Cognition Behind Access Control: A Usability Comparison of Rule- and Category-based Mechanisms.

Denis Obrezkov[0000−0001−8822−2932]

TIB Leibniz Information Centre for Science and Technology, Hannover, Germany
University of Bremen, Bremen, Germany
denis.obrezkov@tib.eu

Abstract. Usability of a security mechanism has a notable impact on its efficacy. For instance, if users do not understand how to use the mechanism, they will make frequent mistakes. Given the magnitude of the problem, it seems desirable to understand what underlies the usability of security solutions. To achieve this, one needs to rely on solid theoretical foundation of human perception. In this paper, we investigate a problem of access control usability in the light of cognitive science. We rely on evidence from cognitive psychology and compare two systems that regulate access based on rules and categories. We perform a user-study of two approaches (N=46). Our study reveals that a category-based approach has a higher perceived usability in terms of mental load and user performance. These results allow us to formulate recommendations for designers of access control systems.

Keywords: access control · categorization · cognition

1 Introduction

The usability of modern access control systems often raises significant concerns. Let us consider a hypothetical example of interaction with a modern Android system.

> *User*: I want to **protect my data**.
> *System*: You need to go to System settings and **restrict your applications**.

Indeed, it can be clearly seen that *"protect data"* and *"restrict applications"* are noticeably different tasks. The inference from one to another is not possible without additional knowledge — *"protection in the Android system is based on restriction of applications from the Settings menu"*. Since there is new knowledge, it is essential to convey it to users. However, users might just lack motivation to learn a protection technology [27].

The problem of access control complexity is also faced by experienced users, e.g., security administrators. Let us consider an example of SELinux—an access

control extension, which is utilized in Linux-based systems, including Android. SELinux introduces Mandatory Access Control (MAC) in Linux systems. It requires one to define labels for files and applications along with a rule-based policy for decision-making. However, it also adds new knowledge to acquire. For example, it introduces not only the mechanism and labels, but also new concepts: SELinux users, SELinux roles, SELinux types and sensitivity levels. The evidence of a high complexity of SELinux can be found in a guide by Vermeulen [25], he starts one of the sections in the following way:

> "This is perhaps a weird section to begin with, but disabling SELinux is a commonly requested activity. Some vendors do not support their application running on a platform that has SELinux enabled. System administrators are generally reluctant to use security controls they do not understand or find too complex to maintain."

It is not a surprise that given so many new and partly repetitive concepts (consider *Users* and *SELinux users*), security administrators and policy developers face certain difficulties with learning the technology.

These examples provide us with the evidence that usability of a security mechanism is a complex problem. In accordance with the work of Reeder et al., where the authors investigate how the usability of access control depends on underlying mechanisms [19], we state that security should be made usable from the ground up. First, it should be possible to make security natural and to decrease the amount of newly introduced concepts and knowledge. Second, this principle should be applied at all architectural levels of a security system.

In this paper, we address the aforementioned considerations. We rely on evidence from cognitive science, and compare rule- and category-based access control mechanics. In section 2 we establish the parallels between access control and the evidence from cognitive science. In section 3, we compare two approaches by conducting a survey to assess the usability of two approaches. Section 4 provides an overview of the research on the usability in access control and user-centered security. In section 5, we discuss possible applications of the obtained results, limitations of our work, and a prominent future research direction.

2 Motivation

In this section we aim to establish the parallels between access control mechanisms and psychological theories that led us to the presented evaluation. First, we review the prominent access control models. Second, we introduce two related concepts from cognitive psychology on knowledge representation: categorization and schemata. Last, we formulate our research question and hypotheses.

2.1 Access control systems

We provide an overview of the four access control models: Mandatory access control (MAC), Role-based access control (RBAC), and Relationship-based access

control (ReBAC), and Attribute-based access control model (ABAC). Interestingly, they reveal a common underlying feature: they rely on mechanisms of categorization and on specification of rules.

Mandatory access control, or MAC, can be defined as a system that constrains a user according to a policy (MAC policy), defined by a system administrator. One of the MAC models is a system proposed by Bell and LaPadula [5]. The authors rely on the notions of security levels and formal categories. The model consists of a small number of fixed rules, for example, a person of a certain security level can read object from the same or lower levels, and write to objects from the same or higher levels ("no read-up, no write-down"). The formal categories, e.g. "NATO", "Nuclear", "Crypto", allow establishing the compartmentalization: a certain subject can read an object, if the subject's categories form a superset over the object's categories. The interesting detail about this model is that it relies on a small number of rules and heavily leverages categorization of subjects and objects.

