# Poster: Towards Improving Usability of Access Certification Interfaces

[Poster Abstract] *

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

Identity management (IdM) comprises the processes and infrastructure for the creation and maintenance of user's digital identities and the designation of who has access to resources, who grants that access, and how accountability and compliance are maintained. Identity management in organizations is done centrally using an enterprise identity management system (IdM system) or in a distributed fashion using different applications across the organization.

IdM involves various sub-activities including configuration and deployment, policy creation, identity creation, management of identity lifecycle, basic and advance provisioning and de-provisioning, audit, access certification, role engineering, and self-service [1]. In this poster, we focus on access certification. Access certification is an activity in which the assignments of permissions to users are reviewed in order to minimize the risk of unauthorized and unmanaged access. In this ongoing work, we studied access certification activity by conducting 10 semi-structured interviews with security practitioners and identified their needs and challenges during performing access certification. We then proposed a new user interface for supporting access certification activity, and plan to evaluate the usability of the interface using a multi-method approach.

## 2. METHODOLOGY

The goal of this research project is to identify challenges in performing access certification and improve current IdM technologies to address the identified challenges. In order to achieve the aforementioned goals, we have used the following methodology:

1. Understanding the problem: To further the understanding of the access certification activity we used two methods: (1) We performed 10 semi-structured interviews with security practitioners who had experience with identity and access management, and collected qualitative data. The data is later analyzed using grounded theory to build a model of access certification activity, and identify challenges in the activity. In addition to the interviews, we conducted a heuristic evaluation of one of the existing IdM technologies, and identified 10 problems related to access certification user interfaces (reported by 24 evaluators).

2. Prototyping: To address the identified challenges and problems, we designed a new user interface that visualizes the access profile of the user. We first designed a low fidelity paper prototype of the access profile, and after multiple rounds of refinements, built a high-fidelity prototype.

3. Confirmatory survey and refining the prototype: To refine the prototype, and strengthen and generalize the model of access certification activity, we designed an online survey. It is yet to be distributed in online communities of security practitioners (e.g., Linked-In). Our goal for conducting the survey is to test if the identified model of activity is valid, and to refine our proposed solution. Furthermore, we plan to use the collected data to design realistic scenarios for lab study of the proposed interface.

4. Evaluation of the proposed interface: We plan to evaluate the proposed interface using two different techniques: (1) We will perform a comparative heuristic evaluation of the proposed and existing interfaces and refine the proposed interface based on the result of the evaluation. (2) We plan to conduct a lab study of the proposed and two existing interfaces for access certification. We will compare the three interfaces in terms of efficiency, and accuracy of performing access certification. Furthermore, we will compare the three interfaces to see which interface leads to better assessment of a risk associated to assigning a permission to a user.

## 3. PROBLEM DESCRIPTION

Analyzing the interviews shows that one of the challenging activities in IdM is access certification. Access certification is done on a regular basis as the part of organization's policy (e.g., quarterly), or on an ad-hoc basis based on a request of a stakeholder or based on job changes of users. The interview data shows that the access certification is usually requested by security team and performed by the managers. In this activity, each manager is responsible for reviewing, and validating the permissions of employees under his or her management. The result of the validation of each permission is a "certify" or a "revoke" decision.

Our participants mentioned that managers have many challenges in performing access certification including: (1) the lack of understanding of the permissions, (2) lack of time to spend on certification, (3) size of certification data (i.e., large number of users, and permissions), (4) frequency of certifications, (5) exceptional cases, and (6) communication and negotiation required to perform certification.

Furthermore, during the heuristic evaluation, our participants reported many problems with the access certification user interface of the evaluated IdM system. Looking at the user interface of other access certification tools also showed that many of the reported problems might be commonly shared between the the existing user interfaces.

