Usable Security Research in Technology Innovation Projects: A Case Study with Personas

Shamal Faily [a]
University of Oxford
Oxford, OX1 3QD, UK
shamal.faily@cs.ox.ac.uk

John Lyle
University of Oxford
Oxford, OX1 3QD, UK
john.lyle@cs.ox.ac.uk

Cesare Cameroni
Politecnico di Torino
10129 Torino, Italy
cesare.cameroni@polito.it

Ayşe Göker
AmbieSense Ltd / City University London
Aberdeen, AB15 4YD, UK
ayse@ambiesense.com

Ivan Fléchais
University of Oxford
Oxford, OX1 3QD, UK
ivan.flechais@cs.ox.ac.uk

Andrea Atzeni
Politecnico di Torino
10129 Torino, Italy
andrea.atzeni@poilto.it

Hans Myrhaug
AmbieSense Ltd
Aberdeen, AB15 4YD, UK
hans@ambiesense.com

Robert Kleinfeld
Fraunhofer FOKUS
10589 Berlin, Germany
robert.kleinfeld@fokus.fraunhofer.de

Abstract

Projects aiming to build technology innovations may encounter novel usable security challenges, but investigating these is secondary to a project's commercial or research goals. To answer this, we describe a case study for how personas can be used as a focal tool for getting engineers to undertake usable security research. This research aimed to understand how access control decisions are made in different contexts, as part of a large european technology research & development project. We show how this approach informed the design of context-sensitive access control policy editors, and discuss its implications.

Author Keywords

HCI-Security, Innovation, Personas, Affinity Diagram

ACM Classification Keywords

H.5.2 [User Interfaces]: User-centered design

General Terms

Design, Human Factors, Security

Introduction

Innovation is a key driving force behind many technology development projects. When faced with the explicit challenge of identifying and building new products,

[a] Primary contact

CHI'13, April 27 – May 2, 2013, Paris, France.
ACM 978-1-XXXX-XXXX-X/XX/XX.

processes or technologies, engineers will invariably encounter novel problems and situations. Our key area of interest is the potential for these projects to uncover new challenges in the usability of secure systems.

Addressing these challenges has two potential benefits: first we can improve the usability of the secure system being developed; second we can also gain useful insights and advance the broader field of usable security research. How can we undertake usable security research in technology innovation projects – where engineers focus on innovation rather than on the research?

Our approach makes use of personas as a focal tool for undertaking usable security research in *webinos*: a European Union (EU) funded research project. Personas are narrative descriptions of a system's archetypical users, embodying their needs and goals, and grounded in empirical data from representative users carrying out realistic activities [17]. Personas are useful when communicating user requirements, or justifying design decisions for interactive systems. For example, these can be incorporated into ideation activities such as feature brainstorming [17], where their voice might provide insight into any new ideas. However, if the activities of interest are sufficiently novel that no representative activity can be observed reliably, then building personas to explore specific insights is impossible without generalising the activities or making potentially unwarranted assumptions. Thus, while personas appear useful for exploring and communicating the security and privacy expectations of users, there has been little research in exploring how they can be used for novel modes of interaction.

In this paper, we describe how software engineers from various *webinos* project partners elicited and analysed data to understand how access control decisions were made in different contexts of use, and used this knowledge to inform the design of a context-sensitive access control policy editor. We start by outlining the design problem that motivated our approach, then we briefly review related work in design research, innovation, and HCI-Security. We then describe our approach, and how it was used to elicit these factors and their design implications. We conclude by discussing the implications of our approach for research and innovation.

Design problem

Personal information about ourselves is no longer locked to specific locations, where access control can be succinctly and formally described. Instead, personal information is distributed across a variety of personal devices: mobile phones, tablets, and even home media systems. Because our relationship with these technologies is still maturing, many questions remain unanswered about how access control policy tools for these federations of devices should be built, especially given the varying contexts within which these devices are used.

Access control policy editors

Improving the usability of access control policy editors for both developers and users has been a popular line of HCI-Security research in recent years, e.g. [18, 9]. While past work has cast light on some of the challenges in using and developing policy management tools, using these to supplement pervasive software applications leads to three new problems.

