HOW USERS BYPASS ACCESS CONTROL – AND WHY: THE IMPACT OF AUTHORIZATION PROBLEMS ON INDIVIDUALS AND THE ORGANIZATION

Steffen Bartsch, CASED, TU Darmstadt, Hochschulstr. 10, 64289 Darmstadt, Germany, steffen.bartsch@cased.de

M. Angela Sasse, Department of Computer Science, University College London, London, WC1E 6BT, UK, a.sasse@cs.ucl.ac.uk

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 consider the full range of underlying problems, and their impact on organizations. We present a study of 118 individuals' experiences of authorization measures in a multi-national company, and their self-reported subsequent behavior. Building on recent research that applies economic models to show the impact of lack of usability, we analyze the interrelations of authorization issues with individuals' behaviors and organizational goals. Our results indicate that authorization problems significantly reduce the productivity and effective security of organizations. We analyzed the authorization problems of different stakeholders, and found they are mostly caused by the procedures for policy changes (e.g. long change lead-times) and the decision-making (e.g. inexperienced decision makers); the consequence is the circumvention of access control (e.g. by sharing passwords). As one research contribution, we develop a holistic model of authorization problems. More practically, we recommend to provide guidance for non-compliance, such as password-sharing, and to establish light-weight procedures for policy changes with adequate degrees of centralization and formalization, and support for decision-making.

Keywords: Access control · Authorization · Security usability · Security management · Empirical study.

1 Introduction

Authorization is a core aspect in organizations to enforce security policies in information systems[1]. 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 (West, 2008). A number of studies have analyzed the usability of authorization and found that crafting authorization policies[2] is difficult, both in laboratory experiments (Brostoff et al., 2005; Zurko and Simon, 1996) and in practice (Bauer et al., 2009; Smetters and Good, 2009).

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 (Beautement, Sasse, and Wonham, 2008), 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 problems surrounding existing authorization mechanisms, and their impact on organizational goals. We apply models of security economics and the organizational information security to motivate our study and emphasize the impact of security mechanisms on the individual and the organization. We conducted 118 in-depth interviews on security compliance at a large infrastructure company with a variety of authorization contexts.

We systematically analyzed the transcripts of those interviews to identify causes and effects of the problems with authorization, and how they impact organizational goals. Particularly notable are the effects of long lead-times for changes of permissions and of the lack of expertise of those deciding on the changes. We also compare two authorization contexts within the organization that differ in their degree of formality and centralization of procedures, and show that the procedures for changing authorization policies and the policy decision-making are particularly important. Based on our findings, we discuss approaches to mitigate the problems, including explicit guidance of circumvention, clear procedures, and supporting the decisions for policy changes.

2 Background

2.1 Problems with authorization 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 (1998), *Bauer* et al. (2009), and *Smetters* and Good (2009) examine how the expressiveness of authorization models affect policy management and suggest model improvements. Bauer also analyzes the interactions of policy authors with different roles. In contrast, *Whalen* et al. (2006) not only explores the problems of managing authorization, but also how authorization interferes with the primary tasks of functional users.

[1] We refer to authorization as the restriction of activities of a principal in a system – the second step in access control

[2] We use the term authorization policy for the restrictions enforced by information systems. Security policies herein denote the management-level definitions of how the organization aims to achieve its security goals (Baskerville & Siponen, 2002)

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 if, only as anecdotal individual cases – the authorization issues are ignored. One reason is that the scale and the actual impact on organizational goals are not known. 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.

