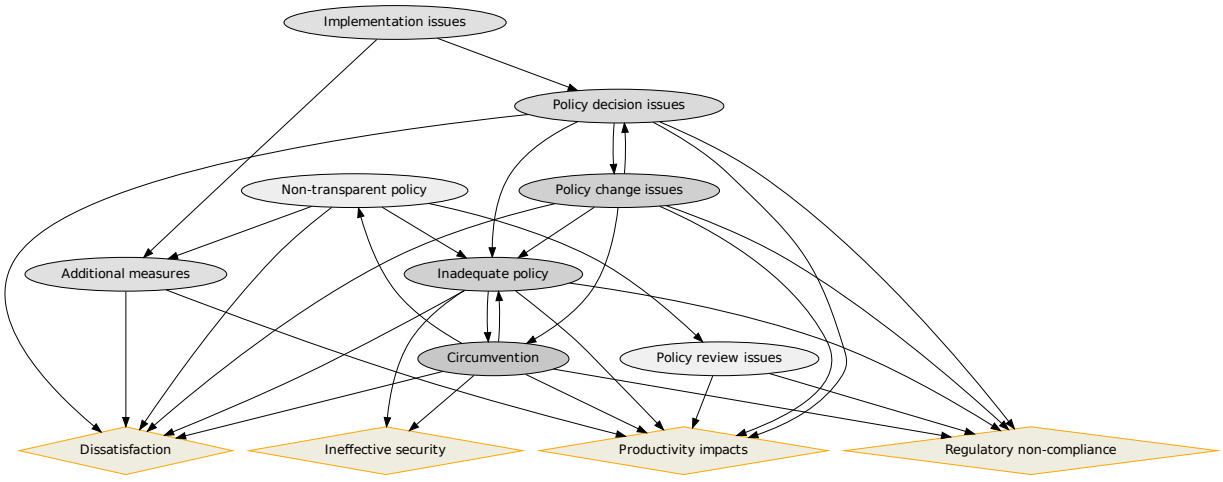

Figure 1: Categorized authorization challenges

(concerning her employment) or the consequences for the society in general from the disclosure of critical data. Due to these considerations, she tries to comply with the security policies and requests changes to the existing permissions, but the requests can require a *high effort* and *take a long time* to become active, both operational authorization issues. For some systems, it is not clear to her how to request changes or it is known that not all requests succeed. Motivated to keep their documents secure, her team decided to also protect documents in the system with passwords, in addition to the system's authorization, since it is not always transparent who has access.

Emily also works as a business analyst, but has more technical experience. She tries to mitigate the problems with authorization that originate, for example, from too granular permissions or missing functionality in their systems. Because of her interests, she was tasked to develop the SharePoint site for her team. As a result, she also manages the permissions to the site, but *lacks clear guidance* in the form of a high-level policy to whom she should grant what permissions. She generally does not feel she has the *necessary expertise* to make these decisions and it is sometimes *unclear* to her which *permissions* need to be assigned and how to do this correctly. There are only *informal procedures* for handling permission requests and she sometimes feels a *high emotional pressure* to grant permissions, even though she is unsure whether the permissions are appropriate.

Brandon is the personal assistant to a manager, who has delegated the decisions on who should receive permissions to him. He has similar attitudes towards information security as Amber, and is particularly affected by the *non-transparency of the current policy*, since this makes it difficult to limit the authorized employees to those with a legitimate need.

4.2 Functional management

Lauren manages 40 employees in the financial department and feels responsible for their compliance to the security policy. She motivates her staff to comply by reminding them of why the data is sensitive, and the consequences of non-compliance, including sanctions. She is motivated by both consideration for her own employment (she values job security and also is rewarded for meeting compliance related performance objectives) and an awareness of the risks to the organization caused by non-compliance with regulations. At the same time, she also cares about the productivity of her staff.

