Threats or threads -from usable security to secure experience?

Niels Raabjerg Mathiasen
Department of Computer Science
University of Aarhus
Aabogade 34
8200 Aarhus N, Denmark
+45 8942 5687
nielsm@daimi.au.dk

Susanne Bødker
Department of Computer Science
University of Aarhus
Aabogade 34
8200 Aarhus N, Denmark
+45 8942 5630
bodker@daimi.au.dk

ABSTRACT
While the domain of security dependent technologies brings new challenges to HCI research it seems that the results and breakthroughs of HCI have not been used in design of security dependent technologies. With exceptions, work in the research field of usable security may be criticized for focusing mainly on adjusting user behavior to behave securely. With our background in newer HCI perspectives we address secure interaction from the perspective of security technology as experience. We analyze a number of collected user stories to understand what happens when everyday users encounter security dependent technologies. We apply McCarthy & Wright's [12] experience framework to the security domain and our collected stories. We point out that there are significant differences between being secure and having a secure experience, and conclude that classical usable security, focus on people's immediate security experience, and the full focus on experience proposed by McCarthy & Wright lead to three very different interaction concerns, analytically and as regards design. We illustrate these differences by examples, and conclude with a discussion of how to advance the field of usable security.

Categories and Subject Descriptors
H.5.2 [User Interfaces]: Information interfaces and presentation – user-centered design.

General Terms
Usability, security, experience.

Keywords
Usable security, user experience, user story collection, user testing, human-computer interaction.

NordiCHI 2008: Using Bridges, 18-22 October, Lund, Sweden

1. INTRODUCTION
Lack of usability has proved an important hindrance for raising IT-security among everyday users [6]. Everyday users are concerned with data privacy, confidentiality and authorization. These same everyday users are forced or encouraged by computer systems to behave in a secure way.

To ensure IT-security, computer scientists and system designers have invented strong cryptology and secure protocols to enforce security. Hacking of state-of-the-art security systems is now so difficult that hackers turn to users and the use situation. Early attempts to improve security of use situations have led to systems and system maintainers that request users to behave securely. In 1999 Whitten & Tygar [16] defined the term usable security and five properties of the security domain. They used their definition and properties to analyze and explain why users behave inappropriately when using PGP 5.0.

The rising research field of Usable Security, also known as HCI Security, features around 300 papers[1]. Several approaches may be identified within this emergent field. One approach is to investigate users' choices, statements, knowledge, etc. Surveys [8] and scenarios to investigate user choices [10] are dominant instruments of this approach, leading to such results as quantitative measurements and overviews. Another approach is to evaluate different security related applications. We already mentioned the Whitten & Tygar's [16] evaluation of PGP 5.0. Others work with design strategies, design patterns or guidelines. For example Yee [17] that introduces 10 principles of usable security and DiGioia & Dourish [7] that introduce the social navigation pattern to the security domain.

Security is a broad term. It represents personal security, physical security, information security, and computer security. Traditionally, computer security is thought of as software security mechanism (e.g. passwords, encryption), mostly in relationship with electronic information and services. Usable security is less well-defined. Often usable security is concerned with improving

[1] The research field of usable security could be thought of as centered around SOUPS (Symposium On Usable Privacy and Security) http://cups.cs.cmu.edu/soups/2008/, a blog http://usablesecurity.com/, a mailing list, and a bibliography http://www.gaudior.net/alma/biblio.html. The bibliography has almost 300 entries.

the usability of security mechanism. Such concerns lead to a focus on systems and their components. If one focuses on the use situation, users, contexts, and the users' prior experiences are included. Accordingly, usable security of use situations is based on a wider definition of security. This definition includes information security if and when it comes to the information the users are interested in. It furthermore includes concepts originating from personal security when it comes to e.g. the perception of being secure and it includes parts of physical security (e.g. electronic door locks, fire alarms). When technology is part of situations where security is at play according to the wide description described above we will refer to it as security dependent technology.

Pedersen & Pagter [14] started to look at security beyond inappropriate use of technology by revisiting hotel guests' security behavior at large. They came up with a model that describes which threats the guest may experience. By its starting point in user experience, this threat model was a first step away from security systems threat models that usually describe the threats, which the systems need to protect themselves against (e.g. denial of service, tampering with data).