The Role-based access control model, or RBAC, defines roles with a specific set of privileges and associates those roles with users [10]. This model fits well in organizational structures, where each employee has a role corresponding to her position. For instance, a company financial manager is associated with the "financial manager" role and has access to all financial reports of the company, at the same time, she does not have access to the company's legal reports if she is not assigned to the "lawyer" role. A distinctive feature of RBAC models is that they associate not only users with roles, making explicit categorization, but also roles with permissions. Thereby, RBAC models rely on categories for subjects (roles) and leverage a large number of specific rules (role-permissions assignments) for the roles.

The Relationship-based access control model (ReBAC), allows one to define access control policies based on relationships between users [6]. The mechanism is developed with the concept of Online Social Networks in mind. A data owner is considered to have a number of relations: friends, colleagues, neighbors. In this case, she can specify a policy that grants access to those who are, for instance, friends. ReBAC model relies on both categorization (an owner categorize someone as her friend) and rule assignment (e.g., friends and colleagues can read).

In the Attribute-based access control model, or ABAC, decisions are made based on the assigned attributes of the requester, assigned attributes of the object, environmental conditions and based on the policy that specifies rules for those attributes [26]. MAC and RBAC can be considered as special cases of ABAC. The most important benefits of the model are its flexibility and ability for dynamic decision making. Similar to MAC and RBAC, ABAC can be viewed as a model with a set of categories and policy rules for specifying access control.

2.2 Categorization in cognitive psychology

In cognitive psychology, it is often considered that human knowledge is stored in the brain in a form of concepts and categories [8]. *Concepts* can be thought as mental representations of objects. There are different ways of defining concepts.

We can do it, for example, by extracting a common feature for a set of objects within one concept. Another approach, a prototype view, is to represent concepts as a set of weighted attributes. In that case if an object has many relevant concept's attributes, it can be considered a typical exemplar of the concept.

Categories are considered to be a class of objects that belong together [8]. For example, if we speak about a smartphone and an armchair, we can categorize them as 'an electronic device' and 'a household furniture'. It is considered that categorization is a fundamental mechanism: it can be found in both human and animal brains [23].

A schema can be defined as a form of knowledge representation inside of a human brain, it can be described as "a structured cluster of concepts" [9]. Multiple schemas constitute schemata. It is believed that schemata are dynamic and based on previous experience of a human [4]. The described structure is also capable of accounting for the underlying patterns of human knowledge. In that case, a schema can also consist of variables or slots. The latter are filled with the appropriate concepts or sub-schemata to better represent a current situation.

Let us consider an example of schema:

can_put (what_to_put_slot, where_to_put_slot)

This schema models human knowledge of putting something somewhere. In particular situations, these slots can be filled in with concrete concepts:

can_put (book, table)

can_put (dress, wardrobe).

It should be also noted that each slot is restricted. For instance, in the previous example "what_to_put_slot" is restricted to movable concepts, for example, we cannot put our mood on the table in the literal sense.

Let us now consider a typical access control rule:

can_read (subject_label, object_label)

It is easy to see that this rule, allowing an application with *subject_label* to read a file with *object_label*, is very similar to a schema. Let us consider this example:

can_read (browser, photo).

In this rule we allow an application with label *browser* to read from a file with label *photo*. Given that schemata are built on the user's previous experience, we can say that this rule allows a user to transform a virtual system into the state in accordance with her view of the world. Thereby, if a user believes that a browser should not be able to read her photos, she can attach appropriate labels to the program and the images and then define the rule that would enforce this belief.

As we can see, there are notable similarities between the presented access control rule and the concept of schemata. Furthermore, cognitive science allows one to distinguish between different types of categories [13]. For example, a category *table* is considered to be of a feature-based type. The concept can be described with a set of features: *has legs*, *has a surface*. At the same time, a category of *reading* has a relational schema-based structure: there is always *reader* and *reading material*. Additionally, cognitive science provide us with a valuable input in the context of the usability: feature-based categories are easier

to acquire and retrieve than their schema-based counterparts [12]. With this evidence in hand, we can formulate our research question and hypotheses:

RQ: "How do rule-based and category-based mechanics affect the usability of an access control system?"

H1. A new system, which is relying on categorization, will lead to higher usability.
H2. Users of the category-based system will perform better in access control tasks.