As part of her role, Lauren needs to make decisions about authorization policies and review existing

permissions on a regular basis. In this function, she is affected by operational authorization issues, such as the *inefficiency of the procedures*, when, for example, the procedure requires the signature of more senior personnel or from other departments. Generally, she sees the policy-authoring aspects of decision-making as a burden, since the *risk-assessment is complex* and *requires security expertise*. Moreover, it *requires significant technical expertise* to set the permissions due to a *lack of usability* of the management tool. The authorization model sometimes does not allow the precise setting of permissions or they can only be set in inefficient ways, for instance, requiring her to set numerous permissions for each individual of her staff. Consequently, she delegates some of the decisions to her subordinates. For reviewing existing policies, the lack of transparency of the current policies causes a high effort and even limits her ability to review. Since there are no automatic procedures for role changes, employees will also in many cases *retain their permissions*. When delegating functional tasks, Lauren is also affected by the lack of delegation options in the authorization mechanism, forcing her to sometimes share her password.

4.3 Technical staff

Nicole administrates and develops applications as part of the information system department. Because of her detailed knowledge of the systems, she is often consulted on how policy changes can be achieved in the system, for example, which permissions are necessary, and whether the changes are appropriate. In effect, she takes the decision in many cases, although she is not aware of all relevant high-level policies and is sometimes caught in *conflicts of authority*, for example, between departments when one is more security or business-focused than the other. Nicole is also affected by cumbersome permissions that make the policy management difficult and inefficient, for example, when permissions need to be set in a number of separate applications to allow an activity.

5 Causes and effects

The authorization issues raised in the interviews allow us to derive general conclusions on authorization challenges, their causes and effects. The causal diagram in Figure 1 depicts the interrelation of challenges at a high level. Beginning at the impacts on organizational goals in the bottom of the diagram and following the causal links backwards, we describe the most severe and frequently mentioned challenges in the following:

5.1 Restrictive policies and over-entitlements

As stated for the functional staff persona Amber, the main direct impact of authorization on primary tasks results from its operation through missing permissions due to restrictive policies (40 mentions), often seen as frustrating and affecting productivity, particularly when accessing the Web (26):

> *"all forums are blocked which is a bit of a pain... you are looking for sort of technical information... and you'll find an old forum on it and you can't view it so you kind of get ground to a halt"*

In contrast, over-entitlements (16) affect the organizational security when users have more permissions than necessary for their work. Interviewees named a number of causes for restrictive policies and over-entitlements. The most important ones are related to the policy change procedures as well as to the decision-making for policy changes, discussed below. A further reason is the non-transparency of policies (13), which leads, for example, to over-entitlement when stakeholders cannot keep track of who has permissions on folders so that previously required permissions remain. Generally, retained

permissions (4) are seen as an important cause for over-entitlement, for example, when an employee changes role within the organization.

5.2 Requesting policy changes

To correct restrictive policies and, less frequently, over-entitlements, functional staff, such as Amber, request changes to the policy as part of the authorization operation. The most frequently mentioned issues are the required effort to request changes (15) and the change lead time (14), that is, the duration from requesting a change until its enactment in the system:

> *"if someone... need to get access... immediately because it is job critical, then they will use that password in the meantime while they are waiting for theirs to come through."*

The result from those issues is that the requester is forced to circumvent the authorization measure. The perception of the lead time and required effort also deters the functional stakeholder from requesting a permission in the first place, for example, when convenient circumvention is possible or the permission is only required temporarily. Similar to these issues are problems of unclear or ineffective procedures (13):

> *"accesses were challenging at the time,... knowing who you go to, ask for what and how you know that that's what you want... Shared areas... were... problematic in identifying where the data was, who needed to approve the access to it"*

In these cases, the procedures are unknown or known not to help, thus further increasing the perceived effort due to the need to discover the procedure or reducing the perceived effectiveness of pursuing a change of policy.

