# While working around security

Niels Raabjerg Mathiasen
Aarhus University
Aabogade 34
DK-8200 Aarhus C, Denmark
+45 8942 5697
nielsm@cs.au.dk

Marianne Graves Pedersen
Aarhus University
Aabogade 34
DK-8200 Aarhus C, Denmark
+45 8942 5639
mgraves@cs.au.dk

Susanne Bødker
Aarhus University
Aabogade 34
DK-8200 Aarhus C, Denmark
+45 8942 5630
bodker@cs.au.dk

## ABSTRACT
The title of this paper describes our work at two levels. First of all the paper discusses how users of IT deal with issues of IT security in their everyday life. Secondly, we discuss how the kind of understanding of IT security that comes out of careful analyses of use confronts the ways in which usable IT security is established in the literature. Recent literature has called for better conceptual models as starting point for improving IT security. In contrast to such models we propose to dress up designers by helping them understand better the work that goes into everyday security. The result is a methodological toolbox that helps address and design for usable and useful IT security. We deploy examples of analyses and design, carried out by ourselves and by others to fine-tune our design perspective; in particular we use examples from three current research projects.

## Categories and Subject Descriptors
H5.2, K 4.1, K6.5

## General Terms

## Keywords
Security, interaction design, experience

## 1. INTRODUCTION
In a recent CACM Viewpoint, Susan Landau [26] calls for an understanding of the complexity of human behavior underlying IT-security and proposes a multidimensional approach with contributions from areas such as business, anthropology and engineering. Butler Lampson [25] discusses how the relationship between IT systems and users is all about rules, regulations and policies. While he is critical towards existing models of security, he still calls for better conceptual models of IT-security. In this, he concords with Don Norman [30], who takes his starting point in how even security experts work around security mechanisms to get work done. While both authors question the idea that we should strive for perfection and complete models of IT-security, they argue that the conceptual model of security mechanisms that users have, or should be provided with, is the key to better security.

In Human Computer Interaction (HCI), we have witnessed the raise and fall of conceptual modeling in general. In the 1980's changing human behavior was the focus. The complexities of human behavior were captured in models in order to inform design. Around 1990 came a second wave of HCI research that questioned the usefulness of this type of approach, pointing out how human behavior is contingent and situated, and that human beings are active actors working around whatever technical solutions exist. [1,5]. In more recent years this has been supplemented with a focus on emotion [30] and experience [27, 28, 29]. More than ever, these point away from conceptual modeling.

We are puzzled about the optimism around conceptual models in the IT-security area as represented by the above authors. It seems as if part of the area of IT-security does not embrace the insights from the past decades of HCI research and this poses challenges to HCI as well as IT-security.

In the past we have worked with second and third wave of HCI from the tradition of user participation in interaction design and organized a workshop on user-centered security at the NordiCHI 2008 conference. Our discussions in the following are strongly influenced by this workshop[1]. Our primary background is however in the ITSCI project and the eGov+ project (see below).

One of the very serious problems of providing models of security, which covers all possible uses, is that models become very complex (as Lampson acknowledges). Models are static and users need to activate the entire, complex model to achieve even simple things. While my home is my castle, most people prefer open and friendly environments to Fort Knox, even in the virtual world. Building large and complex security mechanisms and models is overkill for most situations and leads to a push for even further complexity. We propose to go with Alan Kay's well-known maxim: to make simple things simple, and complex things possible, even when it comes to security. Accordingly, in this paper we propose to give up modeling as a basis for usable IT-security, and go for a minimalist approach that makes simple and recognizable what most people need to do in most situations, while making it possible to do more in rare, complex and critical use situations.

In everyday life human beings choose the lock(s) of their front door to match tradeoffs between the general risks of the area that they live in, and the inconveniences of locking, alarming, letting

[1] The participants were: John Sören Pettersson, Torbjörn Näslund, Tim French, Dag Svanæs, Morten Harning, Gunnar Rene Øie, Peter Wolkerstorfer, Julian Seifert and the authors.

children in and out etc., knowing that their choices provide no 100 % guaranties against burglary etc. In this example as well as in IT-security, the perfect is the enemy of the good, and we propose to take seriously how people handle such deliberations in everyday life.

We describe our research background in sec. 2. In sec. 3 we describe our experiences with analyzing and designing for security dependent use situations. In sec. 4 we discuss the underlying methodology for design and toolboxes and in sec. 5 our experiences are captured in a toolbox, which is discussed in sec. 6.

## 2. Research background and motivation

The work reported in this paper is part of the IT Security for Citizens project (ITSCI), a four-year project that bridges between competencies in cryptography, mobile computing and HCI. As a driver for testing out new technologies, designs and methods, we iteratively design a mobile digital signature solution.

The aim is to replace an existing solution, where citizens may request a digital signature from the municipalities, in order to be able to login, authenticate, encrypt/decrypt, and sign their interaction with governmental institutions. This solution is installed on a single PC, and can be used from that PC only (unless you are a very proficient computer user). This solution has proven to be difficult to install for many people (an informal query among a group of 60 people working with IT in the public sector showed that only 3-4 had managed their own personal installation without problems). Furthermore the digital signature is activated in different manners as can be seen in this example experience from one of the authors: The author has used her digital signature for a long while to handle her taxes and in relation to the municipal services she acquired, when a new service got introduced. At a governmental health care website she would be able to find information about her records from doctors and hospitals, etc. Out of curiosity she tried to activate this service, and failed. The hotline service told her that she had not installed the digital signature correctly. This was indeed confusing since it had been working with other services for years. But, as the hotline representative phrased it: "We are not these other services!" While this was quite possibly true, and the website had been developed in a different organizational setting, it was not very obvious for the user that as a result, the digital signature needed to be installed and work differently.