As with the hotel guest, security dependent technologies are often used in a mixed context. Users may be alone or collaborating with others. They may be at work or at home. They may be participating in activities at work interleaved with activities originating from the rest of their lives. Security dependent technologies often bridge between the physical and the virtual: hotels apply electronic key-cards, credit cards help us pay in the supermarket, and physical devices may even be necessary to grant access to entirely virtual information in e-banks or airport-security systems. It is not likely that everyday users get a deep understanding of how encryption and decryption algorithms work. Instead, in our everyday life, we base our security dependent choices on a mix of rationality and experiences.

It is in the field between properties of the security domain, and the experiences that users gain in everyday situation that we place this research. In our research we analyze user stories to gain insight into experiences at play in security dependent use situations. From these analyses we get a better grip of the tensions between how security systems may work to encourage secure behavior from their users, and the importance of the total use situation as well as past experiences of the users.

2. A RICHER PERSPECTIVE ON SECURITY

In accordance with Bødker [3] HCI research has largely come in three waves. The first, with roots in cognitive science bloomed in the 1970s, while the second, identified by Bannon [1] took HCI "from human factors to human actors". Theory focused on work settings and interaction within well-established communities of practice. Situated action, distributed cognition and activity theory were important sources of theoretical reflection, and concepts like context came into focus. Rigid guidelines, formal methods, and systematic testing were abandoned for a variety of participatory design workshops, prototyping, etc. In the third wave use contexts and application types broadened. Computers are increasingly being used in the private and public spheres. Technology spreads from the workplace to our homes and everyday lives and culture [2]. New elements of human life are included in the human-computer interaction such as culture, emotion and experience [13]. Conceptually and theoretically, these HCI perspectives focus on the cultural level.

Within the usable security field, Whitten & Tygar's [16] definition and five properties of usable security have largely been defining the concerns thus far. They state that security software is usable if the people who are expected to use it:

1. Are reliably made aware of the security tasks they need to perform
2. Are able to figure out how to successfully perform those tasks
3. Don't make dangerous errors
4. Are sufficiently comfortable with the interface to continue using it

Furthermore they describe five problematic properties of the security domain:

1. *The unmotivated user property*–users will normally not attend to a system with security issues as their main task. Therefore they may not be motivated to do necessary security task.
2. *The abstraction property*–it-security policies and security mechanism may consist of abstract concepts. These abstract concepts can be hard to grasp for the users.
3. *The lack of feedback property*–hard concepts and the security configuration of the system can be very hard to communicate to the users.
4. *The barn-door property*–if the barn door is open and the horse gets out it is too late to close or improve the barn door. If a secret is revealed or if a back door is installed, it is too late to defense one self from that.
5. *The weakest link property*–a system is as secure as it's weakest link and the users may end up playing the role as the weakest link.

Both the definition, these properties and much of the everyday rhetoric in the area are concerned with making certain that users behave appropriately and that security issues are black-boxed away from users' misconduct and mistakes. The user is perceived as a cogwheel in the system, providing only the necessary action and information when such cannot be retrieved by the system itself. This is a good example of the passive user of HCI's first wave, discussed by Kammersgaard [11], the contrast to Bannon's human actor.

Evidently, both first and second wave HCI has ways of mending this limited perspective. Nonetheless we would like to suggest that research on usable security would benefit from third wave thinking, while still emphasizing the second wave perspective of users as actors. In particular we will look further at McCarthy & Wright's [12] perspective of technology as experience, while addressing usable security as experience (In line with Pagter & Pedersen [14]).

3. MOVING AHEAD

Our focus is dual: On the one hand we are concerned with how users experience security, e.g. the extent to which secure technology makes them feel more or less secure. On the other hand we are concerned with how security elements of technology as such adds to experiences of the technology, hence enhancing

the quality of the interaction; does it help engagement, enchantment, fulfillment or irritation (McCarthy & Wright's terms)?

In McCarthy & Wright [12]'s framework there is a close connection between the experience and the way human beings make sense. These two levels both help discuss the security experience as such and they help methodologically frame our study.