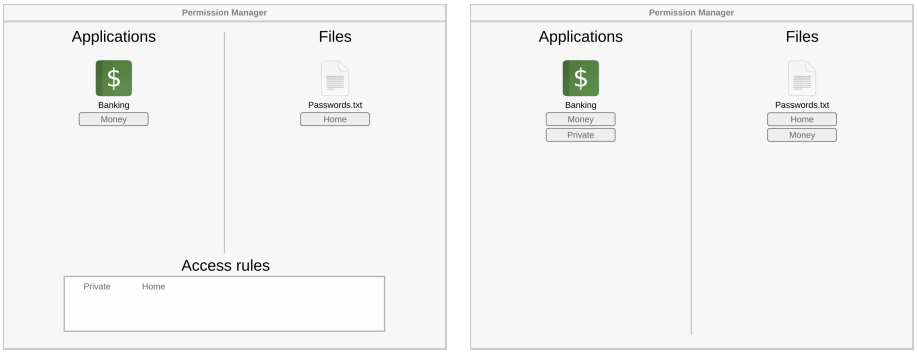
It should be noted that in this work we do not compare cognitive mechanisms. The presented evidence only allowed us to formulate hypotheses relevant to the field of the usability in access control systems, and the topic of cognitive mechanisms underlying security perception is future work.

3 Survey of rule- and category-based AC perception

The goal of the study is to evaluate two underlying cognitive mechanics in the context of access control. It is tempting to compare these mechanics via assessing the usability of the respective prototypes. Unfortunately, this approach would heavily lack internal validity: it would be hardly possible to associate the observed difference in usability with the introduced treatment. For instance, an interface of a rule-editor might significantly affect the results of a user study. Thereby, an artificial environment is required to measure the target effect.

In order to evaluate the influence of the two mechanics on the usability of access control systems, we designed two versions of a questionnaire (both versions are available in appendix A). The first one evaluates the cognitive load of the category-based approach, the second assesses the rule-based alternative. In the beginning of the questionnaire, respondents received an instruction. The latter represents an image with one application and two files. The version for assessing a rule-based approach also consists of labels and access control rules. A category-based alternative leverages only labels. For both versions, the example image represents a situation where access for the application will be granted for one file, and denied for another. An instructional text explains why a certain access control decision will be enforced. We were not able to find any existing questionnaires that connect access control and cognitive concepts, therefore, we designed our survey from the ground up.

Both of the questionnaires consist of two parts. In the first part, a user is asked to evaluate whether access is granted for a certain combination of categories/rules. An example of two question variants is shown on Figure 1. The second part of the questionnaire asks users to deny or grant access for certain combinations of applications and files. The tasks have identical textual questions in two versions. The first part is also designed to have the same answer options across the versions. After each question, users are asked to evaluate their perceived difficulty of the task. It is shown that the latter can be a good approximation of a system's usability [20]. We conclude the survey with the NASA-TLX



(a) Rule-based version (b) Category-based version

Fig. 1: Two variants of a question. The access will be denied in both cases.

questionnaire to assess the perceived task-load [14]. The survey was designed in accordance with the ethical principles outlined in the Menlo report [1].

Additional measures were implemented to balance the two versions of the questionnaire. First, since a human working memory is sensitive to amounts of information, we aimed to equalize either a number of shown categories and rules between two versions, or a number of category and rule pairs. For instance, when an application and a file have three different categories, a rule-based version operates on three different labels (see Figure 1). Second, we placed the 'Access rules' section in the same window together with applications and files. It was important for us to prevent the influence of users seeking a 'Access rules' section on the perceived usability of the mechanism. Lastly, we included an attention question, where users were asked to fill in certain values into the response fields.

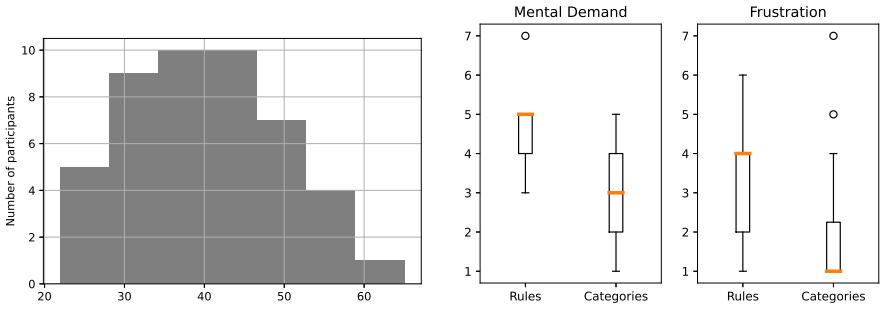
Survey results. The questionnaire was prepared in English and Russian versions. The link to the survey was distributed using a crowdsourcing website Toloka [1]. The top 10% of site users were chosen as possible respondents. A compensation for participation amounted to 1$. The links to the survey were distributed randomly among participants. We used a between-subjects design in our study.