Despite such usability problems, more than one million signatures have been issued. Our design is intended to replace the existing solution and therefore our intended users are a variety of people in a variety of everyday situations. As more and more information becomes electronically available, the need for a digital signature to replace the handwritten signature is rising, and these digital signatures must be more usable and useful to even more people across contexts as illustrated above. With a mobile digital signature, digital signing could happen in other places than at home at the computer desktop, for instance at a counter in a store or post office, in a bank, at the doctor or at municipals offices. This mobile digital signature design is a research challenge both in terms of cryptography, mobile protocols and interaction design. In this paper we report on the methods we developed to address the experience of security. The solutions themselves are still being iteratively designed and will be reported elsewhere. As such the mobile digital signature serves to set the stage of the design activity presented in this paper.

In the ITSCI project, and the affiliated eGov+ project[2], we have in additional worked to identify a number of use situations and experiences where IT security is at stake. We will activate these examples in the following along with examples from literature.

## 3. Reframing usable security

In the following, we move on to address a number of dimensions along which we propose that a change of perspective is necessary. We exemplify how the perspective on usable security can be reframed and how this change may support design.

### 3.1 Situated security and ongoing negotiation

Human beings in general depend on least-effort strategies [35] to achieve what they need to do, and they develop ways of working around technology if so needed [15]. [27] discusses an example of Niels' trip to Budapest with some friends. These friends had already bought their tickets on the Internet from a discount airline company when Niels was still considering buying his. The tickets were very cheap but prices were going up a little every day, and Niels needed to act quickly. He booked, issuing his credit card number, etc. He received no confirmation but for a withdrawal from his bank account matching the price. Days later he realized he had paid twice and tried to contact the airline company, only to learn that this could be done only via e-mail. Niels worried that he had been fooled; that the airline and trip were frauds; and that he would not get his money back. However, the departure went as scheduled, and even though he never got his money back, it was still an enjoyable and affordable vacation. In this example, Niels' trust in his friends, and the urgency of the situation, caused Niels to ignore many aspects that he would otherwise be concerned with, e.g. whether the e-travel site had a physical address. In this manner Niels did indeed act insecurely, even though the actual website was probably secure. However, this type of security did not prevent the double payment, and Niels decided not to be bothered because the trip was so cheap and nice anyway.

Grinter et al. [20] describe how households manage their concerns regarding internet security as a combination of technical solutions and such procedures as not allowing children to be online in private, e.g. in their own room. By giving children access to the Internet from a computer in the living room only, they imagined that they would be able to monitor what their children were doing and shield them from the worst of trouble [20]. These examples illustrate that security is situated.

Both of the above cases also illustrate that security is negotiated among several users as well as with past experiences of the user in question. [31] analyzes how hotel guests exercise security behavior at large and describe which threats the guest may experience. This model was a first step away from security systems threat models, towards an understanding of how hotel guests negotiate their security between electronic key-cards, credit cards, locked doors and personal belongings. In our everyday life, human beings base their security-sensitive choices on a mix of rationality and experiences (positive or negative), such as "it worked last time", "other people went there before me" or "the last time I used this type of terminal I had problems…". [27].

Accordingly, security can usefully be seen as element of an experience. McCarthy & Wright [29] show that experience with a given technology is not limited in time to the actual use situation.

[2] www.borgernesitsikkerhed.dk and www.egovplus.dk

Prior experiences influence our anticipation and future experiences influence how we reflect and look back on an experience. An analysis of web payment of a flight ticket, as in the story of Niels is likely to include questions like: What is being bought and why? Has the buyer used this website before? Does he know others who have? Does he normally shop this way or not? Would he feel differently about his trip, if later he bought another, and this led him to be stranded at a remote airport? We propose that in order to get to better security it is essential to capture such experiences, and to investigate how security is negotiated socially and over time.

As further illustrated, in everyday life we often assess security, safety and convenience by looking at what other people have done. In life in general, we assess the quality of a restaurant by the number of guests, and the safety of a path in the forest by how much it seems to be used. DiGioia & Dourish [10] turn such social navigation into a design strategy for security. They explore how visualization of other users' choices may enhance users' assessments of security, and how accordingly security can be seen as a collaborative effort, rather than as the individual protecting himself from the world. Knowing if other people, in particular even friends, successfully bought tickets from a particular website help us make informed choices (however not perfect), just like knowing how and when our neighbors lock their doors, leave them open, or turn on light, may help us make our own choices, and together monitor the security of a neighborhood. Accordingly, this example illustrates how security is shared or collaborative.

Grudin [22] points out how the Internet at large makes it literally impossible for us to control where and how information 'live' on, once placed somewhere on the Internet. Dourish and Palen [33], similarly, illustrate how information posted to a website may come back to 'haunt' the contributor much later. While Facebook pictures from parties may seem innocent, it is less obvious that a patient who has once granted a particular doctor access to her personal health information might grant such consent indefinitely. Generally, we have very little control over where such information ends up, and who can access it years later, and this illustrates how security measures cannot be determined once and for all. Human routines and needs develop, our social networks change, and our use of technology changes accordingly, yet our need for security, and control over security may change over time.

The sense of security, safety and privacy and thereby everyday people's motivation for dealing with such security, safety or privacy sensitive technology is negotiated over time. Whatever measures people end up taking towards protecting themselves and others, the underlying assessments are a product of an ongoing negotiation with themselves, others or experiences with prior encounters with technology. The taken measures may therefore vary even in similar situations. The actual activity, the context, prior experiences, others that are involved directly, others who are indirectly involved and the idea of what "others" would have done are all factors that participate in the actual negotiation of the sense of security, safety and privacy. In this context, sense includes perceived threats, perceived risks, and perceived effects of measures at hand. A common way to manage security, safety and privacy in IT are through policies, policy specification and policy enforcement. Inherently such policies lead to situations where users of IT artifacts specify policies in one situation, which are enforced in another situation.