First, many policy tools have been implicitly designed with specific application domains in mind, such as healthcare [8] and e-Science [1]; in these cases, a certain degree of compliance with organisational norms can be expected. However, when people use software for personal use, the values and norms influencing policy decisions may be shaped around personal freedom rather than information security compliance.

Second, our access control decisions are influenced not only by the objects and different (human or machine) subjects, but also by their contexts. Moreover, people may make access control decisions in a physical or social context which is different from the context where the decision is enforced. For example, a person might install a mobile app with permissions to access location data from home, but not use the app itself until he is somewhere else.

Third, presenting the ability to react to all variables in a context leads to complexity overload. Too many or too few options may lead to habituation, and such habituation can lead to less useful policy settings.

These problems suggest that, when designing policy editors, we need to understand how security and privacy expectations are shaped in situations where the system is used. However, because the editors are part of a larger system, we need to capture these expectations with respect to the larger system that the editors support. Unfortunately, because the research necessary to better understand this is not a primary goal when building a system, research activities are likely to be sacrificed in the face of competing pressures. There is, however, increasing evidence that, if properly integrated with opportunities for engineers, interaction design techniques can both inform broad design activities and address ill-defined, non-trivial research problems [21].

The webinos project

Our design problem arose in the *webinos* project: an EU funded project to build a software infrastructure (*webinos*) for running web apps across different device platforms [6]. The project team was drawn from 24 organisations across Europe, including universities, network providers, handset and car manufacturers, mobile software houses and market analysts. *webinos*' software architecture includes policy management components for facilitating cross-device access control [12]. The use cases upon which these components were based describe the flow of data between end users and system components, but these are generic and framed in terms of whether or not users can access device features via applications running on different devices.

As part of the project, a collection of personas was developed to provide a voice for archetypical users and developers impacted by *webinos*. While useful for envisaging perceptions that users and developers might have about *webinos*, it was still unclear how their expectations about access control might change in line with subtle changes in physical or social contexts within which *webinos*-enabled apps might be used. Without knowing these expectations, it would be difficult to formatively evaluate tools for creating and managing context-sensitive access control policies. When it became apparent that team members had difficulty even envisaging user interfaces for context-sensitive policy management, we decided to explore the impact of the concept of *context* on *webinos* policy specification and management.

A lack of time and resources meant that experienced researchers within the project could not undertake any research activities without help. This made it necessary to involve engineers in the research activities, albeit those that had assisted in the creation of the personas. Based on their experiences creating these personas, we were concerned about the danger of techniques they didn't understand (or appreciate) being misappropriated. For example, associated with each persona was an argumentation model that grounded the data used to create it; these were designed to help team members better understand how persona characteristics were derived [5]. Unfortunately, rather than using these models to decrease stereotypical assumptions, some engineers first wrote persona narratives and used these models to motivate assumptions they made about their descriptions; this effectively bypassed the data elicitation and analysis processes altogether.

Another concern related to language barriers we might face when carrying out research. Everyone on the project team spoke excellent English but, for the research to be meaningful, representative subjects from across the EU would need to be recruited; there was no guarantee these subjects would be comfortable engaging with researchers in any language other than their native tongue.

Related work

Research and Innovation

Many published studies provide accounts of research carried out to investigate specific research questions, or broad themes of interest that are independent of any particular design intervention. However, if we assume that a system's access control policy editor is designed to support that system's access control mechanisms, then any study should be carried out with respect this larger system's design.