## 4. NEW ACCESS CERTIFICATION INTERFACE

To address the reported challenges with access certification, and based on the identified problems during the heuristic evaluation, we designed a new tool for access certification. The design is guided by the our previously proposed guidelines [2], and involved following design decisions:

- Showing the history of activities, including the history of user-permission assignments, job-function changes, and previous certifications.
- Revealing activity context, by correlating user-permission changes with job-changes of users, and previously performed certifications.
- Providing knowledge sharing by showing the meaning of each permission, and the reason why it is granted.
- Providing communication channels to allow managers seek help from other stakeholders like permission owners, and security administrators.
- Providing different cues to help managers evaluate the risk associated with user-permission assignments.

To realize the above decisions, we first built a low-fidelity paper prototype to get feedback from industrial sponsor of the project. Then we built an interim medium fidelity prototype and refined it through multiple rounds of internal feedback. We extended the medium-fidelity prototype to a high-fidelity prototype that can import the certification data (including users, permissions, and user-permission assignments) as XML files, and allow users to practice access certification. To compare the usability of the proposed tool with the available tools, we prototyped two of the existing top five access certification systems. We chose prototyping over using the actual systems to address lack of access to the executable version of one of the systems, to make the interfaces accessible remotely, and to provide three interfaces at the same level of fidelity. We plan to further refine the proposed interface by collecting data through an online survey. The prototype of the proposed interface, populated with synthetic data, is available online at: http://goo.gl/a7RRV

## 5. EVALUATION OF THE PROPOSED INTERFACE

We plan to evaluate the proposed interface using two different approaches:

**Heuristic evaluation:** We plan to use heuristic evaluation to find problems in the three representative prototypes and compare the number, severity, and root causes of the identified problems in the three interfaces. Such study will contribute to improvement of existing interfaces as well as the proposed interface. A combination of Nielsen's and ITSM heuristics [3] will be used for heuristic evaluation.

**Controlled laboratory study:** The goal of the controlled lab study is to answer the following questions: (1) is using the new interface leads to better awareness about different roles that a user posses, and better evaluation of correctness of user-role assignment?; (2) is using the new interface leads to more accurate certification?; and (3) is using the new interface leads to faster certification?

*Study overview:* To answer the above questions, we designed a between subjects study with three conditions: (a) Existing interface (CA), (b) Existing interface (Aveksa), and (c) Proposed interface. The study will consist of the following stages:

**Background** : This step involves activities to prepare participants for the study including: (1) collecting the participants' background information, (2) training on roles, permissions, and certification, (3) providing participants with the description of the role they are going to play; and (4) introducing the interface they are going to use and going through all the features of the interface. Then showing an example of one task to be performed on the interface.

**Experiment:** In this step, participants perform the study tasks.

**Feedback:** For the last step, we probe certain decisions that participants made during the study session.

*Study tasks:* Four tasks will be performed by the participants: (1) Basic task: certification of the permissions for certain number of employees. The permissions include those that the certifier can recognize. (2) History task: we simulate multiple certifications that happens over a period of time (e.g., in one year a manager needs to perform at least four certifications). We expect participants to focus on the changes in access profile since the last certification instead of going through the all permissions. (3) Details task: the goal of this task is to assess the use of permissions details to make certification decisions. (4) Evaluation task: The goal of this task is to test if the proposed interface leads to better situational awareness and evaluation of user-permissions assignments. We want to understand if users can employ the cues in the interface and assess the assignment of permissions to users that they do not have prior knowledge of. A user is presented with a series of access profiles. Then, the participants should rate on a five point Likert scale the risk associated with the possession of each permission.

In the first three tasks we measure and compare time to completion and number of mistakes between three conditions. For the fourth task we calculate the agreement between participants' ratings and researchers' ratings.

## 6. REFERENCES

[1] Jaferian, P., Botta, D., Hawkey, K., and Beznosov, K. A case study of enterprise identity management system adoption in an insurance organization. In *CHIMIT*. ACM, 2009, 46–55.

[2] Jaferian, P., Botta, D., Raja, F., Hawkey, K., and Beznosov, K. Guidelines for Designing IT Security Management Tools. In *CHIMIT*. ACM, 2008, 7:1–7:10.

[3] 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.