Granlien & Hertzum [18] describe work at a hospital ward. Physicians prescribe medicine, nurses dispense medicine and they jointly administer the medicine. In the transition from a paper-based to an electronic medicine system the practice of negotiating the boundaries between prescribing and dispensing (thereby the security of the system) was replaced by static policies describing who could do what in the system. This change tended to obstruct the workflow and a new feature, where nurses could prescribe medicine through delegation mimicked the previous negotiation.

The taken measures of security are negotiated in one situation and enforced in a situation where the actual negotiation is not taken into account. Often these policies are specified once and then enforced over and over again. Moreover, security policies can be specified by one group of people and enforced in a situation involving another group (e.g. system administrators, security professionals, or management are specifying policies that end up being enforced in situations involving everyday users).

## 3.2 Groups or networked individuals?

Churchill [9] discusses how much of the recent focus on networked individuals has led to misleading design decisions with consequence for security and privacy. Since Facebook contacts are seen as equal to friends, much information about the page owner is open to the entire contact list, independent of whether the user finds this appropriate in the real world or not. She uses this example and others to call for a renewed focus on groups, a concern that we pursue here as well.

The National Danish Digital Signature has been praised internationally, whilst being criticized heavily in Denmark. It has, for those who managed to install it, given secure and uniform access to a large number of governmental, municipal and semi-public services. However, it has been difficult to install, and the method is inherently tied to one computer. The next version of the digital signatures has now been developed, and is no longer dependent on a "one user-one computer paradigm". Nonetheless, in the national vision of how to proceed with public services and security, there is a continuous mentioning of "the citizen" that needs an individual and personalized service, etc. Nowhere it seems is there a concern for how users may join forces and help each other. Neither is it clear how such (more or less stable) units as: couples, families or other smaller groups of citizens may be dealt with, beyond their own individual access.

An example from the eGov+ project illustrates that such units cause challenges to public services in general and security concerns in particular [2, 3]. Planning parental leave involves the mother, the father, the child (to the extend that a lot depends on the actual birthday of the child, which is not known when the planning starts), the employers of both mother and father, and the local government to the extent that one of the parties is unemployed, or partially so. Both father and the mother may distribute some part of the leave among themselves whilst other parts of the leave are bound to either the mother or the father. All in all, the leave can be deployed over the first eight years of the child's life. This obviously means that many families need to juggle their annual leave entitlement of not only one, but also several children at the same time. Also the planning may for the same reason involve a network of spouses and ex-spouses, some of whom one may want to share control and "secrets" with, and others not. Parental leave planning is a process involving several parents, employers and a municipal office, sometimes happening at the dining table in the family home, and at other times happening at work of one of the parents or face-to-face with the municipal caseworker.

In any event it is not something to be resolved simply by a single individual citizen acting alone in one location.

Based on such examples we propose that e.g. the prisoner's dilemma exists for security as well as for group technology in general [21], and optimizing the trade-off between effort and security for the individual, may be different from doing a similar optimization for the group, for instance.

Holone & Herstad [23] investigated the longitudinal experiences with a collaborative tool for route planning for wheelchair users. Wheelchair users could get route suggestions from A to B that were traversable in a wheelchair. If they got stuck somewhere they were able to report that this particular spot was not accessible in a wheelchair and get an alternative route. Users of the tool reported that they would mark a place inaccessible if they did for instance have to use the cargo elevator to access it. It could have been useful information for other wheelchair users to know that even though a place did not offer proper wheelchair accessibility they still offered an alternative. However, the wheelchair users were seeing this lack of information as a way of protecting the privacy of wheelchair users in general. Privacy is not only about private personal information it also has a group dimension.

## 3.3 Artifact and infrastructure

Research in IT security in large has addressed protection of systems and systems data. For instance a bank deploys security measures to protect their account data or tax authorities to protect their taxation data from tampering. For a while a lot of research has been addressing how large systems like bank systems or like could be made friendlier and more usable still being secure. This has lead to designs where users are encouraged, helped or enforced to do things in a "right" way. As we have mentioned in our previous examples, such systems cannot and should not be separated out when seen from the point of use.

Experience links these systems together as does their various kinds of interconnectedness in use.

Star & Ruhleder, [36, p. 254] introduce infrastructure as terminology to focus on this issue: "No artifact, computer-based or otherwise, is a discrete entity, a standalone thing. Its development and use are defined by complex relationships." They use an example to address this relational perspective and point out how infrastructural challenges can be identified within the setting of use, regarding as a result of unforeseen consequences of design or conflicting issues of use, and between different ways of thinking about use and, in our case, security.

At the same time as security must be addressed in terms of infrastructure, security is influenced by many different design-choices made in relation to many different components of the specific IT artifact in focus. From choice of hardware and communication protocols, over visualization and interaction design to anticipated use situations all influence how users assess and act on security.

This means that design of and for usable IT-security cannot be separated from the design of the IT artifact or infrastructure at large, neither in terms of process nor product.

## 3.4 Security, safety, trust, privacy

The security domain has a very large set of more or less well-defined concepts. However these concepts stems from a professional perspective on security IT issues. If we really want to understand IT security from within an everyday context we have to analyze these contexts from within.