Zimmerman et al.'s framework of interaction [21] proposes a model for carrying out design research for "wicked", ill-defined problems. This framework seems reasonable for building *innovative* products, but may be insufficient for tackling research carried out while building technology *innovations* for several reasons. First, research into *true* models and theories may be carried out of the necessity to generate the *how* knowledge necessary for progressing a technology's innovation. Such research may need to be concluded in a matter of days or weeks, rather than longer periods researchers may prefer. Second, we cannot rely on the presence of anthropologists and behavioural scientists when carrying out research, making it necessary to rely on design research techniques that can be quickly adopted by engineers. Third, the role of engineers in innovation may not be as simple as developing or revising specifications for technology opportunities based on an articulated invention. By drawing on these ideas and their expertise to situate the invention within the broader socio-technical system, engineers are fulfilling the role of entrepreneurs rather than simply inventors or software architects. The most prominent difference between these role is that, while engineers are system-centered, and their designs a realisations of a system's goals, entrepreneurs are opportunity centered, and their architectures fit into a broader innovation strategy [4]. This distinction is important: while software architectural design is concerned with shaping an architecture to fit a socio-technical environment, innovation is equally concerned with shaping the socio-technical environment around the architecture.

The priority of innovation over design qualities is evident when considering the role usability engineering has played in a number of recent security and privacy research projects. For example, the EU funded PrimeLife project [16] demonstrated how privacy technologies can enable people to control their on-line personal information based on their legal rights. Based on their experience in developing a number of Privacy Enhancing Technology

(PET) exemplar applications, the project identified several useful heuristics and idioms when designing and evaluating user interfaces for PETs. Usability researchers played an important role in evaluating PrimeLife, but there is less evidence of their influence in the design of the exemplars themselves. For example, several personas were created during the project to guide design decisions. However, in an example of privacy in social software [2], one of the personas is used only to illustrate access control policies in web forums rather than describing how it influenced the design decisions. While it is possible that the personas were used to inform architectural and application design, how this was carried out was not reported.

Usable Authorization

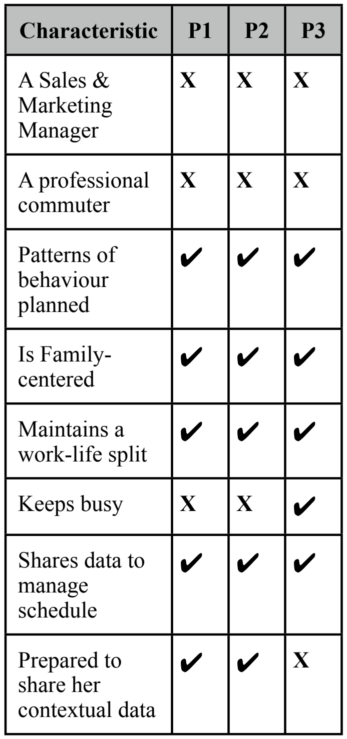
In recent years, the HCI-Security community has taken a keen interest in closing what Norman [14] describes as the *gulf of execution* between the intentions of users, and the system's means of implementing them. Studies into enterprise policy management tools have gone some way towards closing this gap. For example, work by Reeder et al. [19] identified several general policy authoring challenges that need to be addressed by tool developers; these include enforcing consistent use of terminology, making the concept of default rules and their rationale clearer, and facilitating the grouping of objects.

Past research has highlighted the difficulties people face creating a priori specifications of access control policies. The problems people have found devising categories of objects that remain useful when making policy decisions [9] mirror the results of earlier work by Lederer et al. on evaluating privacy preference tools [11]. Because they need to understand the privacy implications of situated use, Lederer et al. argue that users prefer to carry out actions with imperfect default settings, rather than semi-intuitively configuring data on an a priori basis. The notion that people will work off a general access control policy and vary this by different contexts was also identified by Smetters and Good [20].

Much of this related work is framed from the perspective of the solution space of policy editors, rather than the *problem space* of how people make access control decisions in their day-to-day lives. By looking at how people are making such decisions can provide insights guiding the creation or selection of appropriate design models for policy editing. A recent study about how people think about controlling digital content at home [13] suggest that people would, given the opportunity, vary access control policies across people and household. Other experimental studies [10] found tagging personal photos with descriptive text, such as keywords or captions, can help users to create intuitive and accurate coarse- and fine- grained access control rules.