After obtaining the results we performed data clearance. We declined responses that failed to provide the expected answer to the attention question. After this step we received 46 filled-in questionnaires, to which we will refer as 'all responses'. In addition, we perform two steps to empower further analysis. First, we distinguished entries that had mistakes in the first part of the survey. Thereby, we are able to more deeply analyze those responses that did not reveal misunderstanding of how the corresponding access control mechanism works. Second, for the purpose of a more reliable analysis in each group ('rule-based responses' and 'category-based responses'), we removed outliers with regard to

[1] https://toloka.ai/tolokers/

	Mistakes in assessing predefined sets	Mistakes only in adding new rules/labels	No mistakes	Total
Rule-based	14	7	3	24
Category-based	6	10	6	22

Table 1: Distribution of respondents among two conditions, and their performance.



(a) Age of participants.

(b) NASA-TLX constructs with significant difference.

Fig. 2: Age of participants and NASA-TLX responses for two subscales

the time taken to perform the survey. After this step, we received 9 rule-based and 16 category-based responses, suitable for cognitive load analysis. We have used all 46 responses for analyzing respondents' performance.

The gender distribution among all respondents was the following: 65% - male, 35% - female. The age distribution among participants is shown in Figure 2a. The countries of residence were reported as follows: Russia (40), Ukraine (2), Belarus (1), Uzbekistan (1), 2 respondents did not provide any answer. All participants completed the survey in Russian. In total, we obtained 24 respondents for the rule-based approach condition, and 22 for the category-based (see Table 1).

Our analysis of the survey results starts at assessing users' performance. As it was previously mentioned, the administered survey had two parts. The first part asked participants to choose whether an access will be granted for a certain combination of files, labels and rules. This set of questions aimed to determine whether a respondent understood how the presented mechanism works. The second part of the survey asked participants to use additional labels or rules to grant or deny access according to a given task. In Table 1, we provide results on user performance. The first column describes how many users make at least one mistake in the first part of the survey. Using Fisher's exact test, we have compared these numbers with those who did not make any mistakes in the first part. We found a significant difference in performance for two conditions ($p = .042$). In

other words, the proportion of successful respondents was higher in the category-based condition. We also compared the performance with regard to the time taken to complete the survey for the rule-based ($M(t) = 734.03, SD = 143.11$) and category-based ($M(t) = 656.39, SD = 121.97$) approaches. After establishing normality of both variables using the Shapiro-Wilk test ($p_{rb} = .68, p_{cb} = 0.39$), we performed the Welch's t-test and failed to reject the null-hypotheses of equal times spent on completing two versions ($t = 1.37, p = .19$). Thereby, users of a category-based version did not spend significantly less time on completing the survey. To summarize, given the difference in the respondents' performance in terms of success rate, we conclude that we have obtained a reasonable evidence to support hypothesis **H2**.

	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
Rule-based	2.00	2.00	1.00	2.00	1.00	2.00	3.00	3.00	3.00	4.00
Category-based	1.00	1.00	1.00	1.50	1.00	1.50	2.00	2.00	2.00	3.00
MWU test	.114	.244	.217	.388	.107	.334	.167	.034	.293	.065

Table 2: Participants' assessment of the ease of the tasks (median values). The question with a significantly different perceived ease of use is highlighted.

To assess hypothesis **H1** we evaluated results of each post-task mental load question together with NASA-TLX survey results. Even though, most of the medians of post-task question responses were lower for the category-based mechanism (see Table 2), we were able to reveal a significant difference only in one case. At the same time, there were two constructs in NASA-TLX post-survey questionnaire that differed significantly between two conditions (see Figure 2b). First, using the Mann-Whitney U test we found out that mental demand is significantly higher for the rule-based approach ($U = 24.5, p = .0062$). Second, the frustration effort is also significantly higher for the rule-based variant ($U = 39.0, p = .046$). We were not able to find any significant difference for other NASA-TLX constructs. To conclude, we state that there is enough evidence to support **H1** hypothesis.

4 Related work

In this section, we examine existing approaches to the usability in security and access control systems. We provide an overview of how existing works address the usability issues and apply user-centered approach in security systems.

One of the earliest works in user-centered security was produced by Zurko and Simon[30]. In this work they mention the Bell-LaPadula model as the model where "mathematical rigor was emphasized over usability". The authors note that models developed with the mathematical rigor in the first place might fail to emulate user intuitions or current practices.