When doing research on usable security it is virtually impossible to separate this issue from concerns for safety, trust and privacy (see also discussion in [11, 12, 24, 34]. While they are not the same, there are many overlapping concerns and issues, as illustrated in e.g. the Facebook examples given above. In literature, there are many different measures and strategies to tackle privacy, security or safety related issues when designing secure IT infrastructure. However, as with research it is not clear that these distinctions make sense in everyday use of technology. People encounter different privacy, security or safety related phenomena, but they do not distinguish between them in a rigid way. For instance many of the European languages even do not have two words for security and safety[3].

Trust is often mentioned along with the concepts of privacy and security. It has a variety of meanings and definition and often it is hard to distinguish between them. Trust can mean trust in a person or trust in an institution, which is trust in a different way than people trust their colleagues, friends, or family [see also [12]). Giddens state that a characteristic in modern society is that one has to trust expert systems (technology which one delegates some tasks to without knowing how the system carry out the tasks) [17].

The lack of clarity between these distinctions may lead to users utilizing measures meant as protection for one threat as protection for another threat, as described by Norman [30]. As a simple example it is difficult for people to understand the difference between why passwords would be used for net banking, Internet web shops, wireless Internet spots, and pause screens on the PC to mention a few examples. That users often are not helped in making such distinctions can be illustrated by examples where websites demand strong passwords just because they can, or because the activity for which the password is requested looks quite differently from use than it does from design.

In the eGov+ project we have seen several examples where log-on through digital signature to municipal websites was requested even though there was no need for this level of security: One example was signing-up a child for day-care. Where initially one municipality had chosen to use digital signature for such sign-up, they realized that there was no risk involved in the procedure for them, or for the citizens, and hence they developed a much simpler procedure without any security measures at all. Obviously security is needed at a later stage when parents are actually offered and accepting a day-care facility.

IKEA offers a wish list/shopping list facility on their website[4]. Even though this cannot be used for anything beyond gathering wishes, it is designed as part of their account system, and hence users need to log-on with a strong password in order to make use of the wish list, an obvious example of confusion even on the part of the designers.

## 3.5 Minimalist security?

Most often security measures are focused on worst-case scenarios. This is the case both when analyzing the need for security measures and when these are invented, despite the situation that we have described earlier: that people apply least effort strategies in their everyday activity, and work around technical complications

[3] Scandinavian languages, Finnish, German and properly more has only one word for security or safety phenomena.

[4] www.ikea.com

whenever they can. Past experiences help users in developing these strategies (for good and for bad).

When security tools are based on maximal complexity, they seem cumbersome or unnatural for everyday users, who end up working around them. For instance in a teleconference setting it can be crucial to know who is present and thereby listening and viewing in remote locations. However, the problem also exists even if the matters discussed are not confidential or controversial. A presenter most often want to know who is paying attention and thereby who can be expected to get the message. A solution that requires a lot of interaction and new practices might be suitable for teleconferences where serious and confidential matters are discussed; it could be way too complex for weekly meetings among colleagues and friends. Taking Alan Kay's famous maxim as an outset: "make simple things simple, and complex things possible" an ideal tool should handle both cases and make it possible for users to develop practices for use through everyday use and hence be experienced users when it matters.

Asking users to change their passwords repeatedly results in users re-using their passwords for several sites or services. While from the perspective of one service provider this (may ideally) increase security for their site, from the perspective of the user or customer, the result may be to the contrary. Increasing security for one party may inevitably decrease it for the other party.

The research project as reported in [31] was, through concrete interaction design, concerned with making human beings feel safe as they explore personal digital materials on 'foreign' displays in a hotel room. Here the resulting design consisted of a mobile phone being used as the key to personal digital materials. Namely, simple gestures for pushing personal materials to the 'foreign' displays in the hotel as well as a simple gesture for deleting them from the hotel host machine and (metaphorically) bringing them back to the personal device again.

# 4. Users and design

While the last two decades of research in HCI have strongly emphasized the relevance of actively involving future users in design, such approaches have not yet reached the security area as the three discussion pieces illustrate [25, 26, 30]. At most, users or other stakeholders have been included in the formulation of a security policy or in the specification of who can access what and when. Involving users in the security design process may be difficult, because so far, concepts and methods applied in the area have entirely come out of technical research. Concepts such as public key cryptography and hash functions are not directly connected to the everyday life of people, and it is time for research to reframe the agenda and provide a view from use.

Overall, our quest echoes the warnings to designers of Grudin [21] and Churchill [9]: The user is not you, and you are not the user! In other words we propose a framework that help designers avoid making many of the assumptions discussed above, while at the same time helping designers focus on how use of secure and insecure IT actually happens in the particular use context.

Instead of new conceptual models we propose to focus on the challenges of collaborating with users to help them explore security experiences. Research needs to provide methods to do so. We propose to strive for simplicity and openness in security design so that development of security in collaborative use may be accommodated for, immediately as well as in long-term perspectives.

## 4.1 Basic assumptions about use and design

Based on the above insights from literature and own empirical investigations, we move on towards proposing a design methodological toolbox for HCI-based security.

In line with Stolterman [37], or [6] we aim to dress up designers for their design activity when it comes to designing usable and secure IT. There are several ways in which this may happen: conceptual glasses to help designers see use and security in new ways, techniques and tools to address such matters in design, etc.

Our perspective on such a toolbox is open-ended, in terms of where security-specific interaction design ends, and general issues of HCI, security or software design at large begin. It is also incomplete to the extent that designers need to tailor the toolbox to their own experiences and to the particular situations that they are facing [6].

Our perspective on design for usable and secure interaction is based on a number of general assumptions about technology in use and how to design for it that are developed elsewhere [4].