Our Approach

To understand how representative users would experience access control decisions across multiple devices and contexts, engineers across *webinos* ran nine persona-based participatory design workshops; each workshop was situated around the characteristics and activities of a particular persona. Following discussions within the project team, we were interested in three particular representative users. The first of these was a web application developer (Jimmy). *webinos* would not be successful if developers did not adopt it, so their stake in access control decisions would be critical. The second persona (Clara) represented younger, teenaged users, because we felt such users were more likely to adopt new technology. The final person represented the parent of a young child (Helen); this persona represented users that



Characteristic	P1	P2	P3
A Sales & Marketing Manager	X	X	X
A professional commuter	X	X	X
Patterns of behaviour planned	✔	✔	✔
Is Family-centered	✔	✔	✔
Maintains a work-life split	✔	✔	✔
Keeps busy	X	X	✔
Shares data to manage schedule	✔	✔	✔
Prepared to share her contextual data	✔	✔	X

Figure 1: Table summarising the characteristic match between a workshop's participants and its related persona (Helen)

had made lifestyle choices making them sensitive to security & privacy concerns. For each workshop, participants were recruited based on how closely they matched the characteristics of the three different personas, and workshop facilitators summarised this information using a simple template, as illustrated in Figure 1.

Participants were presented with a scenario meaningful to them, and asked to elicit and categorise types of data that would need to be subject to access control. For example, Helen workshops were structured around making decisions about the security and privacy implications of a networked in-car entertainment system being used by her young son while on a long car journey to see her parents.

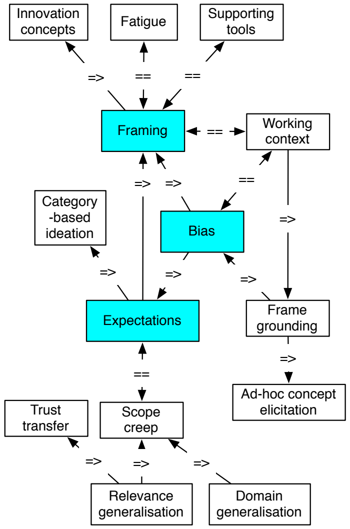
Each workshop involved 3-4 participants, and lasted approximately 1.5 hours. The participatory design activity revolved around an affinity diagramming exercise that followed a specific structure. After introducing the scenario and providing a brief overview of affinity diagramming, each session was divided into three stages. In the first stage (object clustering), participants spent 20 minutes eliciting data objects that would be subject to access control, writing these on post-it notes, and affixing the notes to a wall or whiteboard; these object post-it notes were then grouped under categories the participants found useful for making access control decisions. In the second stage (subject clustering), participants were required to elicit types of people (subjects) that should or should not have access to the objects elicited in the first stage. The participants then re-categorised the objects depending on what each subject should be allowed or denied access to; this stage took 30 minutes. After a 10 minute break, participants spent 20 minutes on the third and final stage. This involved identifying different contexts associated with the scenario and, for selected subjects, repeating the subject clustering stage based on the specific context. Following the third stage, the participants walked through the affinity diagrams created, after which a short debrief session was held to find out how the participants found the exercise.

Audio and visual data was captured for each workshop. Following each workshop, the workshop organiser prepared a short report summarising the event's outcome and the main themes emerging from the affinity diagrams and the associated discussions.

We devised this approach because team members were already familiar with affinity diagramming from their previous work developing personas. This previous work also helped them recruit suitable participants, based on the workshops they were organising. Because the experiments were concerned with the subjects' behaviour rather than the affinity diagrams themselves, both the scenarios could be explained and sessions run in the local language, as only the session report needed to be written in English. The report structure guided participants towards the sort of observations that needed to be made, and subsequent telephone conferences helped validate the research being carried out because it gave team members an opportunity to present and discuss their results.

Results

Once all the sessions had been completed, the workshop reports and transcripts were subject to a Grounded Theory analysis [3]. Following open and axial coding, 14 refined thematic concepts were identified. On investigating the relationships between these concepts and their grounding in the empirical data, we identified three factors that influenced the elicitation and categorisation of context-sensitive access control policies: *framing*, *bias*,



Relationship Symbol	Description
=>	Implies
==	Equivalent

Figure 2: Conceptual model of factors influencing the elicitation and categorisation of context-sensitive access control policies

and *expectations*. Each of these factors, and the concepts associated with it, are described in more detail in the following sections. The factors, and their associated concepts are summarised in Figure 2.