Study	*Study design*	*Environment*	*Focus/scope*	*Findings*
Sikkel	Subjective: interviews	Private and public organizations	How users specify policies	Policies are stated as grants/denials, refined by exceptions, e.g. scopes
Whalen	Subjective: survey, interviews	Medium-sized research laboratory	Individuals' problems from mechanisms	Users manage policies, but struggle with it; authorization interferes with primary tasks
Bauer	Subjective: interviews	Diverse organizations	Challenges for policy professionals	Problems from stakeholder interactions and inadequate models
Smetters	Objective: historical policy data	Medium-sized corporation	Usage of authorization features and models	Complex, rarely changed policies, management errors

Table 1: Prior studies on authorization in organizations

2.2 Economic perspective

Usable security research to date has focused on the mistakes users make, and how they reduce security. In authorization research, for example, it has been observed that entitlements are not adjusted to reflect organizational changes, resulting in over-entitlement which in turn can enable security breaches (Sinclair et al., 2008). 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 (West, 2008).

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 (Anderson, 2001). Beautement et al. described the Compliance Budget (2008) and Herley analyzed the externalities of security measures (2009). They argue that we need to consider the costs and benefits of security measures, particularly from the individuals' point of view, to understand their behavior. Beautement et al. show that insecure use of USB sticks and violations of password policies are caused by high perceived effort for no gain. Herley (2009) argues that users often act rationally in not complying with security advice, since the risk/effort ratio is too large. This line of thinking can be applied to authorization as well. As already noted above, authorization has been found to impact the primary tasks of employees (Whalen et al., 2006). 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 to 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 (2009) 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 extent 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 problems and their impacts in practice, we studied the security compliance of employees in a large multi-national company, which 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

The interviews explored compliance issues with a range of policies and mechanisms, but our analysis here focused on the authorization-related segments in the transcripts. We applied a Grounded Theory approach (Glaser and Strauss, 1967) and coded for authorization usability issues and their causes and effects. Almost two-thirds of the interviewees (75 of 118) mentioned authorization problems in one of the organizational information systems, including, amongst others, file sharing and restrictions to Web access. We applied open and axial coding to the quotes on authorization problems such as the following:

> *"they may need [the password for] temporary access... a lot of the IS setup takes so long, these are workarounds to solve a temporary problem...it tends to bounce around...for quite a long while"*

To establish relationships between the codes, we conducted a "causal" coding. We assigned three types of codes to quotes: the problem ("Change lead time" in the above example), causes ("Complex procedure"), and effects of the issue ("Social circumvention: Password sharing").

We related the diverse problems to the following organizational goals that we identified by projecting Schermerhorn et al.'s (2008) organizational goals to authorization measures:

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

We identified 540 authorization-related quotes in the interview transcripts and coded the quotes with the system context (primarily, the kind of application) as well as causes and effects as tuples or triples

in a spreadsheet. We explored the data with a custom analysis tool that derives relationships from the coded quotes and generates diagrams using the Graphviz tool suite[3]. An example of the diagrams is shown in Figure 1: causal edges connect causes with problems, 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. The darkness of the shade of the nodes in the diagrams refers to the number of mentions in the study.