1. Use is dynamic and under continuous development and it cannot be fully anticipated in design.
2. Human use activity is happening through shared practices and not only through individual use; hence design must engage with the level of (communities of) shared practices as well as with individual routines.
3. Human activity is mediated by multiple artifacts that deploy a variety of security strategies and technologies. Design must pay attention to these multitudes of technologies and strategies.
4. Human beings use ordinary language in their everyday encounters with each other, and they activate past experiences in these encounters. Hence the everyday language games of security are important when designing for usable security.

In the following we relate these rather general assumptions about the relationship between design and use to the specific discussions above. This is done in order to give some simple pieces of advice to dress up the IT security designer for action.

# 5. Toolbox and framework

With the proposed perspective on use, it is important to work with users to identify particular use situations to be explored further in design, to eventually identify the situations that the future product has to serve, and design how. In [37] prototyping is seen as "framing and exploring a design space", by traversing the design space, providing prototypes that are "purposefully formed manifestations of design ideas". Prototypes, in other words, help designers sketch and filter design ideas. An alternative view of prototyping, rooted in participatory design is that of prototypes as means for helping users get hands-on experience in design [7]. This is a way for the users to experience the future hands-on throughout the process of design. The reasons for this are that hands-on experience is necessary for understanding the possible future use, and breakdowns in use are the points where problems of future use get exposed to the users and designers [7].

When identifying typical and critical use situations it is important to look for:

1. The users/actors and how they are related to each other (their peers) with respect to collaboration and negotiation.
2. The material conditions, relevant objects and related artifacts with and through which security is executed.
3. Experiences, practices and rituals relevant for the (security) acting in the current situation.

In general scenarios and personas may be used to capture such situations in design [6]. In our particular project, we have worked with identifying quite specific user stories as basis for design in the usable security context [29, 30].

Designers and users and designers together, may use such stories to challenge their assumptions about security in use, and to situate workshops addressing future secure technology in use.

In line with [6, 8] it is useful to distinguish between situations and scenarios that are typical in terms of security, and such who are critical.

By addressing this distinction it is furthermore possible to discuss and address worst-case scenarios and least-effort strategies so as to discuss and assess when maximum security is necessary and when weaker measures are sufficient (see below).

By analyzing and discussing such situations with users it is possible to pull apart the often entangled issues of security, privacy, safety and trust). This will help the designers identify the appropriate measures. However, it seems equally important to work with the users to understand how the users experience the situation as a whole with appropriate security, privacy, safety and trust.

Finally, it is important to remember that use develops. First of all the collection of current relevant use situations are NOT the future use situations, even if they may be used as basis for creating future use scenarios [6].

## 5.1 Use of the toolbox

Before designing IT artifacts for a certain domain, in-depth analysis is a must. We propose to analyze as realistic situations as possible. Only in realistic contexts are relevant prior experiences activated, established practices utilized and authentic and pragmatic security assessments carried out. Their exist a variety of different qualitative methods to capture activities from realistic contexts: Cultural probing [16], mobile probing [28], observation, participant observation, design games [13], enactments [28], participatory design workshop [19], focus groups, semi-structured interviews and even more. Such methods generate user stories, observation notes, video recordings, audio recordings, transcriptions of recordings or other forms of qualitative empirical data.

Our toolbox provides conceptual glasses that help emphasize empirical findings that regard IT security. Analysts can look at their empirical data through these conceptual glasses hereby improve how their analysis inform design of secure IT-artifacts. The concepts from the proposed toolbox do not point out specific phenomena from the data. By being abstract interrelated concepts they allow and require analysts to find and define what the concept's concrete versions are and by that ground their analysis.

The toolbox can also be utilized to improve prototyping and intervention activities. In iterative design processes prototypes are created with the purpose of intervening in a contexts and by that capture qualitative data. By looking at design sketches, or early versions of prototypes through the conceptual glasses designs may be informed even before the interventions. Also the terms can help structure a design argument among designers. Obviously, these iterations may at some point end up as the end product. In that sense the toolbox can be said to also inform design of end products.

Like the toolbox can be used to structure an argument among designers it can also be used in participatory design activities that involve future users of a product. Facilitators of, for instance, participatory design workshops could present the terms along with examples of how the abstract concept could be concretized in the specific context [28]. Then workshop participants can apply the terms to their common practice and thereby structure arguments among each other or towards designers.

## 5.2 The dimensions and the conceptual glasses

The toolbox consists of five dimensions: *In-situ–ongoing*, *Acting subjects–groups, Artifact–infrastructure, From within–from without,* and *Minimalist–perfect*. A phenomenon and its related empirical findings may be seen through the conceptual glasses of more than one of these dimensions. The five dimensions should not be seen as an exhaustive list, however they are expressive tools from our own research and design work. Each dimension describes a set of open-ended concepts and how these concepts relate to each other. We exemplify how these concepts and -dimensions have been used in this work to support analysis, prototyping and user participation.

| Dimension | Conceptual glasses |
|---|---|
| In-situ–ongoing | Negotiation<br>Specific peers<br>Elusive peers<br>Negotiation artifacts |
| Acting subjects–groups | Enduring relationships<br>Transient relationships<br>Assumed responsibilities |
| Artifact–infrastructure | Components<br>Influence<br>Interaction |
| From within–from without | Security circumstances<br>Changes<br>Ceremonies |
| Minimalist–perfect | Actions<br>Degree of complexity<br>Degree of criticality<br>Simpler siblings |

**Table 1 Toolbox overview**

### *5.2.1 The In-situ–Ongoing dimension*

This dimension addresses how users make sense of security and thereby become able to make security assessments and decisions. The sense of security can on one hand be the result of an ongoing negotiation or the compromise of an in-situ negotiation among specific and elusive peers. Whether the sense of security is negotiated in-situ or ongoing it can be mediated through negotiation artifacts.