Several works proposed to consider a user in established access control models. An attempt to improve usability of Multi-Level Security, or MLS, (a system that prevents unauthorized information disclosure among multiple information classes [21]) is done by Thorleuchter et al. [24] In their work, the authors try to increase the granularity of the model and, thus, to improve usability. Zhang et al. presume that role-based access control does not work in healthcare organizations, since doctors often have an unlimited access to patients' data, thus, breaking their privacy[29].

A significant number of works attempted to implement or evaluate user-centered security. Whitten and Tygar investigate the usability of encryption software [28]. Though they reveal design weaknesses, the authors also demonstrate that many respondents were able to understand that the image with keys is associated with encryption. The significance of the result lies in the area of metaphor perception. Since metaphors often serve as a method of teaching a user by referring to her knowledge in another domain [16], the authors show the efficacy of such images even in software with not-so-great design.

Human errors were found to be the most common reason for generating complex access control policies [22]. In this work, Smetters and Good investigate how users utilize access control. The authors also reveal that though complex policies are produced, they rarely need to be changed. It is also shown that users rely on the context rather than the content. In this situation a security policy of nearby objects is inherited. Another finding reveals that users make use of named access control groups. We believe that context-awareness and group-orientation represent the way humans think—they associate and categorize objects.

One of the ways to improve access control usability is to provide a form of feedback to a user. Anwar and Fong reveal that visual representation of access control policy allows users to perform better in policy analysis [2]. Other work by Anwar et al. also reveals a positive influence of visualization on cognitive load [3]. The helping role of visual metaphors for access control was investigated by Obrezkov et al [18].

Improving the representation of security information is not the only approach in the usability of access control. Cao and Iverson propose to use intentional access control systems, that would automatically decide how to achieve user goals, thus, mediating users' decisions [7]. Additionally, some works demonstrate how to build a usable access control system on a lower level. Reeder et al. show that the usability can be enhanced from the early stage of design [19]. Krishnan et al. propose a natural semantics to improve the usability of Access Control Lists [15].

5 Discussion

The most prominent outcome of this study is that a category-based access control mechanism exhibits higher usability than its rule-based alternative. We found out that task completion success rate and perceived mental load differ significantly for the two conditions.

Although our study revealed that a category-based approach is more usable in terms of performance and perceived mental load, there are a few limitations that should be considered. First, the gender distribution was not balanced. Though, we are not aware of whether gender affects the perception of access control, future studies might benefit from accounting for this factor. Second, there is a threat to internal validity of the study. From our observations one can see that respondents in the rule-based variant perceived not only a higher mental load but also a higher level of frustration. It is not possible to say whether a higher mental load led to higher frustration, or frustration from more tangled instructions (or tasks) led to a higher mental load. That being said, we should note that we tried to ensure high internal validity by designing similar questions and instructions for both experimental groups. Additionally, NASA-TLX Effort construct exposed no significant difference between conditions. Thereby, it is likely that respondents of the rule-based condition did not feel that they need to work harder to understand the instructions.

Our findings allow for new ways of the access control usability assessment. To demonstrate this, we consider two examples of widely used models: Bell-LaPadula and RBAC. We are going to review them in the light of our initial evidence on lower processing demands for categories rather than rules. Earlier, we showed that Bell-LaPadula model operates on levels, formal categories, and a few static rules (e.g., "no read-up; no write-down"). Levels and formal categories can be viewed as instances of categories, while the static rules as rules. Since the rules are static and their number is small, we can conclude that the MAC users rarely engage in more mentally demanding tasks of rules processing. In RBAC, the situation is different: both roles and permissions are dynamic. In that case, roles can be viewed as categories, and role-permission assignments as rules. For instance, if we have a role `manager`, and a resource group `reports`, the role `manager` can be viewed as a category, while the role-permission assignment "allow a `manager` to read `reports`" can be viewed as the following rule: `can_read(manager, reports)`. Though there is no restriction on the number of rules, RBAC exhibits one interesting feature: it effectively separates processing of categories and rules by introducing role-to-user and role-to-permission mappings. Thereby, the mentally intensive task of role-permission assignment can be delegated to security professionals, while the less intensive task of user-to-role mapping (e.g., assigning a new employee to the role `manager`) can be performed by general staff. It is easy to see that both Bell-LaPadula and RBAC utilize strategies to reduce mental load implied by rule processing.

The obtained results on the difference in perception of categories and rules allow us to formulate the following recommendation: **to design a more usable access control system, one should mitigate the mental load induced by access control rules.** The possible strategies include fixing a number of static rules (as in Bell-LaPadula model) and separating the tasks of categorization and rule creation (as in RBAC). For example, let us consider a distributed MLS system. In that case, security administrators might be provided only with a limited number of rules, while given a greater freedom in utilization of security labels.