Framing
Although not formally acknowledged by the participants, each workshop appeared to elicit and categorise data within the frame of a working context.

The ability of participants to frame data was mediated by three factors. The first of these were the nuances in the working context; these range from varying the time-frame of a working context through to changing the family relationship of subjects in a context. Exploring these shed new light on pre-existing objects, but also led to considerable discussion, slowing down the rate of progress. The second factor was general fatigue. Framing and re-framing objects and categories within a working context was both tiring and time-consuming. In some cases, a rigorous exploration of objects and subjects in the working context left participants so tired that contexts were specified around pre-existing subjects or locations closely related to that associated with the working context. The third factor was the use of supporting tools - in particular sketches and check-lists. Sketches were used in one workshop as a supplement to the context clustering affinity diagramming to explain particular subtleties of a context. Mental checklists were in a number of workshops to check the relevance of concepts, or validate a concept's inclusion under a particular category.

Although primarily used for concept elicitation and categorisation, framing was also useful for identifying concepts and categories forming the basis of innovation within the general domain. Examples included the elicitation of commercialisation and regulatory concepts that might foster improved security and privacy.

Bias
The ability of participants to frame concepts and categories was influenced by pre-existing biases. In some cases, biases led to restrictive thinking about concepts because of pre-existing domain knowledge. This was most obvious in the Jimmy workshops, which centred on specifying policies for a training course website. Pre-existing knowledge about how courseware was used, or assumptions about how hardware was setup appeared to unnecessarily dismiss objects as disallowed to particular subjects and context. Pre-existing biases were most evident when considering the implicit working context during object and subject clustering. Sometimes, these biases were re-enforced by participants when discussions were grounded around a particular frame; these frames were based on anecdotal experiences of the working context or when prompted by the facilitating workshop organiser.

As well as restricting thinking, biases and grounding also facilitated the elicitation of concepts which might otherwise have been missed. In almost all workshops, grounded discussions around particular working concepts led to the identification of concepts which were missed during the initial context free object clustering stage.

Expectations
The ability to frame concepts was also influenced by expectations held about the behaviour of particular subjects. Some of these were formed by pre-existing biases because participants felt they were proxy users for subjects under discussion. In others, participants espoused opinions they believed subjects might find important, irrespective of whether *they* found it important. For example, in one of the Clara workshops, participants

proposed Digital Rights Management restrictions that they felt content providers would find useful. In some workshops, participants felt confident enough in their knowledge of subject expectations that concepts would be moved between allowed and denied sections of the white board or wall by category and, in some cases, categories would be elicited before concepts, and subsequent concepts grouped by static, pre-existing categories.

Expectations were important for envisaging the impact of policy decisions but, in certain cases, this also led to scope creep when participant knowledge of subjects or the domain appeared to be deficient. One of the factors contributing to scope creep was generalisation about the problem domain; this arose due to lack of knowledge or only a superficial treatment of concepts. The other contributing factor was generalisation due to perceived lack of relevance. Examples of this included collectively grouping "interface" or "service" technology because they seemed equally relevant to all subjects and contexts, and generalisation categories for concepts that were disallowed for particular subjects and contexts. In some cases, relevance generalisation led to an implicit transfer of trust onto objects or subjects related to generalised objects or categories. For example, "administrator" subjects were, in some cases, given untethered access to concepts. Similarly, in one workshop, participants considered a context where a "secure" terminal might be used by an administrator in an untrusted location.

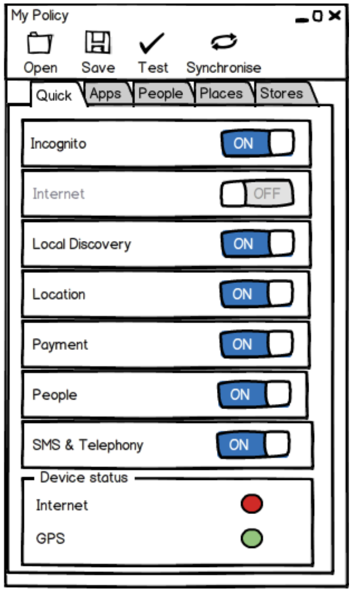
Design Implications

We believe these factors have three implications for the design of context-sensitive access control policy management tools.

