Poster: Helping users review and make sense of access policies in organizations

Pooya Jaferian
University of British Columbia
Vancouver, Canada
pooya@ece.ubc.ca

Hootan Rashtian
University of British Columbia
Vancouver, Canada
rhootan@ece.ubc.ca

Konstantin Beznosov
University of British Columbia
Vancouver, Canada
beznosov@ece.ubc.ca

1. INTRODUCTION

Understanding and authoring access control policies has been known as a challenging problem. Previous studies (e.g., [5]) show that understanding and changing implemented access policy is challenging for users. But the focus of those studies was on personal access control, where the data owner, policy maker, and policy implementer are the same person. But this problem has not been extensively studied in organizational context. In this paper, we address this problem by proposing and evaluating AuthzMap, a new user interface for sense making and reviewing implemented access policies or, in short *access review*.

Access review is an important IT security activity in organizations, where the managers make the access policy and security administrators implement it. The managers are mandated by many security regulations such as SOX, HIPAA, etc. to regularly review and validate the access privileges of users. On the other hand, access review for every 2,000 to 3,000 users consume one full-time-employee equivalent per year, and many organizations cannot even finish the process before a new campaign begins [1].

The overarching goal of this work is to improve technology support for access review. We performed two studies to understand and address the problem. In the first study, we explored the access review activity and identified its challenges through a series of semi-structured interviews. Based on the results of the first study, we modeled access review in the activity theory framework [3], and used activity theory guidelines to design a new user interface named AuthzMap. We then asked 12 usability experts to perform heuristic evaluation of the interfaces and compared the number and severity of the reported problems between three interfaces. Our results show that AuthzMap contained fewer problems than the two existing interfaces and improved the visibility of activity context.

2. UNDERSTANDING ACCESS REVIEW

Methodology: For understanding the problem, we conducted 11 semi-structured interviews with security practitioners involved in managing and reviewing access policy in large organizations. We analyzed the interview data using grounded theory methodology by performing open-coding, axial-coding, and selective coding.

Results: We use the triangle model of activity [3] to lay out our description of access review (Figure 1). We will later refer to this formulation when we justify our design decisions.

Description of the model: Access review is a human activity with the goal of verifying users' access rights to minimize the risk of unauthorized and unmanaged access. *"Reviewer"* is the main **subject** in the activity who performs access review. Our participants indicated that different stakeholders act as reviewers: (1) Managers act as reviewers by reviewing employees under their authority. (2) Application owners review the access of users who have access to their applications. (3) Security team review all employees' access. The **object** towards which the activity is performed is a user-to-role assignment. When managers or security admins perform access reviews, they review a set of roles assigned to a user (user access review). When application owners perform reviews, they review a set of users assigned to a role (application access review). The **division of work** between stakeholders is as follows: A member of security team requests review of users' access rights. The reviewer (a manager in most cases) receives the request. He goes through the list of users, and for each user-to-role assignment, he chooses to certify or revoke the assignment. The reviewer might contact the application owners, the user, or the security team when he is unable to determine the correct action. Different **rules and constraints impact access review**, including the security policy of the organization, seperation of duties, and the review deadline set by security team. The **artifacts** used during the access review include the information about the user, roles, and user-to-role assignments.

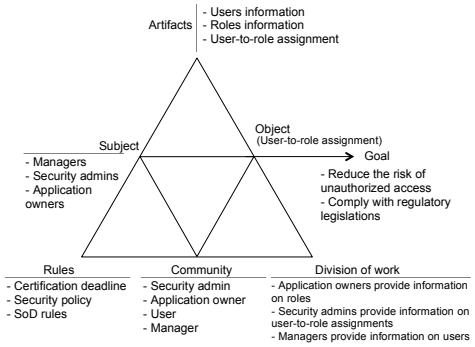

Figure 1: Overview of Access Review Activity

Challenges in the activity: We classified the challenges our participant mentioned during interviews into 5 categories: (1) Scale: access review can involve large number of users, roles, and permissions. (2) Lack of technical knowledge: managers do not have the technical expertise to understand the meaning of roles and permissions. (3) Frequency: reviewing access is not the main job of managers, yet they are frequently asked to perform this activity. (4) Human errors: The activity involves eye-balling large list of users and roles and is prone to human errors. (5) Exceptional cases: the validity of user-to-role assignments cannot be accurately determined by knowing the user's job function. Users might need to fill in another employee's role for a period of time, or they might need temporary access when they are on training.

3. AUTHZMAP DESIGN GOALS

Here, we present 3 design goals to address identified challenges:

Flexible support for review actions: In access review activity, reviewer performs following actions: viewing list of users and identifying them, identifying users' job function, checking the list of users' roles, and certifying or de-certifying user-to-role assignments. Furthermore, according to [3], technology should provide alternative ways of achieving the goal of activity. Therefore, we represent information at different levels of abstraction, so that users can choose the representation that best matches their goal. Also, we allow users to selectively automate repetitive actions such as certifying or de-certifying user-to-role assignments.

Visibility of context: Activity theory suggests that access to tools and materials necessary to perform actions should be provided to the user, and these material can be integrated with each other and presented in a way that reflects the spatial layout and temporal organization of the context [3]. The context of access review activity includes all the users, roles, and user-to-role assignments. In addition, the context includes: job function changes of the user, other users that need to be certified, previous reviews, and other users involved in the activity. Revealing the context can address the scale, frequency, and human error challenges.