Another example, is the case of Relationship-based access control (ReBAC) systems [11]. Those models allow one to create policies based on relationships between the owner and the requester (e.g., grant access for `friends` or `neighbors`). These relationships can also be viewed as categories [17]. Thereby, to increase the usability one can delegate the rule construction based on relationships to a third-party (e.g., to a security recommender system).

6 Conclusion

In this paper we investigated the usability of two access control mechanisms: based on rules and based on categories. The comparison of two approaches was performed by means of a questionnaire. Respondents were presented instruction windows, and then were asked to answer questions on access control. After each question they evaluated the perceived task load. The respondents also filled in a NASA-TLX questionnaire after the survey. Our analysis revealed that users of the category-based variant performed significantly better and claimed lower perceived mental load.

The results of our study can be used to improve the usability of existing access control systems. To achieve this, we recommended to consider the mental load induced by access control rules. We discussed how widely used systems address this problem and revealed two mitigation strategies. Given that our study produced only the initial evidence, we believe it would be beneficial to verify our findings in future experiments.

Acknowledgements. We would like to thank Karsten Sohr for careful reading of earlier versions of the paper. We would also like to thank the anonymous referees for their valuable feedback. This work was co-funded by the European Research Council for the project ScienceGRAPH (Grant agreement ID: 819536) and the German Ministry of Education and Research (BmBF) for the project KISSKI AI Service Center (01IS22093C).

References

1. The menlo report. IEEE Security & Privacy **10**(2), 71–75 (2012)
2. Anwar, M., Fong, P.W.: A visualization tool for evaluating access control policies in facebook-style social network systems. In: Proceedings of the 27th annual ACM Symposium on Applied Computing. pp. 1443–1450 (2012)
3. Anwar, M., Fong, P.W., Yang, X.D., Hamilton, H.: Visualizing privacy implications of access control policies in social network systems. In: Data privacy management and autonomous spontaneous security, pp. 106–120. Springer (2009)
4. Bartlett, F.C., Bartlett, F.C.: Remembering: A study in experimental and social psychology. Cambridge university press (1995)
5. Bell, D.E., La Padula, L.J.: Secure computer system: Unified exposition and multics interpretation. Tech. rep., MITRE CORP BEDFORD MA (1976)
6. Bruns, G., Fong, P.W., Siahaan, I., Huth, M.: Relationship-based access control: its expression and enforcement through hybrid logic. In: Proceedings of the second ACM conference on Data and Application Security and Privacy. pp. 117–124 (2012)

7. Cao, X., Iverson, L.: Intentional access management: Making access control usable for end-users. In: Proceedings of the second symposium on Usable privacy and security. pp. 20–31 (2006)
8. Eysenck, M.W., Brysbaert, M.: Fundamentals of cognition. Routledge (2018)
9. Eysenck, M.W., Keane, M.T.: Cognitive psychology: A student's handbook. Taylor & Francis (2005)
10. Ferraiolo, D.F., Barkley, J.F., Kuhn, D.R.: A role-based access control model and reference implementation within a corporate intranet. ACM Transactions on Information and System Security (TISSEC) **2**(1), 34–64 (1999)
11. Fong, P.W., Siahaan, I.: Relationship-based access control policies and their policy languages. In: Proceedings of the 16th ACM symposium on Access control models and technologies. pp. 51–60 (2011)
12. Gentner, D., Kurtz, K.J.: Relational categories. (2005)
13. Goldwater, M.B., Markman, A.B., Stilwell, C.H.: The empirical case for role-governed categories. Cognition **118**(3), 359–376 (2011)
14. Hart, S.G., Staveland, L.E.: Development of nasa-tlx (task load index): Results of empirical and theoretical research. In: Advances in psychology, vol. 52, pp. 139–183. Elsevier (1988)
15. Krishnan, V., Tripunitara, M.V., Chik, K., Bergstrom, T.: Relating declarative semantics and usability in access control. In: Proceedings of the Eighth Symposium on Usable Privacy and Security. pp. 1–13 (2012)
16. Neale, D.C., Carroll, J.M.: Chapter 20 - the role of metaphors in user interface design. In: Helander, M.G., Landauer, T.K., Prabhu, P.V. (eds.) Handbook of Human-Computer Interaction (Second Edition), pp. 441–462. North-Holland, Amsterdam, second edition edn. (1997)
17. Obrezkov, D., Sohr, K.: Ucat: The uniform categorization for access control. In: International Symposium on Foundations and Practice of Security. pp. 3–14. Springer (2023)
18. Obrezkov, D., Sohr, K., Malaka, R.: "Do metaphors influence the usability of access control?": A gamified survey. In: Proceedings of Mensch Und Computer 2022. p. 472–476. MuC '22, Association for Computing Machinery, New York, NY, USA (2022)
19. Reeder, R.W., Bauer, L., Cranor, L.F., Reiter, M.K., Vaniea, K.: More than skin deep: measuring effects of the underlying model on access-control system usability. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. pp. 2065–2074 (2011)
20. Sauro, J., Dumas, J.S.: Comparison of three one-question, post-task usability questionnaires. In: Proceedings of the SIGCHI conference on human factors in computing systems. pp. 1599–1608 (2009)
21. Saydjari, O.S.: Multilevel security: reprise. IEEE security & privacy **2**(5), 64–67 (2004)
22. Smetters, D.K., Good, N.: How users use access control. In: Proceedings of the 5th Symposium on Usable Privacy and Security. pp. 1–12 (2009)
23. Smith, J.D., Berg, M.E., Cook, R.G., Murphy, M.S., Crossley, M.J., Boomer, J., Spiering, B., Beran, M.J., Church, B.A., Ashby, F.G., et al.: Implicit and explicit categorization: A tale of four species. Neuroscience & Biobehavioral Reviews **36**(10), 2355–2369 (2012)
24. Thorleuchter, D., Van Den Poel, D.: High granular multi-level-security model for improved usability. In: 2011 International Conference on System science, Engineering design and Manufacturing informatization. vol. 1, pp. 191–194. IEEE (2011)