First, we believe the order in which policies are developed should be reversed. While the workshops were designed to initially stimulate thinking about objects which needed to be secured, framing them with a working context meant that context could not be divorced from the policy specification processes. For this reason, it may be more fruitful to begin the process by eliciting contexts of use before objects within them, or subjects that use them.

Second, security policy development should be broken down into a discrete set of operations. The workshop results suggest that policies are sufficiently difficult to develop that both users and developers are prepared to surrender control of the non-periodic process of creating them. Previous work has suggested that the use of wizards may be appropriate for guiding users through the process of policy design [7], but it is not yet clear whether subjects or objects should immediately follow from context in the wizard sequence. Moreover, because an appropriate set of defaults needs to be incorporated into each policy, some burden is added to policy developers to specify reasonable settings based on the application, the problem domain, and the expected user base. This rationale also needs to be communicated clearly and transparently to users.

Finally, additional tools are needed not only for editing policies, but also for creating supplemental information. The workshop results showed that techniques such as sketches and checklists were useful. Previous work in the HCI-Security literature has also found that, if supplemented with contextual information about policy rules, matrices improve speed and accuracy when viewing and changing policies over traditional policy management tools [18]. Based on both the literature and the workshop results, subject/object matrix controls for editing access control policies should support supplemental information to allow policy editors to reconstruct the frame used by policy developers when creating the additional policy. This



Incognito ON
Internet OFF
Local Discovery ON
Location ON
Payment ON
People ON
SMS & Telephony ON
Device status
Internet 🔴
GPS 🟢

Figure 3: Coarse-grained access control settings panel. The settings were based on types of category elicited during the workshops

supplemental information may include multi-dimension matrix cells such as [18], or additional controls to allow the attachment of image files or design rationale.

Conclusion

In this paper, we have shown how personas can be used as both a design technique, and a basis for carrying out usable security research while situating a technology innovation. In applying our approach, we elicited three factors influencing the elicitation and categorisation of context-sensitive security and privacy policies. Rather than viewing our study through the lens of a specific tool, and drawing from a random user sample to carry out a general policy authoring scenario, we have instead used participatory workshops to understand the experiences associated with policy decisions. We have also based our approach around scenarios that were specific to the demographics of the participants engaged in these workshops.

To provoke further discussion around design research for innovation, we conclude with two broad implications of this study. First, our approach highlights the value of intermediate design artifacts, such as affinity diagrams. For example, when prototyping possible interfaces for an access control policy editor, we wanted to create coarse-grained access control settings, such as that shown in Figure 3. When considering what the coarse-grained items should be, we used the categories of objects elicited in the affinity diagrams created in the workshops. This secondary use of design data suggests the value such research can have given the increasing prominence placed on research where agility and lightweight techniques are encouraged, and where collaborating engineers are encouraged to *fake* process and focus on a final product [15]. Second, rather than simply the recipients of deliverables from interaction designs suggested by [21], engineers can also become engaged in the elicitation of field data, and participate in the creation of models and theory. As research and innovation activities merge in many design interventions, we need more ways of empowering engineers as both designers and innovators.

Acknowledgements

The research described in this paper was funded by the EU FP7 *webinos* project (FP7-ICT-2009-05 Objective 1.2).

References

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

[2] Camenisch, J., Fischer-Hübner, S., Rannenberg, K. *Privacy and identity management for life*. Springer, 2011.

[3] Corbin, J. M., Strauss, A. L. *Basics of qualitative research : techniques and procedures for developing grounded theory*, 3rd ed. Sage Publications, Inc., 2008.

[4] Faily, S., Fléchais, I. To boldly go where invention isn't secure: applying Security Entrepreneurship to secure systems design. *Proceedings of the 2010 New Security Paradigms Workshop* (2010), ACM, 73–84.