5.3 Making policy changes

The second perspective on change procedure challenges is from policy authoring, from those deciding on and implementing the changes to the policies. Several of our identified personas are involved in these activities, including functional managers (Lauren), technically-informed functional staff (Emily), personal assistants (Brandon), and administrators/developers (Nicole). Here, one issue is the informality of procedures (3), leading, for example, to non-authoritative decisions (13):

> *"The responsibility in my group was just given to people that were the most computer-savvy at the time."*

The primary challenge for decision-makers is the lack of a high-level policy (5) that defines which permissions should be granted to whom. Determined to take appropriate decisions, decision-makers find it difficult to properly evaluate requests without this kind of guidance:

> *"I don't know about any policy on who should get access to my SharePoint site. It's just based on need."*

A common consequence is that many decisions are taken without a comprehensive consideration of the consequences of the decisions (17):

> *"did somebody actually sit there and think 'Do you need this access?'... I get a person come and says 'Hey, somebody told me I need this, can I have it?' 'Give me this form and I can give it to you [signed].'"*

In this way, decisions are sometimes overly business- or security-driven, leading to over-entitlement and restrictive policies, respectively. In other cases, decisions are solely based on formalities, for example, neglecting to consider whether the access is actually necessary as long as the formalities, such as a specific training, are fulfilled by the requesting employee.

Related to these issues is the problem of conflicts of authority (2), for example, when permissions are bargained between departments:

> *"one of the owners of the... shared drive, I'm one of the others, he was allowing all these other people, saying 'I need to put so and so on.' Well, I said 'Do they have the [certification]? ... You've given them access to all that information.'"*

In other cases, particularly when decisions are decentralized, the emotional costs of denials (2) are relatively high and might even lead to decision-makers taking inappropriate decisions:

> *"there have been a couple of people that have been 'Well, I'm not doing anything with it,'... 'Why are you so difficult'*

Another challenge arises from the implementation of authorization in information systems. In systems with inadequate authorization models (11), such as only offering coarse-grained restrictions, it is difficult to enforce the appropriate restrictions.

> *"So all the things people are working on, everyone has access to... that's the granularity that's given... because of the logistics associated with managing that sort of access."*

In some cases, the lack of usability of policy authoring also leads to high effort costs when employing finer-grained restrictions, thus preventing precise restrictions.

5.4 Circumventing authorization measures

The interviewees frequently reported that authorization operation issues, foremost restrictive policies and the perceived effort for policy changes, lead to the circumvention of the system, for example, through sharing passwords with coworkers:

> *"Sometimes people don't have access to information that they need to do their job and therefore the passwords are shared within teams. And I flagged that before, but it does happen, because it can take so long, months, to get something through. So it would be, 'Use somebody else's account.'"*

Overall, interviewees describe a high level of compliance in the organization, for example, generally feeling uneasy when not complying. Considering the general tendency to comply, the high number of mentions of circumventions related to authorization (58) is alarming. The identified circumventions differ widely in severity with respect to their impact on the organizational goals. Circumventions range from sending documents by email instead of changing the policy to the sharing of passwords to grant access. We grouped the types of circumventions into the following categories:

- Workarounds (13): using technical means within the system, for example, using multiple accounts,
- Technical circumvention (20): using technical means outside of the system, such as sending documents on physical media,
- Social circumvention (25): employing social means to work around authorization measures, such as sharing passwords.

We summarized the types of circumventions with examples and potential effects in Table 3 and found that circumventions impact five of the six organizational goals, including the productivity (security and functional efficiency), security effectiveness, regulatory compliance, and employee satisfaction.

Table 3: Workarounds, technical and social circumventions of authorization measures

Workaround/circumvention	Example	Effects
Utilize tech. loopholes (6)	Rename attachment extension	Functional inefficiencies
Increase redundancy (3)	Copy a document to a place which can be accessed	Inefficient, non-transparent policy
Multiple accounts (2)	Switch between accounts for different permissions	Undermines identity scheme, inefficient
Spare accounts (1)	Teams e.g. prepare a number of accounts for new temps	Potential missing traceability of activities
Make doc. public (1)	Move document to a public folder to allow access	Undermines policy enforcement
Share through alternative media (12)	Send document by email or physically on CD, rather than changing the policy	Loss of control over data; potentially increased risk; redundancy of data
Use private device (6)	Access information not available from work devices from smartphone or home PC	Risks from data on devices not governed by organization's security policy
Use external system (2)	Post documents on an organization-external system to grant access to externals	Risks from documents outside of the organization's security realm
Share passwords (21)	Share password instead of waiting for permissions to be changed	Lack of traceability/audibility; breaking security policy
Coworkers as proxy (3)	Turn to coworkers for a task due to lacking permissions	Potentially inefficient
Share logged-in account (1)	Have coworkers complete tasks at a logged-in computer	Lack of traceability/audibility

6 Authorization Paradigms

In the previous section, we studied general causes and effects of authorization issues. However, employees of the organization are affected by challenges in a broad range of systems that inhibit very different characteristics with respect to the authorization context. To analyze how these characteristics affect the challenges, we selected two system contexts, "Shared folders" and Microsoft SharePoint, for a focused, comparative analysis. These systems are similarly employed and were mentioned frequently, but have opposing characteristics, representing different authorization paradigms in the formality and centralization of the change procedures and decision-making.