McCarthy & Wright investigates experience through four threads: compositional, sensual, emotional, and spatio-temporal. The compositional thread helps us address questions of how the security element of an experience fits into the coherent whole of the experience, and even if there are elements of the experience that may make people feel more or less secure. The sensual thread helps address how generally the technology adds to the feelings of the situation in general, in particular the feeling secure. E.g. this thread helps address what happens to the security experience when people are under e.g. time-pressure. The emotional thread helps address what emotions comes with the security element (e.g. fun, excitement or frustration), and even what emotions related to security does to the experience. The spatio-temporal thread relates experience to time and place, and relates the security experience e.g. to the difference between sitting at home with a computer versus being in a long line at an ATM machine.

When people make sense of experiences they do so through six interrelated processes: anticipating, connecting, interpreting, reflecting, appropriating and recounting. These processes emphasize how we prepare for experiences, and digest them by placing them into patterns of past experiences as well as we tell the experiences to ourselves and others. This framework emphasizes how to understand the security experience or the secure experience; we need to move beyond the narrow situation where the technology is used. While it is still necessary to capture use as it happens, to get the picture of conditions that make for particular actions, some of this as well as the experience processes are captured through users' immediate interpreting and reflecting, as well as through the surrounding processes of anticipating and connection, on the one hand, and appropriating and recounting on the other. This has consequences for the scope of our empirical investigations as well as for the methods needed in the investigation.

In order to further address the relationship between the security technology and its use, our starting point is in the fundamental dialectics between a technological artifact and its use [4]. On the one hand the artifact is designed for a particular use, and often determines (resists, constrains and directs) quite strongly how it may be used. On the other hand, the technological artifact is used according to the needs and intensions of the user. Gasser [9] documented how the use of even rather rigid computer applications develops beyond pure adaptation by the user, through workarounds. This means that even such computer technologies that strongly constrain use get transformed in use.

We capture and understand use as experience [12], and we concern ourselves with how, on the one hand, the use experience is determining the security technology, while on the other hand, the security technology resists, constrains and directs the use experience.

4. TOWARDS USABLE SECURITY

The background of this investigation is a project under the heading of IT Security for Citizens, which bridges between research competencies in HCI and security. In this project, we develop methods and concepts to analyze digital signature systems and security systems in a broad sense from the point of view of contemporary HCI. The project includes literature studies of usable security as well as empirical investigations and design work. This paper reports on fieldwork, targeting user experiences of and with security technology. We aim at improving security technology through our perspective and future efforts will be directed towards prototyping and evaluation.

5. THE STUDY

The particular study was set up to understand better users' immediate experience of security technology, as part of their everyday use of technology, be this at home or e.g. in the supermarket. We focused on user narratives, told by users while they happen or immediately after they interpreted the experience. Such narratives point to the experience, appropriating and recounting of user experience, while limiting the time frame and holding on to immediate surprises. The narratives were collected as semi-structured data through email and text messages. In analyzing the data we based ourselves on a grounded approach [5]. Users were found through an open invitation on the project website with additional active solicitation of friends of friends.

5.1 User Stories Collection

In total ten people signed up to participate. They volunteered to report back whenever they had anything to tell. This could be successes, failures, frustrations, or strategies they used or was requested to use. Users were asked to report their experiences through text messages (SMS), picture messages (MMS), text messages, pictures or video clips using e-mail, a voice mail answering service or through notes sent by surface mail. It was the thought that at least one of these ways would come natural to all users. It was important that users' efforts were minimal and the time was short from an observation occurred to it was reported. In addition they were warned that we would return for in depth interviews with some participants later.

Observations were collected for one and a half month. We received 41 observations. Of these 28 were text e-mail messages, 2 were screenshots via e-mail, and 11 were text messages via SMS. Some participants were very active and one did not report anything at all. Some of the observations were triggered by interactions at point-of-sales counters, some by interactions at the participant's personal computer, and others were placeless statements or wonderings.

