A Multi-method Approach for User-centered Design of Identity Management Systems

Pooya Jaferian, David Botta, Kirstie Hawkey, Konstantin Beznosov

University of British Columbia, Vancouver, Canada

{pooya,botta,hawkey,beznosov}@ece.ubc.ca

1. INTRODUCTION

Identity management (IdM) comprises the processes and infrastructure for the creation, maintenance, and use of digital identities [1]. This includes designating who has access to resources, who grants that access, and how accountability and compliance is maintained [3, 8, 4]. IdM has become an important aspect of IT security infrastructure in organizations, and some consider it to be the most important solution for enabling compliance [9]. To facilitate identity management, usable technological solutions are important. In this ongoing research, we plan to study the practice of identity management from a socio-technical point of view, and study how technology can improve IdM. Our final goal is to develop recommendations for user-centered design of IdM systems.

We've devised a multi-method approach to address this problem. To begin with, we performed a case study of IdM adoption and use in an insurance organization. The case study provides us with a high level understanding about the problem domain and directions for the rest of our research. We plan to continue our research in two phases: (1) evaluate the usability of an IdM system using heuristic evaluation, and (2) perform a field study to further our understanding about IdM practices and technologies, validate the results of our heuristic evaluation, and develop recommendations for user-centered design of IdM systems.

In this poster we present an overview of each phase of our ongoing research. At the time of writing, we finished the case study and developed a list of heuristics for heuristic evaluation of IT security tools. We plan to conduct a heuristic evaluation on an IdM system, and then a field study.

2. A CASE STUDY OF IDM DEPLOYMENT

We performed four semi-structured interviews with participants from the Security Administration (SA) group of an insurance organization. Also, we analyzed the organization's initial Request for Information and Qualification (RFIQ) document. The participants were involved in the selection and/or deployment of the IdM system. The interviews spanned more than two years, covering selection, and two phases of deployment, which enabled us to describe the state of the organization at different stages of identity management. We reported this work in detail in [6].

The insurance organization had about 2,500 employees – 2,000 of them in the head office, and the rest in branch offices. The central IT security group's responsibilities included developing policies, standards, and practices related to IT security, plus managing digital identities and computer-related access control. A vendor was contracted, and the IT security group operationalized phase one, which included self-service password recovery, and *basic* provisioning for commonly needed services like e-mail and connection to the Internet). Their "Data Guardianship Policy" (developed before the IdM project) specified that every resource had an owner (a data guardian), who was normally the manager of the business unit to which the resource belonged. Requests for access would be granted by the data guardian. SA would periodically provide training about policies and procedures for data guardians and data stewards (stand-ins for data guardians).

The basic workflow (before full deployment of an integrated IdM system) was: (1) Human resources creates an ID for a new employee. (2) Both the SA group and the employee's manager are automatically notified, while SA manually processes it. (3) SA provides basic permissions. (4) On behalf of the employee, the employee's manager requests SA (via electronic form) for access to the systems that are appropriate for that employee, including additional or temporary access. (5) A security administrator deploys the request to one or more data guardians, depending on whether the data is distributed . If the data was on an independent network, the security administrator forwards the request to the pertinent administrator, who could implement the access. (6) The data guardian might delegate the request to a data steward. (7) The security administrator performs a follow-up cycle, to handle non-response or lag from data guardians. (8) If the data guardian or data steward grants permission, the security administrator implements the access. (9) When an employee is terminated or their status changed, the employee's manager is responsible for notifying SA.

The challenges that motivated adoption an IdM system included: (1) lag between when a new employee begins work and when HR creates an ID, (2) insufficient knowledge to make requests or grant access, (3) failure to resolve issues and permission accumulation because of failure to follow up, or lack of accountability, (4) heterogeneity leading to complexity in troubleshooting, and (5) inappropriate delegation of authority.

An integrated IdM system was expected to address the challenges. Two milestones were a self-service password management system sub-system – phase one, to show benefits to end-users and obtain management support for the rest of the project – and phase two, role based access management. Deployment was complex, especially the creation of a complete and correct set of roles. Full deployment was expected to improve reporting, and to reduce security administrators' workload and free them to upgrade to security business analysts.

3. EVALUATION OF IDENTITY MANAGEMENT SYSTEMS

The usability of information technology (IT) security tools is hard to evaluate by regular methods. Laboratory experiments have validity issues with respect to the complexity of live security problems, and recruitment of IT security practitioners for interviews and observation can be difficult. Furthermore, IT security management (ITSM) is a complex and collaborative context that involves diverse stakeholders, and thereby the study of IT security tools, including IdM systems, inherits the difficulty of studying collaboration. Heuristic evaluation helps allay these difficulties.