6.1 Microsoft SharePoint

Microsoft SharePoint is used in the organization for the sharing of documents in teams, departments, and organization-wide. Departments and teams develop and manage local SharePoint sites, including the authorization policy that defines the restrictions on the access of SharePoint-hosted resources, granted for individual employees. A high-level visualization of the interrelation of authorization challenges is shown in Figure 2. Most impacts are on the effectiveness of security and regulatory compliance, primarily causing circumventions of the authorization measures in the system, for example, using email for sharing instead of adapting the policy, and permissive policies (inadequate policies). These, in turn, mostly result from issues with the policy change procedures and decisions, which are detailed in Table 4. Implementation problems, such as usability problems with the policy management, and the lack of transparency of the policies, preventing implicit policy reviews, affect organizational goals to a lesser degree.

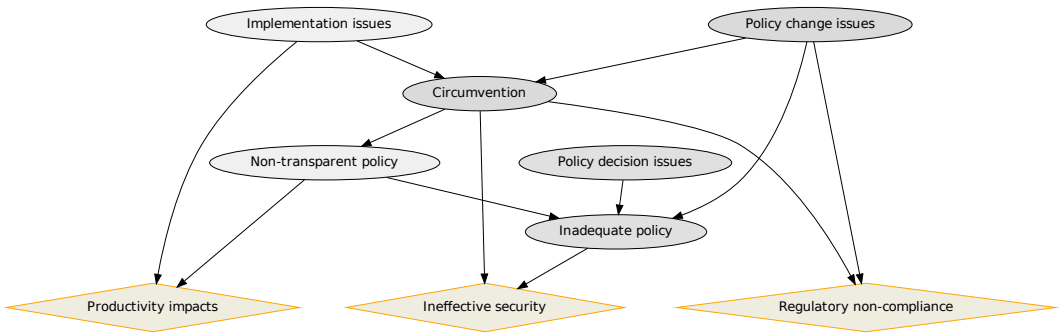

Figure 2: Categorized challenges related to SharePoint sites

Table 4: Comparing mentions of problems with decisions and procedures

	SharePoint		Shared folders	
Issues	Dec.	Proc.	Dec.	Proc.
Decentralized decisions	2			
Required/present expertise	5			
Lack of high-level policy	3			
Non-comprehensive decision	3			
Business-driven decisions	1			
Coarse-grained restrictions	2		1	
Lack of usability	2			
Change lead time		2		7
Required change effort				4
Ineffective change procedures		2		2
Availability of authority		2		1
Informal procedure		1		1
Inefficient procedure				5
Unclear procedure		1		4
Conflicts of authority				1
Non-authoritative decision		5		1
Effects				
Loss of traceability		2		
Over-entitlement	5		8	
Restrictive policy		1		6
Circumvention		8		13
Inefficient security		2		5
Functional efficiency		3		9
	23	29	9	59