5.2 User Stories Analysis

The observations were inserted in a spreadsheet and tagged with the observer's ids, times and dates of reception, and the ways users reported the observation. Afterwards they were tagged with several tags dependent of the type of observation and what the observation was about. In particular we focused on identifying technology that determine the use experience or use experiences that determine the use of technology.

6. SECURE INTERACTION?

Many of our observations are narratives about systems that one may define as usable secure. Still the participant chose to report these observations as concerns over security. Defining a system usable secure according to Whitten & Tygar's definition requires that the users behave securely which they most often did in the following examples.

"[...] how irritating it is when a website that I rarely use is protected by password. Especially the Danish tax authorities self-

service web site. I only use this web site once a year and I never remember what password I chose a year ago [...]"

Most citizens in Denmark only communicate with the tax authorities once a year when they do their final taxes for the past year. Every citizen receives a tax form stating what they have earned, and paid in tax. This is an invitation to correct the figures and to add e.g. deductions. For many years it has been possible to make this correction through a self-service website using ones social security number and a password of the citizen's own choice. One may order a new password through e-mail, in which case one receives a one time password, which should be changed immediately after log-in. Hence, while users may not actually remember their password, this causes annoyance and uncertainty, but does not constitute a dangerous error according to Whitten & Tygar's definition this system is usable secure.

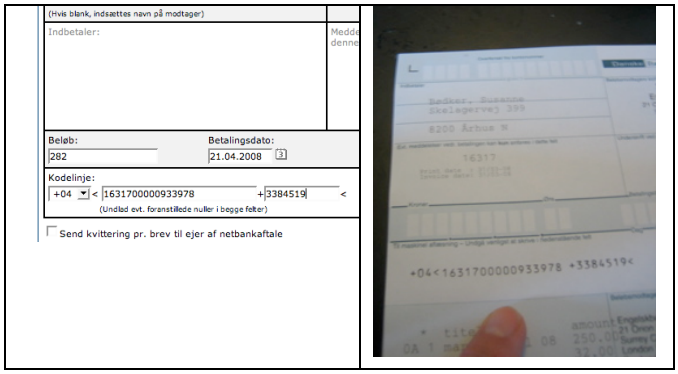

Fig. 1. Typing digits into home bank (giro form right and bank web left)

"[...] I used home banking to do a payment. Every time I do such a task I have this insecure feeling that I mistyped some digits [...]"

It is usual for Danish citizens to receive postal giro forms for various payments (Fig 1). You may choose go to a bank and they will scan the giro form to read the exact digits identifying the receiver, the customer and the payment. Or you may use home banking to avoid physically going to the bank during their limited opening hours. In home banking, the only way to identify the receiver, the customer and the payment is to type in three very large numbers. Mistyping one single digit will send the payment to another receiver or tell the receiver that the money came from another customer. Despite this, most customers actually manage to type the right digits, often because they check the numbers twice. According to Whitten & Tygar, home banking can be seen as usable secure. Nonetheless, many customers are left in doubt that they typed in the right digits, and hence paid the right receiver the right amount of money.

"[...] I went to a toy store to buy a game paid with a credit card. The sales clerk told me to use the chip on my credit card, but to sign a slip instead of typing my pin code. I swept my card through the normal machine! First I was worried, I mean, it should be the same in any store, but the store belongs to a big chain and it did not seem to matter if my payment was enabled by a knuckle buster or not."

Normally the procedure for paying with a credit card is to 1) Insert a credit card 2) Type your 4-digit pin code 3) Acknowledge the amount of money 4) Remove your credit card. When the terminals are offline they cannot contact the server and check the pin-code so one has to sign a slip to confirm the payment and prove the ownership of the credit card. Earlier generations of the terminals would not work if they were offline. Stores used a card imprinter to take an imprint of the card's serial number. This imprint one could then sign. This way customers pay without dangerous errors and they can continue using their credit cards despite the breakdown. Hence, according to Whitten & Tygar, we may consider the credit card payment system usable secure.

"I just found out that you can freeze your home banking account […] if one suspect misuse–smart–weird that they [the bank] don't make you aware of that."

People like to know that if they get too worried they can always pull the plug. To know that one can actually freeze one's account may determine how one feel about using home banking. One may argue that, according to Whitten & Tygar, the user needs to be reliably made aware of that. But another argument may be that freezing one's account is not a task one needs to perform [16].