Make history visible: Incorporating historical information can help reviewers make better decisions in uncertain and complex scenarios, and therefore addresses challenges with scale and exceptional cases. Our interviews revealed that users, and user-to-role assignments carry a history with them. On the other hand, roles are rarely changed. Therefore, AuthzMap visualizes the history of users' job changes, and the history of user-to-role assignments.

Knowledge sharing: According to [3], technology should help in problem articulation and seeking help form colleagues and collaborators. Therefore, we provide knowledge of each role for the reviewers in the form of role descriptions, and list of permissions. Moreover, communication channels should be available in the interface for reviewers to communicate with other users who have the knowledge of the roles and permissions. Realizing the knowledge sharing goals will address problems with complexity, lack of technical knowledge, and exceptional cases.

To realize these three goals, we designed a new interface and named it AuthzMap, and made an interactive version available at: http://bit.ly/authzmapinterface

4. COMPARATIVE EVALUATION

To check if the AuthzMap is an improvement over the existing interfaces, we compared it to two other access review tools (CA and Aveksa) in a heuristic evaluation within subjects study. We recruited 12 participants, and asked them to participate in a two hours study session. We first trained the participants on heuristic evaluation method. Then we asked them to spend 90 minutes (30 minutes per interface) for evaluation of three interfaces in the provided order (we counter-balanced the order of the interfaces) using 17 heuristics: 10 Nielsen's [4], and 7 ITSM [2]. Participants reported usability problems, and the heuristics they used for finding them. After the evaluation, we asked participants to review the reported problems and determine the severity of them.

Results: Table 1 shows the classification of the problems for each interface. The "Reports" column shows the initial number of problems reported by the evaluators. The "Valid" column shows the number of problems after: (1) removing those that we could not reproduce, and (2) decomposing reports containing multiple subproblems. The "Aggregate" column shows the number of problems after combining multiple instances of a single valid problem reported by multiple evaluators. Table 1 also shows the classification of aggregated problems based on their average severity (no problem was classified as "0" severity).

Table 1: **Overview of identified problems**

Interface	Reports	Valid	Aggregate	Severity			
				1-2	2-3	3-4	4
AuthzMap	55	55	32	5	14	12	1
Aveksa	83	83	37	2	18	14	3
CA	105	107	33	3	9	16	5

We also tested the following hypothesis to compare the number and severity of the problems in each interface: (1) H_1: Participants will report more problems for List and Search than AuthzMap. Using paired t-test shows that there is a statistically significant difference between AuthzMap and List ($t(11) = -2.74$, $p < 0.05$, $d = 0.76$), and AuthzMap and Search ($t(11) = -5.09$, $p < 0.05$, $d = 1.41$). (2) H_1: The average severity of the reported problems for the List and Search will be higher than AuthzMap. Using paired t-test shows that there is a significant difference between AuthzMap and Search ($t(11) = -4.03$, $p < 0.05$, $d = 1.23$).

To evaluate each interface based on the type and severity of the reported problems, we defined a usability metric that combines the number and severity of the reported problems (by one evaluator) using each heuristic. A high value of the metric for an interface shows that the evaluator reported large number of problems and/or severe problems related to that heuristic. We investigated the significant effect of the interface on the value of usability metric using Wilcoxon test. Here, we report the p-value and the effect size for statistically significant effects. Our analysis showed that AuthzMap's ratings were lower than Aveksa for heuristics: ITSM #1- *visibility of activity status* ($p < 0.05$, $r = 0.73$), Nielsen #2- *match between system and real world*) ($p < 0.05$, $r = 0.70$), and marginally ITSM #3- *flexible representation of information* ($p = 0.07$, $r = 0.53$). Furthermore, the AuthzMap ratings were significantly lower than CA for heuristics: ITSM #1 ($p < 0.05$, $r = 0.87$), ITSM #2- *history of actions on artifacts* ($p < 0.05$, $r = 0.70$), ITSM #3 ($p < 0.05$, $r = 0.74$), Nielsen #1- *visibility of system status* ($p < 0.05$, $r = 0.86$), and Nielsen #3- *user control and freedom* ($p < 0.05$, $r = 0.69$).

5. CONCLUSION

The results of our study showed that user-to-role assignments are the main artifacts that should be understood and manipulated during access review. But contextual information such as user's current and previous jobs, similar users' access privileges, and the results of previous reviews could influence how a user-to-role assignment is interpreted by the reviewer. Furthermore, our formative evaluation showed that two of the leading access review tools focus on the immediate artifact, and ignore the context. As other access management activities involve understanding of access policy, our results can be applied to them. These tools should take into account contextual artifacts, and make them accessible to users.

6. REFERENCES

[1] Cser, A. *THE FORRESTER WAVE™: ROLE MANAGEMENT AND ACCESS RECERTIFICATION, Q3 2011*. Technical report, Forrester Research, inc. (August 2011).

[2] Jaferian, P., Hawkey, K., Sotirakopoulos, A., Velez-Rojas, M., and Beznosov, K. Heuristics for evaluating it security management tools. In *SOUPS*. Pittsburgh, PA, USA, 2011, 1–20.

[3] Kaptelinin, V. and Nardi, B. *Acting with technology: Activity theory and interaction design*. MIT Press, 2006.

[4] Nielsen, J. and Molich, R. Heuristic evaluation of user interfaces. In *CHI*. ACM, New York, NY, USA, 1990, 249–256.

[5] Reeder, R. W., Bauer, L., Cranor, L. F., Reiter, M. K., Bacon, K., How, K., and Strong, H. Expandable grids for visualizing and authoring computer security policies. In *CHI*. ACM, New York, NY, USA, 2008, 1473–1482.