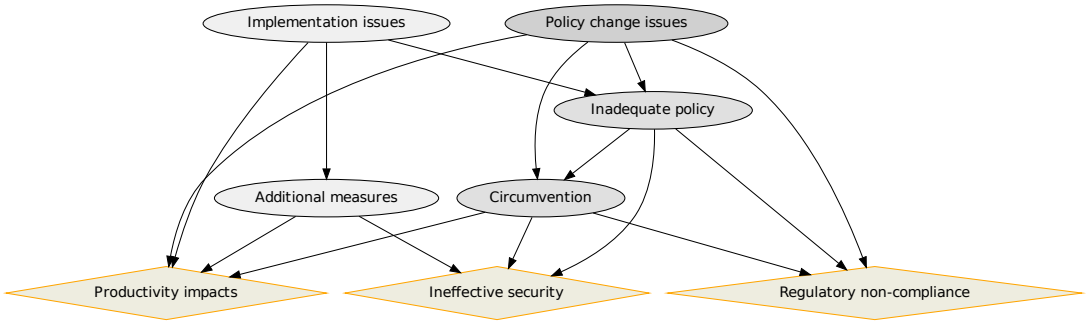

Figure 3: Categorized challenges related to Shared folders

6.2 Shared folders

Shared folders represent the traditional way of sharing documents in the organization. These are meant to be replaced by the above-discussed SharePoint infrastructure. Users access a shared network drive from their desktop through the file explorer. Authorization is primarily enforced on a folder level. In contrast to the SharePoint procedures, folder permissions are granted to employees through a centralized process. As depicted in Figure 3, the policy change procedures were mentioned in the interviews most frequently as challenges that impact, directly or indirectly, on the effectiveness of security, productivity, and regulatory compliance. The policy change issues are given in Table 4, including the important aspects of high perceived change effort and change lead time.

6.3 Comparison

While apparently similar in terms of structures, the challenges of the two contexts reveal a number of differences when focusing on change procedures and policy decisions. Specifically, procedure issues are more prevalent with Shared folders. Table 4 shows that procedure issues (column "Proc.") are mentioned more frequently for Shared folders than for SharePoint. For instance, the change lead time and the required change effort is most relevant for Shared folders. Accordingly, there is less mention of circumvention and productivity impacts from hindering work or inefficient procedures for SharePoint sites.

While the SharePoint procedure has fewer negative impacts overall, there can be more severe problems with the procedure if, for example, the responsible person does not respond:

> *"Sometimes you don't get a response for months and you don't know who to chase. At least with the Shared folders [process] you've got the request number and you can ring up about it."*

Overall, the severity index of procedure issues, derived from the sum of mentions, shown in the bottom row of the table, is significantly lower for SharePoint.

A second area of effects of the paradigms are the decisions on policy changes. As the severity index in the table indicates, decision problems are significantly more frequent for SharePoint than for Shared folders. Primarily, there is a concern in the case of SharePoint that due to the local decisions and the informal nature of the procedure, the decisions might not in all cases be adequate and the local policy administrators may lack security expertise:

> *"a user who is not trained properly can actually give, access to everything quite easily*

through a couple of clicks, um, in SharePoint I think it is quite easy to not give access to the right areas... because it has quite a confusing way of giving permissions"

In contrast, there is only a small number of mentions of decision problems for Shared folders.

Overall, our results indicate that it is more efficient to have decisions taken and enacted locally than in a centralized procedure. Problems with local changes foremost arise from overly informal procedures and a lack of expertise in decision-making. These results are in line with Pallas' theory [12], which predicts the trade-off between hierarchical and market forms of coordination for information security in organizations. Particularly, we see the effects of information asymmetries in the lack of expertise of local decision-makers and the high hierarchical coordination costs for centralized decisions.

7 Discussion

Our findings on authorization issues and their interrelation, and the more focused results of comparing centralized/structured with local/informal procedures and decision-making offer a detailed picture of challenges in organizational authorization. Our results are based on the study of a single organization and the analysis of subjective data. The quantity of mentions may be skewed by the sampling of participants who may have had reason to volunteer for the study so our quantitative results should not be taken as proof. However, this being a rich data set of 118 interviews together with the variety of users and authorization contexts, the results from the study allow us to provide a thorough description of the problems and formulate well-grounded hypotheses on the causes of usability issues in authorization for further research.

7.1 Guide and monitor circumventions

Circumventions of authorization measures are not necessarily the inferior option, particularly when considering the losses of productivity that would occur otherwise, for instance, when waiting for policies to be changed. However, the interviewees often stated that they feel uncomfortable when they are forced to break a security policy and consider potential negative impacts from additional risks. Moreover, architectural authorization measures cannot entirely prevent their circumvention. Formal rules through security policy and informal rules through common understanding in teams must complement architectural measures [12, 21].