"I often forget to log off when I visit web sites that require a password. But actually I do not understand why one has to. If I leave the website for 5 seconds and then return I have to log in again. […]"

Users may access password-protected websites from different computers, locations and contexts. Websites that use password protection may rely on the login as a proof of authentication and authorize the user to do restricted tasks. To prevent hijacking of the authorization, the website encourages it users to log off when the authorization is no longer needed. One may argue that the user makes an error in forgetting to log off, but one may just as well argue that this is not a dangerous error, and accordingly the website is usable secure.

All of these accounts talk about experiences where the participant actually behaves securely and as prescribed and still ends up feeling annoyed, without control, without overview of what is happening to them, i.e. not having a secure experience. In some instances, such as the logon and logoff to websites, the actual security technology added to their uncertainty, in the postal giro example it is the strain of actually "playing machine" duplicating the digits that make users feel unsecure. The password example illustrates that usable security reaches beyond the here and now. The example with the freeze feature of the home banking shows that you can actually design for improving the experience with just a little more effort. And in the toy store example we see that people immediately compare experiences with similar experiences to get an idea of what is going one. The unclear link between the present experience and other similar experiences makes the customer worry.

With these conclusions in mind it is evident that a framework helping focus on security as part of a wider experience is necessary; wider, both in terms of history and background experience, and the situation at large. Even though our data was gathered to focus on instances of security incidents, the above conclusion actually points out that we need to know more about the context to understand the role of security in interaction. The data give us hints of such context, but barely more than that. While the many ways of sending messages support immediate reactions to experiences that called for a security concern, these messages only scratched the surface both as regards the actual setup and conditions that triggered the experience, and the depth of the experience in terms of the full experience process.

7. THE SECURITY EXPERIENCE, THE SECURE EXPERIENCE

To challenge our conception of what is needed empirically and analytically, we turn, for a while, to two experience accounts, from our personal lives.

The first account comes from Palen & Bødker [15] who analyzes Susanne's experience.

"Susanne remembers:

Not long ago, I went to friends' for dinner. It was quite a long drive, and on the way there I remember thinking—do I need gas? No, no, I would probably make it.

On the way back, at almost midnight, I decided to stop for fuel anyway. Off the highway and into the nearest town I went. At the major road crossing was a gas station. It was quite deserted, but I was pleased to see it. I pulled up, took out my credit card and went out to punch in my pin-code and open the gas tank. "Please insert the card"—I did—a pause—"This card cannot be read." I tried to turn the card, but that did not help. Who cares?, I thought, I've got more cards! I inserted another card, and the same happened. Now I started to worry—what had happened to my credit cards? Did I have cash? No. Could I make it home without extra gas? Oh misery!

I decided to move the car to the pump behind me as a last attempt to identify if it was the card or the pump causing the trouble. And I still negotiated with myself whether I could make it home. Somehow the new gas pump did not share the problem—it read my card, and asked for the pin-code. What a delight! There was no problem with my cards, and I would not be stranded on the freeway in the middle of the night! I fuelled the car while another car pulled up across the aisle. An elderly couple —who given the way they talked, were on a date, they weren't married— got out and the woman offered to use her card. That was not accepted by the machine either, and they started to futz about "doing things right." At that point, I had gotten my fuel, and I felt that I could help out by telling them that I had problems too. Somehow, the man's card worked. So in the end, it probably wasn't because I moved the car that the problem resolved; rather it seemed due to some sort of periodic error in the payment system."