Security assessments and decisions are negotiated through ongoing negotiations between specific peers and elusive peers mediated through negotiation artifacts. Peers are the participants taken part in the negotiation in-situ. Elusive peers are non-present (colleagues, management, other stakeholders who are referred to in

the negotiation) or elusively defined peers (e.g. others, customers, hackers, neighbors). The negotiation can be an ongoing negotiation with one self and the IT infrastructure in situations where a user is not interacting with others. However it is likely that also one or more elusive peers would take part. Negotiation artifacts mediate the negotiation directly as when the user has the car-key in hand, or indirectly.

As an example, the inSpace project at Georgia Tech investigated how remotely located participants could be involved in presentations in distributed project work. An idea was to map a physical project room to a virtual world and have remote participants collaborate through an avatar in the virtual world. An electronic whiteboard was mapped to a virtual whiteboard. The virtual whiteboard had a visible zone of engagement. Avatars inside this zone could see and edit the content and simultaneously the avatars were displayed on the electronic whiteboard. Based on this negotiation artifact the design process explored how specific peers would be able to negotiate their security and engagement in situ, while focusing on specific as well as elusive peers.

### *5.2.2 The Acting subjects–Groups dimension*

This dimension addresses users' internal relationships and responsibilities. When people take part in a security dependent situation it may be as an acting subject, in an enduring relationship to others, in a transient relationship to others, or with an assumed responsibility. Wherever people are aware of it or not, they are often acting as members of several overlapping groups.

A user is an acting subject that handles a dynamically changing set of purposes in any given situation. People have enduring relationships (e.g. being a mother of one's son) as well as transient or less prevalent relationship towards other participants (e.g. being somebody's boss, friend or spouse). In many instances acting subjects assume responsibilities (e.g. defending weak groups, handle the interest of someone not their own, handle the interests of someone like themselves) for specific individuals as well as a more elusive someone.

This point towards the attention towards groups, the security needs of which are different from the sum of the needs of the participants. As an example, in project eGov+, a self-service tool was designed where parents, municipal caseworkers and employers could work together in planning parental leave. The local rules allowed parents to be on leave on and off for the first nine years of a child's life. Through these nine years many participants could be involved (e.g. changing employers and new spouses) and it was important to explore in design this variety of enduring and transient relationships together with the possibility of handling security of the group as such.

### *5.2.3 The Artifact–Infrastructure dimension*

An important balance in handling IT security lies between the IT-artifact being designed for usable security and the infrastructure at large. While users interact with the entire infrastructure, they also interact with the different components. Issues of influence to a security dependent use situation stem from different components. Different situations in different contexts emphasize the actual influence from different components. In one situation the influence from component will be almost invisible whereas the same component may require more interaction in another situation.

It is necessary to focus on the usable security of each component as well as the usable security of the entire infrastructure.

In analyzing small user stories collected through cultural probing in order to investigate IT-security in everyday contexts we found that some stories addressed issues pertaining from the fact that a digital signature solution was based on Java Applets. Other stories addressed the physical location of payment terminals at a counter in a store.

In the ITSCI project prototypes were built to explore how different communication schemes influenced users' sense of control over when they were issuing their digital signature and when not. The digital signature was stored on the users' mobile phones and the text to be signed was available on a nearby terminal (e.g. at a counter in a store). Among other components we identified a component responsible for establishing a connection between the mobile phones and the terminals. We also identified a component needed for transferring the data back and forth between the mobile phones and the terminals.

These two components could be implemented either by two different technologies or the same technology. To investigate how different technologies would change these components and influence the sense of control that users had, and to experiment with how users could interact with these component, we explored - combinations of Bluetooth, RFID-tags, 2D-barcodes, SMS (Texting), 3G, and Wi-Fi and discovered how different communication technologies influenced the users' perception of control and interaction. Utilizing Bluetooth or Wi-Fi allowed the user to interact with the infrastructure by removing the phone from a terminal's proximity. In contrast utilizing RFID-tags or barcodes required that users hold their phones close to a designated reader. Texting and 3G-networking did not apply when changing the proximity to the terminal (e.g. by leaving the store) hence illustrating the importance of design choices at component levels for the security of the entire infrastructure.

### *5.2.4 The From within–From without dimension*

This dimension addresses how changes in a groups security circumstances can be made explicit through rituals from within the context or through security measures from without.

In summary, any community or group has different security circumstances, be these preferred or unwanted. Different events change these, either due to decisions and actions of the group, or due to events from outside. Where aspects of these circumstances may, from without, be identified as issues of trust, privacy or safety in addition to security, it is equally important to understand the issue from within, and for how it is understood in the group.

Sometimes changes in circumstances are made explicit through ceremonies that are ritualized to make security explicit. By identifying circumstances, changes and ceremonies of future use situations prior to design of IT-artifacts helps ground the design and make it more useful to future users.

To exemplify such analytical glasses, a municipal self-service website offered a service where parents could sign up their kids for daycare by submitting the kid's social-security number and name. It is preferred that only kids that where electable for daycare would be on the waiting list. An unwanted state would be if somebody without the appropriate needs and rights would end up on the list. Before the web self-service, parents had to show up in person at the municipality office as an example of such a ceremony that was set up to ensure that only the right kind of children were signed up. By addressing the question of whether security in this case should come out of this specific situation, where really

there was no risk in signing up somebody by mistake or as fraud, or security should be aligned with the remaining municipal infrastructure where the digital signature was applied, designers of the self-service system ended up with a simple one-page form without any login or authentication, which would otherwise be a common security strategy in this municipality.