[5] Faily, S., Fléchais, I. Persona cases: a technique for grounding personas. *Proceedings of the SIGCHI conference on Human factors in computing systems* (2011), ACM, 2267–2270.

[6] Fuhrhop, C., Lyle, J., Faily, S. The webinos project. *Proceedings of the 21st international conference companion on World Wide Web* (New York, NY, USA, 2012), WWW '12 Companion, ACM, 259–262.

[7] Inglesant, P., Sasse, M. A., Chadwick, D., Shi, L. L. Expressions of expertness: the virtuous circle of natural language for access control policy specification. *Proceedings of the 4th symposium on Usable privacy and security* (2008), SOUPS '08, ACM, 77–88.

[8] Karat, J., Karat, C.-M., Bertino, E., Li, N., Ni, Q., Brodie, C., Lobo, J., Calo, S. B., Cranor, L. F., Kumaraguru, P., Reeder, R. W. Policy framework for security and privacy management. *IBM Journal of Research and Development 53*, 2 (2009), 4:1 –4:14.

[9] Kelley, P. G., Brewer, R., Mayer, Y., Cranor, L. F., Sadeh, N. An investigation into facebook friend grouping. *Proceedings of the 13th IFIP TC 13 international conference on Human-computer interaction - Volume Part III* (2011), INTERACT'11, Springer-Verlag, 216–233.

[10] Klemperer, P., Liang, Y., Mazurek, M., Sleeper, M., Ur, B., Bauer, L., Cranor, L. F., Gupta, N., Reiter, M. Tag, you can see it!: using tags for access control in photo sharing. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (2012), ACM, 377–386.

[11] Lederer, S., Hong, I., Dey, K., Landay, A. Personal privacy through understanding and action: five pitfalls for designers. *Personal Ubiquitous Comput. 8* (November 2004), 440–454.

[12] Lyle, J., Monteleone, S., Faily, S., Patti, D., Ricciato, F. Cross-plaform access control for mobile web applications. *Policies for Distributed Systems and Networks (POLICY), 2012 IEEE International Symposium on* (2012), 37–44.

[13] Mazurek, M. L., Arsenault, J. P., Bresee, J., Gupta, N., Ion, I., Johns, C., Lee, D., Liang, Y., Olsen, J., Salmon, B., Shay, R., Vaniea, K., Bauer, L., Cranor, L. F., Ganger, G. R., Reiter, M. K. Access control for home data sharing: Attitudes, needs and practices. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (2010), ACM, 645–654.

[14] Norman, D. A. *The design of everyday things*, 1st ed. Basic Books, New York, 1988.

[15] Parnas, D. L., Clements, P. C. A rational design process: How and why to fake it. *IEEE Transactions on Software Engineering 12*, 2 (1986), 251–257.

[16] PrimeLife Consortium. PrimeLife website. http://www.primelife.eu, November 2011.

[17] Pruitt, J., Adlin, T. *The persona lifecycle: keeping people in mind throughout product design*. Elsevier, 2006.

[18] Reeder, R. W. *Expandable Grids: A user interface visualization technique and a policy semantics to support fast, accurate security and privacy policy authoring*. PhD thesis, Carnegie Mellon University, 2008.

[19] Reeder, R. W., Karat, C.-M., Karat, J., Brodie, C. Usability challenges in security and privacy policy-authoring interfaces. *Proceedings of the 11th IFIP TC 13 international conference on Human-computer interaction - Volume Part II* (Berlin, Heidelberg, 2007), INTERACT'07, Springer-Verlag, 141–155.

[20] Smetters, D. K., Good, N. How users use access control. *Proceedings of the 5th Symposium on Usable Privacy and Security* (2009), SOUPS '09, ACM, 15:1–15:12.

[21] Zimmerman, J., Forlizzi, J., Evenson, S. Research through design as a method for interaction design research in HCI. *Proceedings of the SIGCHI conference on Human factors in computing systems* (2007), ACM, 493–502.