Palen & Bødker [15] point out that based on Susanne's experience (and the couple's lack of it), she "read" the situation differently from the couple. They thought they made a mistake, whereas she had ruled that out because of earlier problems with credit cards. However, Susanne's experience was not made better with the dark night, the risk of being stuck along on the freeway, the deserted space, i.e. the spatio-temporal and sensual threads of experience (McCarthy & Wright [12]), adding to the emotional thread of first frustration, then relief. However, the main cause of frustration was exactly the rejection of first one, then two credit cards, i.e. the security system. Security played a further role as a backdrop emphasizing the frustration: Due to Susanne's past experiences she was uneasy with the credit cards actually working, even though she knew there should be nothing wrong. However, due to the time, place and desertedness of the place, no alternatives and no help were to be expected which in itself made the situation feel less secure. If we look at the compositional thread running through this experience, the initial rejection of the credit card (secure behavior according to Whitten & Tygar [16]) colored the experience in many ways: There was no help, alternatives or even workarounds available. Only due to Susanne's past experience did she try an alternative in the form of a different gas pump. The elderly people, on the other hand, were ready to convince themselves that they made a mistake. The behavior that really fitted with the security would in both instances only have lead to not filling the gas tank, and hence, potentially, a different type of security risks: being stuck on the highway at midnight.

Niels has a natural interest in experiences related to security, and here is one of his recollections:

Some years ago my girlfriend went to Budapest with some fellow students from the university. We planned for me to join her on an extended trip. The students had already bought their tickets on the Internet from some discount airline. The tickets were very cheap when they were booked early. Everyday one hesitated to buy the ticket the price raised a little. This put a lot of pressure on me to act quickly.

Hence, I went ahead and bought the ticket. I supplied my credit card number, expiration date and security number as you do with such payments on the Internet. I also gave my full name as stated in my passport, as demanded by airline security.

The only confirmation I received was a stream of e-mails advertising other cheap flight tickets. Some days later I found an entry in my bank account informing me that I paid the airline company. Days later again, I found a similar entry informing me that I paid the once more. First I felt irritated that the booking system didn't work; then I felt upset that I had to spend time correcting the mistake. I went to the airline company's website and found that the only way to contact them was via e-mail. I could not find any surface mail address or telephone number and I started to worry. Had I been fooled? Did the airline company actually exist? Would I get my money back? Had I booked a trip to Budapest? I wrote them an e-mail explaining the problem in a polite manner. The next days I received no answer or acknowledgment of my e-mail. I spent plenty of time speculating why I bought at ticket from this company. Some days later I received a very brief answer explaining that the airline company's booking systems was flawless. Even paying the double price, it was still an affordable vacation so I decided not to take the problem any further. However, I was still worried if the infallible system had registered my booking at all. Some months later I had a nice and unproblematic trip to Budapest.

In this example, Niels' trust in his friends who ordered the original tickets, and the urgency of the situation, caused him to ignore many aspects that he would otherwise be concerned with, e.g. whether the web shop had a physical address. In this way Niels did indeed demonstrate insecure behavior, even though his interaction with the "flawless" website as such was secure. However, this type of secure behavior did no prevent the double payment.

Niels' calmness when this happened was mainly due to the low price of the ticket even when it turned out that the airline did not acknowledge the double payment. Would there be a price limit where Niels no longer is so calm? Would this price limit be influenced by the relative price of other travel possibilities? How much he cherished the purchase as such and was looking forward to the trip? And in retrospect: how nice the trip actually was?

The final element of Niels' experience is related to his reservation as such, and the lack of feedback from the booking system. From past experience Niels expect that when he paid a company some money they would either provide something in return or send the money back. So normally an entry on his bank account would be

appropriate feedback. In Niels' situation this kind of feedback had failed, no other feedback was provided, and the company did not regard this as a problem. Of course this left Niels with serious worries if the flight had ever been booked.

The compositional thread helps us address questions of how the security element of an experience fits into the coherent whole of the experience, in this case, how the lack of physical address and of feedback from the booking system. These dominated the experience as such for Niels. The sensual thread addresses the issue of time-pressure, as well as Niels' dependence on friends having booked similar tickets. The emotional thread was dominated by the expectation of a nice trip and the cheap price. The spatio-temporal thread helps focus on the distance and lack of physical address of the airline, as well as the slow email response and time distance from the booking to the departure of the trip.

To identify security technology experiences in the original empirical material, we need a more detailed and complete narrative than the immediate, prompted responses of our empirical investigations. It would be interesting to learn if our participant felt that the Danish Tax Authorities was burdening him with this correction work or if he actually felt it was for him to do? It would be interesting to know if our home banking users ever had, or had heard of any one who actually had, problems after mistyping digits or who actually needed to freeze their account? Our participant that went to a toy store refers to other stores. What were really the experiences with this and other stores that made her experience this alternative procedure as secure? And likewise, it would be interesting to learn how our participant, who forgets to log off, regards the resources she was authorized to use.