### *5.2.5 The Minimalist–Perfect dimension*

This dimension addresses the complexity of critical security tasks and in relation to the minimal complexity of the required actions. Since everyday tasks are most-often simple and non-critical, they should be secured through simple actions in contrast to complex or critical tasks that may need to be secured through complex actions. While this dimension reach from a minimalist approach to a perfection approach, reaching for perfect security is most often not necessary and not possible. This dimension promotes a minimalistic approach. By identifying simpler siblings of critical and complex tasks, we focus on the continuums from minimalist to perfect use experiences.

Security phenomena are not inherently complex. People on the other hand act through least effort strategies. Accordingly the majority of actions carried out regards simple matters and should be simple. Most complex and critical security actions have less complex and non-critical siblings. The continuum from everyday routine actions to extraordinary and uncommon ones is essential. Identifying required actions and their degree of complexity help bring forward complex actions simpler siblings and help design for a such a continuum, rather than they make designers focus on the complex solution to be perfect for all situations.

The above daycare example is also an example of the choices made along this dimension, and the estimation of the necessary security measures.

### *5.2.6 Summary*

Security is not a layer that you apply to your IT infrastructure or IT artifacts after they have been designed. If security is needed, it has to be considered even before the initial analysis. The rather impressive variety of different IT security measures should be tailored to and activated in each iteration of design. User involvement and thorough analysis of the future use context and the communities of practices are essential elements of such a process. We suggested the use of several design activities for capturing qualitative data in this process. In this paper, we have developed a toolbox for analysis and for structuring design arguments, hence fine-tuning the sensibility of designers to usable security matters.

The open-ended nature of the toolbox concepts requires that - designers take an outset in concrete use situations. While the concepts are fairly abstract, they help analysts and designers carve out concrete empirical findings from within the intended use context. That turns around the stream of information: where earlier, clever and proven IT security solutions were given to the users of IT infrastructure whether they liked and needed it or not, our toolbox encourages information from the use context to go to the designers in order to inform tailoring of IT security solutions.

## 6. Discussion and future work

Our approach is motivated by an ongoing shift in perspective along several recent contributions in IT-security and interaction design [10, 11, 27, 28, 31, 33]. In much of this research, the focus is on use and the users. When do everyday users need IT-security solutions? Why? And how? How is it possible to address and even design for a balance between use focus and technical challenges? Social navigation [10] is one of the few alternatives proposed for new forms of security. Similar to our ideas this paper proposes to make use of particular social mechanisms in designing IT-security mechanisms. We believe that our approach will lead to further identification of such possible mechanisms arising from use, but we have not here specifically pursued any of those as alternatives to social navigation. However, we have not yet proposed any such alternative mechanisms here.

In [11 and 33] it is indicated that privacy and trust are concepts arising from use whereas security is a concept with a more technical focus. We have worked with an understanding of security that is rooted in use. Nonetheless we have been facing a terminological challenge: Is usable security the same as useful security? Technology that is secure is not necessarily perceived of, sensed or experienced as secure [27]. Some IT artifacts are specifically security technologies, while for many others security is one of many elements of the infrastructure. Finding a suitable vocabulary in this is a challenge per se, and one that we continue to address.

In contrast to the proposed toolbox, the conceptual modeling approach that we have discussed extensively, does not analyze the intended use situations from within and it may require that the entire conceptual model is understood by the users, for it to be applied. In contrast we have proposed to work with a minimalist approach, which tries to target and minimize security measures. We need to pursue this way of thinking further and the design work of the ITSCI project is targeting this issue for future reporting.

The open-ended nature of our toolbox let facilitators give the concept meaning in participating users own context. Thus participating users can be dressed up as well as designers and get help in structuring an informed design argument.

Besides being open-ended towards users and users' context, the toolbox is open-ended towards analyst, designers or researchers. We do not see our toolbox as final, exhaustive or universal. We encourage practitioners to tailor the concepts to fine-tune them even more. Moreover, we will ourselves continue to develop the toolbox and hope that other researchers will be inspired by or challenge the concepts.

Our research will continue to elaborate on the dimensions of the toolbox, and to explore security issues as they are situated in use. Furthermore, we will pursue further design methods for participatory and user-centered IT-security.

## 7. Conclusion

In contrast to elaborate security models we propose to dress up designers by helping them understand better the work that goes into everyday security. The result is a methodological toolbox that helps address and design for usable and useful IT security.

We have demonstrated how more fine-grained concepts help assist analysis and design of useful and secure IT artifacts and infrastructures. Overall these concepts point towards maintaining simplicity when this suffices, providing paths from simple to complex and high-security when that is needed and identifying when perfect security is to strive for.

## 8. References

[1] Bannon, L. (1991). From human factors to human actors: the role of psychology and human-computer interaction studies

in system design, Design at work: cooperative design of computer systems, Erlbaum, pp. 25-44.

[2] Bohøj, M., Borchorst, N.G., Bouvin, N., Bødker, S. & Zander, P.-O. (2010). Timeline collaboration. CHI 2010, pp. 523-532, ACM Press.

[3] Borchorst, N.G., Bødker, S. & Zander, P.-O. (2009). Participatory citizenship, ECSCW 2009, pp. 1-20.

[4] Bødker, S. (1991). Through the Interface – a Human Activity Approach to User Interface Design. Hillsdale, NJ: Lawrence Erlbaum Associates.

[5] Bødker, S. (2006). When second wave HCI meets third wave challenges. ACM International Conference Proceeding Series; Vol. 189. Proceedings of the 4th NordiCHI, pp. 1-8.

[6] Bødker, S. & Christiansen, E. (1997). Scenarios as springboards in design. In Bowker, G., Gasser, L., Star, S.L. & Turner, W. (eds.), Social science research, technical systems and cooperative work. Erlbaum, pp. 217-234.