25. Vermeulen, S.: SELinux System Administration. Packt Publishing Ltd (2016)
26. Wang, L., Wijesekera, D., Jajodia, S.: A logic-based framework for attribute based access control. In: Proceedings of the 2004 ACM workshop on Formal methods in security engineering. pp. 45–55 (2004)
27. West, R.: The psychology of security. Communications of the ACM **51**(4), 34–40 (2008)
28. Whitten, A., Tygar, J.D.: Why johnny can't encrypt: A usability evaluation of pgp 5.0. In: USENIX security symposium. vol. 348, pp. 169–184 (1999)
29. Zhang, W., Li, H., Zhang, M., Lv, Z.: Privacy-aware risk-adaptive access control in health information systems using topic models. In: Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies. pp. 61–67 (2018)
30. Zurko, M.E., Simon, R.T.: User-centered security. In: Proceedings of the 1996 workshop on New security paradigms. pp. 27–33 (1996)

A Questionnaire template

Two variants of the questionnaire are presented. In each variant participants are shown a textual question, a slide with an access control window (see Figure 1), and answer options.

Demographic questions

1: Your age. **2**: Gender. **3**: Country of residence. **4**: What kind of device have you used for the task? [Desktop PC or laptop, Tablet, Mobile phone, Other].

A.1 Rule-based variant

Instruction:
textual part: An application has access to a file if: the file doesn't have a label; the file label matches the application label; there exists a rule that associates the application label with the file label. Example. The Weather application has the label 'Public'. The file Family photo.jpg has the label 'Home'. The file Vacation.jpg has the label 'Images'. The access rules are as follows: 'Public Home', 'Public Media'. There is a rule that allows applications with the 'Public' label to access files with the 'Home' label. Therefore, the Weather application will have access to the file Family Photo.jpg. But the application will be denied access to Vacation.jpg because there is no rule allowing applications with the 'Public' label to access files with the 'Images' label.
slide: Applications: Weather (label: Public); Files: Family photo.jpg (label: Home), Vacation.jpg (label: Images); Access rules: Public Home, Public Media.
First part (yes/no questions):
1: Will the Gallery application be granted access to the file Vacation.jpg?
slide: Applications: Gallery (label: Images); Files: Vacation.jpg (label: Images); Access rules: -.
2: Will the Player application be granted access to the file Sunset.jpg?
slide: Applications: Player (label: Media); Files: Sunset.jpg (label: Images); Access rules: -.
3: Will the Banking application be granted access to the file Invoice.pdf?
slide: Applications: Banking (label: Private); Files: Invoice.pdf (label: Home); Access rules: Private Home.
4: Will the Banking application be granted access to the file Passwords.txt?
slide: Applications: Banking (label: Money); Files: Passwords.txt (label: Home); Access rules: Private Home.
5: Will the Gallery application be granted access to the file Vacation.jpg?
slide: Applications: Gallery (label: Home); Files: Vacation.jpg (label: Images); Access rules: Family Audio, Family Media, Home Audio, Home Images.
6: Will the Browser application be granted access to the file Nature.jpg?
slide: Applications: Browser (label: Home); Files: Nature.jpg (label: Images); Access rules: Family Audio, Family Media, Home Audio, Home Storage.
Second part (grant/deny access questions):
7: Grant access to the Gallery application for the file Park.jpg.