Nonetheless, the examples illustrate certain ways in which the security technology experience gets influenced. First of all, the added work of retyping digits, remembering and rewriting passwords seems to overrule the general experience and indicates a lack of compositional balance. The emotional judgment, of who you do business with, overshadows the real concerns for security. The spatio-temporal thread matters to the concerns for remembering passwords, and in judging the security of the store. We are curious to understand why one of the home bank users thought it comforting and secure to realize that you could freeze your web bank? This may have many interpretations, but the immediacy is mainly sensual, however, and could well result from earlier panic in similar situations. To support the home banking user's secure experiences, changes should be made in the design of the situation: 1) The home bank should be accessible only when a specific mobile phone is in the vicinity of the computer used for home banking. In this manner, the user is able to freeze the account just by leaving the computer while bringing the mobile phone. 2) Instead of typing in digits, the bill that one wants pay could be chosen from a list. Immediate feedback of which bills have been paid should be visible. If Niels had bought his ticket in a way like this, he probably would have avoided some of his uncertainty.

8. DISCUSSION

Our examples illustrate that being secure by behaving securely towards a security dependent technologies, and feeling secure and experiencing a secure interaction leads rather different ways analytically and designwise.

Addressing security technology as experience means addressing important elements of context, connection between security and use situation in general, history, and background from a process perspective. The perspective points out how security cannot be seen in isolation from time, place, emotions, experiences, purpose of the interaction as such, other actors, etc. Compositional balance turns out to be important. The extent to which security may be allowed to dominate the experience depends e.g. on the amount of money at stake as in Niels' case. With this approach we suggest to study further e.g. what role e.g. the size of a payment plays to the compositional balance. We have demonstrated how the general sensual (both positive and negative) and the emotional (e.g. relating to people involved) aspects have a tendency of overshadowing the security experience. Again, it is interesting to pursue further how these sensual and emotional elements may be matched–can security be fun as part of a generally funny experience? Serious when seriousness is needed? As regards the spatio-temporal, it seems no good to provide a slow security experience as part of something that may otherwise happen rapidly. All of these are discussions that need to be developed further to fully utilize the experience framework in designing for security.

However, we are at risk of throwing the baby out with the bathwater, and hence, one may ask what is lost if only applying the secure experience perspective? Turning away from the first wave perspective means to abandon the idea of designing for a secure behavior. Is it possible to rethink, in terms of experience, the challenges from first wave HCI and the challenges that Usable Security Research Field already addresses? User's behavior may be determined from how they connect to a situation and their continued use may depend on how they recount the experience. If errors happen it may be due to how the users anticipate the erroneous experience, and recovering may depend on how the users reflect on the experience. Evaluation of applications, patterns and guidelines may inform our experience approach, but they have to be rethought.

Our method for collecting and analyzing user experiences emphasized situations where our participants behaved securely and somehow also managed to carry out security dependent tasks. Still they experienced the situations as e.g. insecure, problematic, or annoying. While these immediate stories helped us see this, they were not complete enough to actually fully analyze why. However, analyzing use experiences, applying McCarthy & Wright's four threads, helped focus on this wider situation. Collecting user stories as we did is but a first step in such analysis. We learned from this analysis that further interviewing our participants, asking them to recount their experiences, is needed. Semi-structured interviews can help explore how our participants anticipate, connect, interpret, reflect, appropriate and recount secure as well as insecure experiences. Such interviews may be connected e.g. with critical incident techniques, and use of more elaborate diaries.

9. CONCLUSION

Surely the security domain brings new challenges to HCI. Challenges of experience design, mixed context and more. Still we found examples in everyday users life that may benefit from the results of contemporary HCI research. We also shown examples that the research in the community of Usable Security is inspired by first wave HCI and lack in taking second and third wave HCI into account. Especially our focus on experience shows how to analyze security dependent use situations on a more complete basis. By applying McCarthy and Wright's framework on our examples we opened a way to improve security. We found that behaving securely in a situation not necessarily leads to expe-

riencing the situation as secure. Through user narratives, one could get an insight into users immediate interpretation of a situation. Future research concerning use of security technology artifacts should focus on the secure experience.