- *Provide formal rules on circumventions*: Formal rules can define in security policies, for instance, which circumventions are permissible in specific situations. Particularly accounting for the effects of the Compliance Budget (see Section 2.3), employees need a comprehensible and actionable policy, so that compliance can be focused on high-risk issues and employees can be guided to use the circumvention with the least negative effects on the organizational goals.

- *Foster informal rules on circumventions*: Informal rules are built and enforced through social interaction, often on a team level. Awareness campaigns and technological means can shape the informal rules by providing focused input on the risks of different kinds of circumventions [20].

- *Monitor circumventions*: Our findings on the effects of authorization issues show that circumventions are a good indicator of underlying issues and should be monitored closely to identify optimization potential for existing policies and procedures.

7.2 Establish adequate procedures

We found many cases in which the procedures for policy changes caused authorization issues. These issues are part of the operation of authorization, so that this extends the prior work on supporting the communication between stakeholders in policy authoring (see Section 2.2).

- *Define and communicate procedures*: Procedure ambiguity and informality have serious effects on the effectiveness of change operations and organizational productivity. Clearly communicating the procedures to functional stakeholders will also lower the threshold for requesting changes.
- *Reduce the (perceived) change lead time and change effort*: Circumventions are often caused by the duration for the changes to be enacted and the effort to initiate changes. Applying economic models to security usability (see Section 2.3), reveals that we need to reduce the costs of compliance. We thus expect that a reduction of change lead time and effort and their perception will result in less circumventions. However, the relation between the perceived costs and compliance is likely to be non-linear, so that we need to reach a specific target threshold for compliance to become the default.
- *Adjust the degree of centralization*: Theoretical models [12] and our observations on different authorization paradigms show that decentralized procedures and decisions can be advantageous, given that the decision-makers have baseline security expertise (see below) and the procedures remain traceable. More decentralized procedures can also formalize informal delegation and, thus, improve the traceability.

7.3 Support policy decisions

Our results indicate that many authorization challenges originate in the decision-making part of policy authoring:

- *Provide high-level policies on authorization decisions*: Decision-makers need to be supported in taking appropriate decisions on grants and denials. One way to provide support is through high-level policies on how to decide on requests. Similar to the high-level policies on circumvention, these policies need to be adequate for the specific context, actionable, and comprehensible.
- *Increase the expertise and awareness of decision-makers*: In addition to providing guidance on decisions, additional expertise and awareness on consequences from decisions, both on risks from grants and functional impacts from denials, will help to improve the appropriateness of decisions [20].
- *Provide decision support to policy makers*: A further option to support decision-makers is to offer dedicated tools that help in the decision-making process. These can collect factors on the sensitivity of the data and potential consequences of unintended disclosures as well as request-specific factors, such as the purpose of the request. From these factors, a comprehensible overview of decision factors may then be generated to increase the awareness for the full breadth of aspects. This follows the similar suggestions on decision support, such as for password policies [13] and security investments [5], and may also include the risk perception of functional staff [7].
- *Improve authorization models and management tools*: As shown in prior work on policy editing and challenges in practice (Sections 2.1 and 2.2), appropriate and usable policy editing tools and authorization models are required for effective measures. Our results confirm those findings, showing that the precision of policies is governed by the appropriateness of the authorization model.

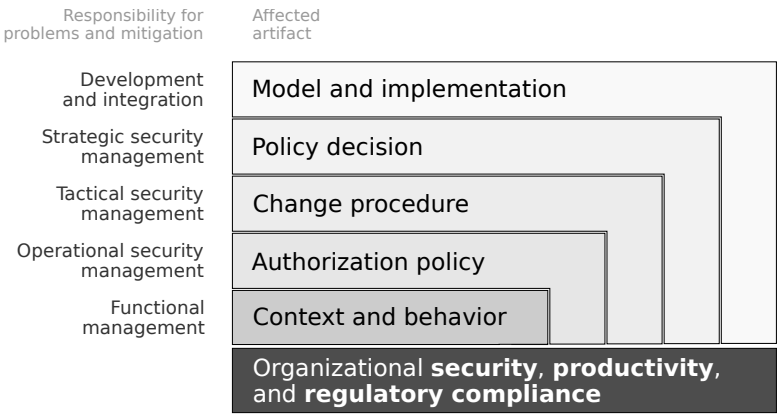

Figure 4: Layered interrelations between issues with authorization artifacts

Table 5: Artifacts in authorization and how issues with them affect the other layers