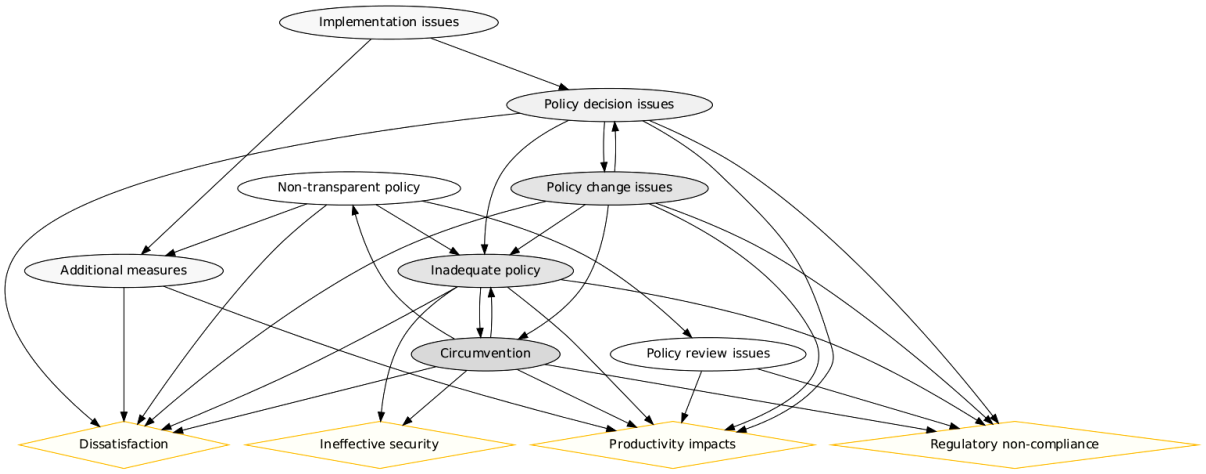

Figure 1: Interrelation of the categorized authorization problems

4 Authorization problems: Causes and effects

The authorization issues raised in the interviews allow us to derive general conclusions on authorization problems and their causalities. We describe the most severe and most-frequently mentioned challenges in the following:

4.1 Restrictive policies and over-entitlements (Inadequate policy)

For the functional staff, the main direct impact of authorization on primary tasks results from 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.

[3] http://www.graphviz.org/

4.2 Problems with requesting policy changes (Policy change issues)

To correct restrictive policies and, less frequently, over-entitlements, functional staff 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.

4.3 Problems with making policy changes (Policy change/decision issues)

The second perspective on change-procedure problems is from policy authoring, from those deciding on and implementing the changes to the policies. Several members of staff are involved in these activities, including functional managers, technically-informed functional staff, personal assistants, and administrators/developers. 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. 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.

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."*

4.4 Circumventing authorization measures

Many interviewees 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 co-workers:

> *"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, and they generally feel uneasy about not complying. Given this stance, 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 found that circumventions impact five of the six organizational goals, including the productivity (security and functional efficiency), security effectiveness, regulatory compliance, and employee satisfaction.

4.5 A holistic model of problems with authorization

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 2. In the diagram, the issues in upper-layer artifacts foremost affect lower layers and ultimately the organizational goals. Examples for stakeholders and problems on the individual layers are given in Table 2.

Prior work on authorization problems often focused primarily on policy authoring (cf. Section 2.1), which can be found in the Authorization policy layer. From the interrelations between the given layers, we can expect that a selective focus will only solve part of the problem. There are effects of higher layers that will reduce the effectiveness of addressing an individual layer. One example given in Table 2 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. Thus, instead of limiting the analysis to a subset of problems, we need to apply the holistic problem-model to solve the problems with organizational authorization.

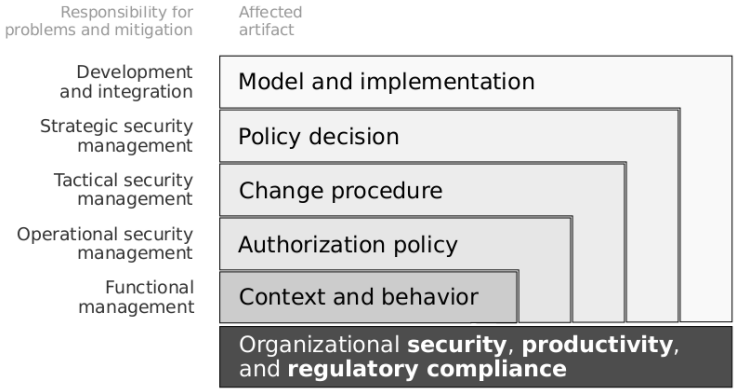

Figure 2: Layered interrelations between issues with authorization artifacts

Artifact	*Responsibility*	*Activity*	*Example problem*	*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 light-weight 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

Table 2: Artifacts in authorization and how issues with them affect the other layers

5 Applying the holistic model for analysis of authorization problems

In the previous section, we studied the general causes of authorization problems and showed how they interrelate in a holistic model. 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 based on the holistic model 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.