10. ACKNOWLEDGMENTS

ITSCI is a project financed by the Danish Strategic Research Council (NABIIT). Ivan Damgaard manages it. Our thanks to Ivan, the industrial partners in the project, the project group (Kaj Grønbæk, Marianne Graves Petersen, Gert Mikkelsen), as well as Clemens Klokmose and Pär-Ola Zander for valuable discussions.

11. REFERENCES

[1] Bannon, L. (1986). From human factors to human actors: the role of psychology and human-computer interaction studies in system design. In Greenbaum, J. & Kyng, M. (eds). Design at work: cooperative design of computer systems, pp. 25-44, Erlbaum.

[2] Bertelsen O. W. (2006). Tertiary Artefactness at the Interface, In Fishwick, P. (ed). Aesthetic Computing, pp. 357-368, MIT press.

[3] Bødker, S. (2006). When second wave HCI meets third wave challenges. In Mørch, A. Morgan, K. Bratteteig, T. Ghosh, G. & Svanæs, D. (eds.): Proceedings of the 4th Nordic Conference on Human-Computer interaction: Changing Roles, pp. 1-8. ACM Press.

[4] Bødker, S. (1999). Computer applications as mediators of design and use - a developmental perspective. Doctoral dissertation, Department of Computer Science, University of Aarhus, DAIMI PB-542.

[5] Corbin, J. & Strauss, A. (1990). Basics of Qualitative Research: Grounded Theory Procedures and Techniques. SAGE Publications, London, 1990.

[6] Danish IT security Council: Pervasive computing – IT security and privacy, http://www.brics.dk/~michael/articles/rfits-uk.pdf

[7] DiGioia P. & Dourish, P. (2005) Social navigation as a model for usable security. Proceedings of the 2005 symposium on Usable privacy and security, pp. 101-108.

[8] Flinn, S. & Lumsden, J. (2005). User Perceptions of Privacy and Security on the Web. Proceedings of the Third Annual Conference on Privacy. http://www.lib.unb.ca/Texts/PST/2005/pdf/flinn.pdf

[9] Gasser, L. (1986). The integration of computing and routine work. ACM TOIS 4(3), 205-225.

[10] Hardee, J. B., West, R., & Mayhorn, C. B. (2006). To Download or Not to Download: An Examination of Computer Security Decision Making. Interactions Magazine 2006 May-June, 32-37.

[11] Kammersgaard, J. (1988). Four different perspectives on Human-Computer Interaction. International journal of Man-Machine Studies, vol. 28, pp 343-362.

[12] McCarthy, J., & Wright, P. (2004). Technology As Experience. The MIT Press.

[13] Norman, D. A. (2002). Emotion and design: Atrractive things work better. Interactions Magazine, ix (4), 36-42.

[14] Pagter, J. I. & Pedersen, M. G. (2008) A Sense of Security in Pervasive Computing-Is the Light on When the Refrigerator Door Is Closed? LNCS pp. 383-388. Springer, Heidelberg.

[15] Palen, L. & Bødker, S. (2008). Don't Get Emotional. In: Peter C., Beale R. (eds.): Affect and Emotion in Human-Computer Interaction. LNCS, vol. 4868, pp. 12-22. Springer, Heidelberg.

[16] Whitten, A & Tygar, D. (1999). Why Johnny Can't Encrypt – A Usability Evaluation of PGP 5.0. In Cranor, L. & Simson, G. (eds). Security and Usability: Designing Secure Systems that People Can Use, O'Reilly (2005), pp. 679-702.

[17] Yee, K. 2002. User Interaction Design for Secure Systems. In Proceedings of the 4th international Conference on information and Communications Security (December 09 - 12, 2002). In Deng, R. H., Qing, S., Bao, F. & Zhou, J. (eds.) Lecture Notes In Computer Science, vol. 2513, pp. 278-290. Springer-Verlag, London.