Artifact	Responsibility	Activity	Example issue	Primarily affected	Example mitigation
Model, implementation	Development, integration	Develop, integrate	Unusable model or interface	Policy author	Improve model or tool usability
Policy decision	Strategic sec. management	Make high-level policy	Missing high-level policy	Policy author, decision-maker	Provide high-level policy
Change procedure	Tactical sec. management	Design process	High change lead time, inefficient procedure	Functional staff, policy author, decision-maker	Establish lightweight procedure
Authorization policy	Operational sec. mgmt.	Change policy	Restrictive policy, permissive policy	Functional staff, organization	Grant adequate permissions
Context and behavior	Functional management	Influence behavior	Reduced productivity, circumvention	Organization	Increase risk awareness

7.4 A holistic approach

Our findings show that effective mitigation of authorization problems requires addressing several interrelated aspects. To visualize the layers and their relationships, we can abstract from the found causal relations and structure the problems by the affected artifact as depicted in Figure 4. In the diagram, the issues in upper-layer artifacts foremost affect lower layers and ultimately the organizational goals (cf. Table 5).

Prior work on authorization problems primarily focused on policy authoring (cf. Section 2.2), which can be found in the *Authorization policy* layer. From the interrelations between the given layers, we can expect that such a selective focus will only solve part of the problem. There are indirect effects of higher layers that will reduce the effectiveness of mitigations on individual layers. One of the examples given in Table 5 is the missing guidance for decisions on the *Policy decision* layer that impacts the adequacy of policy changes. If this problem exists, focusing selectively on the usability of the configuration interface might prove ineffective. Instead, we need to broaden the analysis and mitigation of problems with organizational authorization.

8 Conclusions

We analyzed 118 interviews for challenges with authorization measures and their interrelation with organizational goals. In line with prior practical studies, we found that the authorization models and policy authoring tools impact the authorization usability. Beyond prior findings, we identified

significant issues with the operation of authorization from the procedures for policy changes and the decision-making part of policy authoring. Moreover, we showed that the authorization issues are deeply interrelated and affect the organizational goals of effective security and productivity.

One common consequence of problems with authorization is the circumvention of the security measure. Interestingly, while Adams and Sasse [1] showed how users circumvent security measures due to a lack of security awareness, our participants reported a high number of circumventions to complete their work despite being security-conscious and uncomfortable with breaking the policy. This trade-off between productivity and security risks supports the economic models on security compliance [4, 10].

On an organizational level, we showed that the degree of centralization and formality is a crucial factor in designing authorization measures as predicted by Pallas' theories on organizational information security [12]. Centralized and formal procedures simplify traceability and sound decisions, but increase hierarchical coordination costs. Conversely, delegated, localized decisions and procedures may reduce overhead and circumventions, and increase productivity, at the cost of information asymmetries.

The study is only based on interviews in one organization and the subjective data drawn from them so that we must be careful when drawing general conclusions from the number of mentions. However, the organization has very diverse authorization contexts and the rich data set includes a wide variety of stakeholders. Moreover, where overlapping, our findings are in line with prior studies on organizational authorization and fit with models from security usability and management. Thus, the results offer a detailed description of the problems, make a case for organizations to address them, and should serve as an initial hypothesis for further, quantitative research.

9 Acknowledgments

We would like to thank the organization, which remains anonymous, for enabling the research and the interviewees for investing their time. We are also grateful for the great work of the interviewers.

References

[1] A. Adams and M. A. Sasse. Users are not the enemy. *Commun. ACM*, 42:40–46, December 1999.

[2] R. Anderson. Why Information Security is Hard-An Economic Perspective. In *ACSAC '01: Proceedings of the 17th Annual Computer Security Applications Conference*, pages 358–, Washington, DC, USA, 2001. IEEE Computer Society.