slide: Applications: Gallery (label: -); Files: Park.jpg (label: Public); Access rules: -.
input fields: Gallery, Access rules.
8: Deny access for the Gallery application to the file Family photo.jpg.
slide: Applications: Gallery (label: Images); Files: Family photo.jpg (label: -); Access rules: -.
input fields: Family photo.jpg, Access rules.
Attention question: Attention question. Enter the word "horizon" in both input fields below.
slide: Applications: Gallery (label: Images); Files: Family photo.jpg (label: -); Access rules: -.
input fields: Family photo.jpg, Access rules.
9: Grant access for the Weather application to the file Park.jpg, deny access to the file Passwords.txt.
slide: Applications: Weather (label: Public); Files: Park.jpg (label: Private), Passwords.txt (label: Home); Access rules: -.
input fields: Access rules.
10: Grant access to the Gallery application for both files. Deny access for the Browser application to the file Family photo.jpg, grant access to the Browser application to the file Sunset.jpg.
slide: Applications: Gallery (label: -), Browser (label: -); Files: Family photo.jpg (label: Home), Sunset.jpg (label: Images); Access rules: -.
input fields: Gallery, Browser, Access rules.

A.2 Category-based variant

Instruction:
textual part: An application has access to a file if: the file doesn't have a label; the file label matches the application label; the application has all the labels of the file. Example. The Weather application has the labels 'Home', 'Public', 'Secret'. The file Family photo.jpg has the labels 'Home', 'Public'. The file Vacation.jpg has the label 'Home', 'Images', 'Public'. Example. Since the Weather application has all the labels of the file Family Photo.jpg, it will be granted access to it. But the application will be denied access to Vacation.jpg because the application does not have the Images label.
slide: Applications: Weather (labels: Home, Public, Secret); Files: Family photo.jpg (labels: Home, Public), Vacation.jpg (labels: Home, Images, Public).
First part (yes/no questions):
1: Will the Gallery application be granted access to the file Vacation.jpg?
slide: Applications: Gallery (labels: Images); Files: Vacation.jpg (labels: Images).
2: Will the Player application be granted access to the file Sunset.jpg?
slide: Applications: Player (labels: Media); Files: Sunset.jpg (labels: Images).
3: Will the Banking application be granted access to the file Invoice.pdf?
slide: Applications: Banking (labels: Private, Home); Files: Invoice.pdf (labels: Private, Home).
4: Will the Banking application be granted access to the file Passwords.txt?
slide: Applications: Banking (labels: Money, Private); Files: Passwords.txt (labels: Home, Money).
5: Will the Gallery application be granted access to the file Vacation.jpg?
slide: Applications: Gallery (labels: Family, Home, Images, Media); Files: Vacation.jpg (labels: Family, Home, Images, Media).
6: Will the Browser application be granted access to the file Nature.jpg?
slide: Applications: Browser (labels: Family, Home, Images, Media); Files: Nature.jpg (labels: Family, Home, Media, Storage).
Second part (grant/deny access questions):
7: Grant access to the Gallery application for the file Park.jpg.
slide: Applications: Gallery (labels: -); Files: Park.jpg (labels: Public).
input fields: Gallery, Park.jpg.
8: Deny access for the Gallery application to the file Family photo.jpg.
slide: Applications: Gallery (labels: Images); Files: Family photo.jpg (labels: -).
input fields: Gallery, Family photo.jpg.
Attention question: Attention question. Enter the word "horizon" in both input fields below.
slide: Applications: Gallery (labels: Images); Files: Family photo.jpg (labels: -).
input fields: Gallery, Family photo.jpg.
9: Grant access for the Weather application to the file Park.jpg, deny access to the file Passwords.txt.
slide: Applications: Weather (labels: Public); Files: Passwords.txt (labels: Private), Park.jpg (labels: Home).
input fields: Weather, Passwords.txt, Park.jpg.
10: Grant access to the Gallery application for both files. Deny access for the Browser application to the file Family photo.jpg, grant access to the Browser application to the file Sunset.jpg.
slide: Applications: Gallery (labels: -), Browser (labels: -); Files: Family photo.jpg (labels: Home), Sunset.jpg (labels: Images).
input fields: Gallery, Browser, Family photo.jpg, Sunset.jpg.