[7] Bødker, S. & K. Grønbæk (1991). Design in Action: From Prototyping by Demonstration to Cooperative Prototyping, in Greenbaum, J. & Kyng, M. (eds.). Design at Work: Cooperative Design of Computer Systems. Hillsdale, NJ: Lawrence Erlbaum Associates (pp. 197-218).

[8] Carroll, J. M. & Rosson, M. B. (1992). Getting around the task-artifact cycle: how to make claims and design by scenario. CACM, 10(2), 181-210.

[9] Churchill., E. (2010). The (anti) social net, interactions, 17 (5), 22-25.

[10] DiGioia, P. and Dourish, P. (2005). Social navigation as a model for usable security. SOUPS '05, vol. 93. ACM, New York, NY, 101-108.

[11] Dourish, P., Grinter, B., Delgado de la Flor, J. & Joseph, M. (2004). Security in the wild: user strategies for managing security as an everyday, practical problem, Personal Ubiquitous Computing, 8(6): 391-401,

[12] Dwyer, C., Hiltz, S.R. & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. In Proceedings of the Thirteenth Americas Conference on Information Systems.

[13] Ehn, P. & Sjögren, D. (1991). From System Description to Scripts for Action. In J. Greenbaum & M. Kyng (Eds.), Design at Work: Cooperative Design of Computer Systems (pp. 241-268). Hillsdale, NJ: Erlbaum

[14] French, T., Liu, K., & Springett, M. (2007). A Card-Sorting Probe of E-Banking Trust Perceptions, Proceedings HCI 2007, Lancaster University, UK, **1**, 45-53.

[15] Gasser, L. (1986). The integration of computing and routine work. ACM TOIS 4:205-225.

[16] Gaver, W. W., Boucher, A., Pennington, S., and Walker, B. 2004. Cultural probes and the value of uncertainty. Interactions 11, 5 (Sep. 2004), 53-56.

[17] Giddens, A. (1990). The consequences of Modernity, Stanford CA:Stanford University Press.

[18] Granlien, M.S. Hertzum, M. 2009. Implementing new ways of working: interventions and their effect on the use of an electronic medication record. In Proceedings of the ACM GROUP '09. ACM, New York, NY, USA, 321-330.

[19] Greenbaum, J. and Kyng, M. (Eds.) (1991). Design at Work: Approaches to Collaborative Design, Lawrence Erlbaum, Hillsdale, New Jersey.

[20] Grinter, R. E., Edwards, W. K., Chetty, M., Poole, E. S., Sung, J., Yang, J., Crabtree, A., Tolmie, P., Rodden, T., Greenhalgh, C., and Benford, S. 2009. The ins and outs of home networking: The case for useful and usable domestic networking. ACM TOCHI 16, 2 (Jun. 2009), 1-28.

[21] Grudin, J. (1994). Groupware and social dynamics: eight challenges for developers, CACM 37 (1), 92-105.

[22] Grudin, J. (2002). Group dynamics and ubiquitous computing. CACM 45, 12, 74-78.

[23] Holone, H., Herstad, J., (2010). Negotiating Privacy Boundaries in Social Applications for Accessibility Mapping. NordiCHI 2010.

[24] Karvonen, K., Cardholm, L. and Karlsson, S. (2000). Cultures of Trust: A Cross-Cultural Study on the Formation of Trust in an Electronic Environment. Proceedings of the Fifth Nordic Workshop on Secure IT Systems, NordSec 2000, 12-13 October, 2000, Reykjavik, Iceland.

[25] Lampson, B. (2009). Privacy and security. Usable security: how to get it. CACM 52, 11, 25-27.

[26] Landau, S. (2008). Privacy and security A multidimensional problem. CACM 51, 11, 25-26.

[27] Mathiasen, N. & Bødker, S. (2008). Threats or threads: from usable security to secure experience, NordiCHI 2008 Building Bridges Proceedings of the 5th Nordic Conference on Human-Computer Interaction, Lund, Sweden, 20-22 October, 2008. Lund, Sweden : Society for Industrial and Applied Mathematics, 2008. s. 283-290.

[28] Mathiasen, N. & Bødker, S. Experiencing Security in Interaction Design, accepted for CHI 2011.

[29] McCarthy, J. and Wright P. (2004) Technology as Experience. MIT Press.

[30] Norman, D. (2009). THE WAY I SEE IT. When security gets in the way. interactions 16, 6, 60-63.

[31] Pagter, J. I. and Petersen, M. G. (2007) A Sense of Security in Pervasive Computing - is the light on when the refrigerator door is closed? Financial Cryptography 2007: LNCS 4886, Springer Verlag pp. 383-388.

[32] Palen, L. & Bødker, S. (2007). Don't Get Emotional. In: Peter C., Beale R. (eds.): Affect and Emotion in Human-Computer Interaction. LNCS, vol. 4868. Springer, Heidelberg, pp. 12-22.

[33] Palen, L. and Dourish, P. (2003). Unpacking "privacy" for a networked world. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. CHI '03, 129-136.

[34] Riegelsberger, J., Sasse, M.A., and McCarthy, J. (2005). The Mechanics of Trust: A Framework for Research and Design. *IJHCS*, 62(3), 381-422.

[35] Scribner, S. (1986) Thinking as action: Some characteristics of practical thought. In Sternberg, R. & Wagner, R. Practical intelligence, Cambridge: Cambridge University Press.

[36] Star, S.L. & Ruhleder, K.(1994). Steps Towards an Ecology of Infrastructure: Complex Problems in Design and Access

for Large-Scale Collaborative Systems, CSCW 1994, pp. 253-264.

[37] Stolterman, E. (2008) The nature of design practice and implications for interaction design research, International Journal of Design 2(1), 55-65.