[3] L. Bauer, L. F. Cranor, R. W. Reeder, M. K. Reiter, and K. Vaniea. Real life challenges in access-control management. In *CHI '09: Proceedings of the 27th international conference on Human factors in computing systems*, pages 899–908, New York, NY, USA, 2009. ACM.

[4] A. Beautement, M. A. Sasse, and M. Wonham. The Compliance Budget: Managing Security Behaviour in Organisations. In *NSPW '08: Proceedings of the 2008 Workshop on New Security Paradigms*, pages 47–58. ACM, 2008.

[5] Y. Beresnevichiene, D. Pym, and S. Shiu. Decision support for systems security investment. In *Network Operations and Management Symposium Workshops (NOMS Wksps)*, pages 118–125, Apr. 2010.

[6] S. Brostoff, M. A. Sasse, D. W. Chadwick, J. Cunningham, U. M. Mbanaso, and S. Otenko. 'R-What?' Development of a role-based access control policy-writing tool for e-Scientists. *Softw., Pract. Exper.*, 35(9):835–856, 2005.

[7] R. Coles and G. P. Hodgkinson. A Psychometric Study of Information Technology Risks in the Workplace. *Risk Analysis*, 28(1):81–93, 2008.

[8] A. Cooper, R. Reimann, and D. Cronin. *About face 3: The essentials of interaction design.* Wiley, 2007.

[9] S. Faily and I. Flechais. Persona Cases: A Technique for grounding Personas. In *CHI '11: Proceedings of the 2011 annual conference on Human factors in computing systems*, Vancouver, BC, Canada, 2011. ACM.

[10] C. Herley. So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users. In *NSPW '09: Proceedings of the 2009 workshop on New security paradigms*, 2010.

[11] P. Inglesant, M. A. Sasse, D. Chadwick, and L. L. Shi. Expressions of expertness: the virtuous circle of natural language for access control policy specification. In *SOUPS '08: Proceedings of the 4th symposium on Usable privacy and security*, pages 77–88, New York, NY, USA, 2008. ACM.

[12] F. Pallas. *Information Security Inside Organizations – A Positive Model and Some Normative Arguments Based on New Institutional Economics.* PhD thesis, TU Berlin, 2009.

[13] S. Parkin, A. van Moorsel, P. Inglesant, and M. A. Sasse. A stealth approach to usable security: helping IT security managers to identify workable security solutions. In *NSPW '10: Proceedings of the 2010 workshop on New security paradigms*, pages 33–50, New York, NY, USA, 2010. ACM.

[14] 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.

[15] J. Rode, C. Johansson, P. DiGioia, R. S. Filho, K. Nies, D. H. Nguyen, J. Ren, P. Dourish, and D. Redmiles. Seeing further: extending visualization as a basis for usable security. In *SOUPS '06: Proceedings of the second symposium on Usable privacy and security*, pages 145–155, New York, NY, USA, 2006. ACM.

[16] K. Sikkel and O. Stiemerling. User-Oriented Authorization in Collaborative Environments. In *COOP '98*, 1998.

[17] S. Sinclair, S. W. Smith, S. Trudeau, M. E. Johnson, and A. Portera. Information Risk in Financial Institutions: Field Study and Research Roadmap. In *Proceedings for the 3rd International Workshop on Enterprise Applications and Services in the Finance Industry*, pages 165–180, 2008.

[18] D. K. Smetters and N. Good. How users use access control. In *SOUPS '09: Proceedings of the 5th Symposium on Usable Privacy and Security*, pages 1–12, New York, NY, USA, 2009. ACM.

[19] K. Vaniea, L. F. Cranor, Q. Ni, and E. Bertino. Access Control Policy Analysis and Visualization Tools for Security Professionals. In *USM '08: Workshop on Usable IT Security Management*, 2008.

[20] R. West. The psychology of security. *Commun. ACM*, 51:34–40, April 2008.

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

[22] M. E. Zurko, R. Simon, and T. Sanfilippo. A User-Centered, Modular Authorization Service Built on an RBAC Foundation. In *S&P '99: Proceedings of the 1999 IEEE Symposium on Security and Privacy*, Los Alamitos, CA, USA, 1999. IEEE Computer Society.

[23] 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, New York, NY, USA, 1996. ACM.