5.1 Microsoft SharePoint

Microsoft SharePoint is used in the organization for the sharing of documents in teams and departments. Departments and teams develop and manage local SharePoint sites. This includes the management of the authorization policy that grants access to the SharePoint-hosted resources on an employee level. Staff can request access to resources by clicking on a dedicated link when access is

denied and thus send an email to resource-specific policy maker, who then decides on the appropriateness of the request. Problems primarily occur due to permissive policies and circumventions of the authorization measures in the system, impacting the effective security and regulatory compliance. For example, staff use email for sharing documents instead of adapting the policy. The reasons often are inadequate policies that result from problems with the change procedures and decisions, which are detailed in Table 3. Implementation problems, such as usability problems with the policy management, and the lack of transparency of the policies – preventing effective policy reviews – affect organizational goals as well, but to a lesser degree.

5.2 Shared Folder

Shared Folders represent the traditional way of sharing documents in the organization – and were meant to be replaced by the SharePoint infrastructure (see above) in the long run. 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. 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 3, notably including the high perceived change effort and change lead time.

Decision problems		
Issues	SP	SF
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	
Effects		
Over-entitlement	5	8
	23	9
	44%	13%

Procedure problems		
Issues	SP	SF
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	
Restrictive policy	1	6
Circumvention	8	13
Inefficient security	2	5
Functional efficiency	3	9
	29	59
	56%	87%

Table 3: Comparing mentions of problems with decisions and procedures

5.3 The effects of the different contexts

Structuring the identified problems according to the holistic model, we can observe a number of differences when examining the problems with change procedures and policy decisions for the two systems. Specifically, procedure issues are more prevalent with Shared Folders. Table 3 shows that procedure issues are mentioned more frequently for Shared Folders (SF, 87% of decision and procedure problems for Shared Folders) than for SharePoint (SP, 56%). For instance, the change lead time and the required change effort are 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 proportion of procedure issues is significantly lower for SharePoint.

A second area of effects of the contexts concerns the decisions on policy changes. As the proportions of the problem types in the table indicate, decision problems are significantly more frequent for SharePoint (44%) than for Shared Folders (13%). 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. While we could not control for the same usage intensity and patterns between the two contexts, the clear relative distribution of mentions within each context should sufficiently support our argument.

Overall, our results indicate that it is more efficient to take and enact decisions locally. 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 (Pallas, 2009), which predicts the trade-off between hierarchical and market forms of coordination for information security in organizations. We particularly see here the effects of information asymmetries in the lack of expertise of local decision-makers and the high hierarchical coordination costs for centralized decisions.

6 Discussion

We analyzed 118 interviews for challenges with authorization measures and their interrelation with organizational goals. The study is only based on interviews with a potential self-selection bias in one organization and the subjective data drawn from them so that we need to 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. 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.

Our study confirms prior research regarding how 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. While Adams and Sasse (1999) found that 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 (Beautement et al., 2008; Herley, 2009). Our analysis covered both aspects of the trade-off. 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 (Pallas, 2009). 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.

From our results, we recommend the following for the design of authorization measures:

6.1 Guide circumventions

Circumventions of authorization measures are not necessarily wrong, 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. Thus, an organization should guide when and in which form circumvention is acceptable instead of entirely prohibiting circumvention. This guidance can be given in formal rules through security policy and in informal rules through common understanding in teams. The guidance thus complements the architectural measures of technical authorization in applications (Pallas, 2009; cf. Whalen et al., 2006).

6.2 Establish adequate procedures

We found many cases in which the procedures for policy changes caused authorization problems. This extends the prior work on supporting the communication between stakeholders in policy authoring (see Section 2.1). Specifically, we recommend from our results:

1. *Define and communicate procedures*: Procedure ambiguity and informality have serious effects on the effectiveness of change operations and organizational productivity. For instance, participants did not know how to request permission changes.
2. *Reduce the (perceived) change lead time and change effort*: Circumventions were 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 2.2) indicates 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.
3. *Adjust the degree of centralization*: Our observations on different authorization contexts 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.