But current heuristics do not explicitly address the characteristics of ITSM. That is, ITSM requires collaboration between diverse stakeholders, has an environment of numerous technological and business specializations (is complex), has many issues that need to be handled with discretion, is fast paced, uncertain, requires reliance of practitioners on tacit knowledge, and there is lack of immediate feedback when imposing a change on the system. Our case study shows that IdM shares many of these characteristics. Therefore, in order to evaluate the IdM systems, we adapted Nielsen's heuristics by selecting the ones that are relevant with respect to the ITSM context. We changed the focus of the selected heuristics to address complexity and stakeholder diversity in ITSM based on the guidelines for user-center design of ITSM tools [7]. To address the dimension of cooperation, these are then combined with Gutwin and Greenberg's [5] framework to articulate the mechanics of collaboration.

We plan to test our heuristics by applying them to an IdM system and compare their effectiveness to Nielsen's original heuristics by comparing the number and severity of usability issues identified by each method.

4. FIELD STUDY OF IDENTITY MANAGEMENT TECHNOLOGY AND PRACTICES

We plan to conduct a field study of identity management practices. Our methodological choice is to do a field study that includes interviews, and naturalistic observation of security practitioners in different stages of identity management. Our main challenge will be to gain the participation of organizations that have experience in the deployment and use of IdM systems. One strategy is to advertise to and through the professional contacts that were established by our previous research project (HOT Admin [2]), with the potential cost of not being able to study any one organization in depth, and another strategy is to develop a research partnership with an organization that has many contacts, but also has a vested self-interest, with the potential cost of not being generalizable.

The research focus in our field study will be on the challenges during different stages of identity management (deployment, configuration, and ongoing use), and on how stakeholders involved in identity management communicate and collaborate with each other. We will use a grounded theory approach to analyze the data. The data will be coded using open and axial coding techniques in parallel with our field study. This will allow us to choose further participants and questions based on emerging theory (theoretical sampling). Upon "saturation" (more investigation does not reveal new insights," we intend to model the challenges in communication and collaboration. The results will serve to validate and refine our heuristics (or falsify them). Finally, we will develop guidelines for improving IdM technologies.

5. CONCLUSIONS AND FUTURE WORK

In this paper, we give an overview on our ongoing study of IdM technologies and practices. We started our research with a case study of IdM adoption in an insurance organization. Our case study shows that IdM partakes of characteristics that are typical of the more general ITSM context, such as complexity, collaboration, and stakeholder diversity. Therefore, as a part of our research, we developed a set of heuristics for usability evaluation of ITSM tools. For future work, we plan to evaluate IdM systems with the heuristics. Additionally, we plan to conduct a comprehensive field study of IdM technologies and practices to further our understanding, validate and refine our heuristics, and develop guidelines specifically for the user-centered design of IdM systems.

6. REFERENCES

[1] D. Blum. Identity management - concepts and definitions. Technical report, Burton Group, September 2005.

[2] D. Botta, R. Werlinger, A. Gagné, K. Beznosov, L. Iverson, S. Fels, and B. Fisher. Towards understanding IT security professionals and their tools. In *Proc. of Symp. On Usable Privacy and Security (SOUPS)*, pages 100–111, Pittsburgh, PA, July 18-20 2007.

[3] C. Corporation. How can a comprehensive identity and access management solution help me reduce security risk and achieve easier compliance?, 2008.

[4] M. Corporation. Microsoft identity and access management series: Fundamental concepts, 2006.

[5] C. Gutwin and S. Greenberg. The mechanics of collaboration: developing low cost usabilityevaluation methods for shared workspaces. *IEEE 9th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 2000.(WET ICE 2000). Proeedings*, pages 98–103, 2000.

[6] P. Jaferian, D. Botta, K. Hawkey, and K. Beznosov. A case study of idm adoption in an insurance organization. *Submitted to LISA'09: 23rd Large Installation System Administration Conference*, 2009.

[7] P. Jaferian, D. Botta, F. Raja, K. Hawkey, and K. Beznosov. Guidelines for Designing IT Security Management Tools. In *CHIMIT '08: Proceedings of the 2008 symposium on Computer Human Interaction for the Management of Information Technology*, pages 7:1–7:10. ACM, 2008.

[8] S. Microsystems. Using identity management to achieve security and compliance, 2005.

[9] J. Wright. Final progress reports. Technical report, JISC, November 2007.