6.3 Support policy decisions

Our findings indicate that many authorization problems originate in the decision-making part of policy changes:

1. *Provide high-level policies on authorization decisions*: Decision-makers stated that they lacked any guidance on what decisions on grant and denials were appropriate. 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.
2. *Increase the expertise and awareness of decision-makers*: Participants further stated that decisions were often biased – for example, from formalities, business or security perspectives. 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.
3. *Improve authorization models and management tools*: Participants described how they are impacted by problems with the authorization model and the lack of usability of policy-management tools. This supports prior work on authorization challenges in practice (Section 2.1)

that appropriate and usable policy editing tools and authorization models are required for effective measures.

Acknowledgements

We first and foremost thank the organization and their staff for the access and time given, and Philip Inglesant (UCL) and Simon Arnell (HP), who carried out a number of the interviews. Many thanks to Adam Beautement and Iacovos Kirlappos at UCL for detailed feedback on early drafts of the paper, and helpful comments on later ones, respectively.

References

Adams, A., and Sasse, M. A. (1999). Users are not the enemy. *Commun. ACM*, *42*(12), 40–46. doi:10.1145/322796.322806

Anderson, R. (2001). Why information security is hard - an economic perspective. *Proceedings 17th Annual Computer Security Applications Conference, 2001. ACSAC 2001* (pp. 358 – 365). doi:10.1109/ACSAC.2001.991552

Baskerville, R., and Siponen, M. T. (2002). An information security meta-policy for emergent organizations. *Logistics Information Management*, *15*(5/6).

Bauer, L., Cranor, L. F., Reeder, R. W., Reiter, M. K., and Vaniea, K. (2009). Real life challenges in access-control management. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '09 (pp. 899–908). New York, NY, USA: ACM. doi:10.1145/1518701.1518838

Beautement, A., Sasse, M. A., and Wonham, M. (2008). The compliance budget: managing security behaviour in organisations. *Proceedings of the 2008 workshop on New security paradigms*, NSPW '08 (pp. 47–58). New York, NY, USA: ACM. doi:10.1145/1595676.1595684

Brostoff, S., Sasse, M. A., Chadwick, D., Cunningham, J., Mbanaso, U., and Otenko, S. (2005). "R-What?" Development of a role-based access control policy-writing tool for e-Scientists. *Software: Practice and Experience*, *35*(9), 835–856. doi:10.1002/spe.691

Glaser, B. G., and Strauss, A. L. (1967). *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Aldine Transaction.

Herley, C. (2009). So long, and no thanks for the externalities: the rational rejection of security advice by users. NSPW '09 (pp. 133–144). New York, NY, USA: ACM. doi:10.1145/1719030.1719050

Pallas, F. (2009). *Information Security Inside Organizations – A Positive Model and Some Normative Arguments Based on New Institutional Economics*. TU Berlin.

Schermerhorn, J. R., Hunt, J. G., and Osborn, R. N. (2008). *Organizational Behavior* (10th ed.). Wiley.

Sikkel, K., and Stiemerling, O. (1998). User-Oriented Authorization in Collaborative Environments. *COOP '98*.

Sinclair, S., Smith, S. W., Trudeau, S., Johnson, M. E., and Portera, A. (2008). Information Risk in Financial Institutions: Field Study and Research Roadmap. *Proceedings for the 3rd International Workshop on Enterprise Applications and Services in the Finance Industry* (pp. 165–180). doi:10.1007/978-3-540-78550-7_11

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

West, R. (2008). The psychology of security. *Commun. ACM*, *51*(4), 34–40.

Whalen, T., Smetters, D. K., and Churchill, E. F. (2006). User experiences with sharing and access control. *CHI '06 extended abstracts on Human factors in computing systems* (pp. 1517–1522). New York, NY, USA: ACM. doi:10.1145/1125451.1125729

Zurko, M. E., and Simon, R. T. (1996). User-centered security. *NSPW '96: Proceedings of the 1996 workshop on New security paradigms* (pp. 27–33). New York, NY, USA: ACM.