Investigating how everyday people experience security

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

1. INTRODUCTION

In this paper I propose a method for analyzing everyday people's experiences with IT-security. I furthermore report how I applied the method. The proposal is motivated by work of other researchers and their efforts to get beyond secure behavior, and to get an insight in secure or insecure experiences that everyday users of technology encounter. The background for introducing this method 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 sensible 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 my method to target user experiences of and with security technology.

2. FROM SECURE BEHAVIOR TO SECURE EXPERIENCE

Successful use of security protocols and strong encryption has made hackers direct their attacks towards users and users' interaction with systems. Research came up with ways to enforce, encourage, or help users behave more securely. Whitten and Tygar [8] also define security software as secure if the intended users behave appropriately[i]. To define a system as secure one has to find out if the users behave in the right way. Studies on how users actually behave, have been carried out and the results published (e.g. [8]).

Smetters and Grinter [7] identify 3 approaches from usable security community to improve the usability of security software: (1) improve user education, (2) improve existing GUIs, or (3) built new system from the ground with usability as the primary focus. They emphasize that it is important to improve the usability and the security of software in general, and not just security software. Furthermore they propose 3 ways of usability testing[ii]: (a) collect logs of use, (b) observe users in actual security sensible use situations, which are identified through contextual inquiry, or (c) analyze situations where security is an aspect without asking questions about security directly. Smetters and Grinter Further suggest that we broaden our focus from security software (e.g. encryption application, firewalls) to any application. E.g. most applications run on some network connected machine and involve data that you do not want to share or loose. Dourish et al. [2] address this, arguing that a feature of ubiquitous computing is spontaneous ad hoc networking, which raises a number of security and privacy issues for end-users. Bødker [1] identifies the new challenges to HCI research with what she calls third wave challenges. Use of technology is no longer limited to a specific context like a work setting. Use originating from spare time is now and then interleaved with work related use. Likewise, security and the sense of it are not bound to a work or a home setting.

Dourish et al. [2] emphasize that the security technologies must be highly visible – available for inspection and examination. Instead of hiding it away or making it "transparent" security tasks and the feedback of the security state should seamlessly fit in with interactions with technology. Thus it should not be expressed as the technical terms originating from e.g. encryption but in terms originating from the users' conception of security.

Beyond designing for usability and secure behavior is designing for a secure experience. Smetters and Grinter [7] briefly mention the importance of a *positive user experience*. Grossman [3] explains why users may not feel secure when encountering security mechanisms. He criticizes that existing systems are based on the military principle: "Need to know"–every user is told exactly what is necessary and no more. In the military, this principle enforces a hierarchy of control. Accordingly he claims that people feel insecure when they experience not being in control. Pagter and Pedersen [6] address the *sense of security*. They carry out a case study on how to improve hotel guests' sense of security. Their starting point is empirical material collected by the artist Sophie Calles, when she worked as a maid in a hotel during a three weeks stint. From their empirical material they identify a sense of security, which they describe as the feeling one has when one asks: Is the light on when the refrigerator is closed?

McCarthy and Wright [5] propose a framework for analyzing experiences with technology. The framework describes experiences through four threads: Compositional–how an experience is conceived as a hole, sensual–ones pre-reflective impression (first-hand impression), emotional–the summarizing value judgment, spatio-temporal –how time and place influence an experience. It furthermore describes six sense-making processes that users perceive an experience through: Connecting, interpreting, anticipating, reflecting, appropriating and recounting. Appropriating is the process of comparing an experience with other experiences one has previously had. So to get a grasp of one experience, one appropriates it with other experiences. Recounting is the process of creating a decent explanation or story of an experience. Recounting is when one clarifies to either one self or others why one reacted as they did.

Symposium On Usable Privacy and Security (SOUPS) 2008, July 23-25, 2008, Pittsburgh, PA, USA.

3. HOW USERS APPROPRIATE AND RECOUNT SECURITY

I propose a new method, the purpose of which is to inspect what everyday people experience as related to IT-security in their everyday life. It inspects how people appropriate and recount IT-security experiences. In order to do this I suggest to record user stories immediately upon encounter. This method ensures that it is everyday situations that actually happen that is recorded and avoids depending on informants' sporadic memory (e.g. like the interviewer has to when interviewing). Furthermore, this method can inspect the informants' immediate experience of security technology, as part of their everyday use of technology, be this at home or e.g. in the supermarket. By letting informants choose what to report this method gets beyond the problem that comes a long with observation studies and interviews. Observation studies are limited to contexts in which the user is observed. Interviews are likewise limited even though semi-structured interviews can make the interviewee remember situations from other contexts. Letting the informants choose the recordings from whatever situation lets the analyst record data not only for analyzing security software, but also for analyzing use of any technology, which the user connects with security. With this method only situations involving non-transparent security technologies will be captured.

3.1 Applying the method

As part of the initial phase of an iterative design process aiming at offering digital signatures to every citizen in Denmark in a usable, mobile and secure way, I applied this method in collaboration with Susanne Bødker. We announced a need for informants and ten arbitrarily chosen people volunteered to participate. They where instructed 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 the users' efforts were minimal, and that the time from an observation occurred till it was reported was short. 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. The data analysis and the results are reported in [4].

4. CONCLUSION AND FUTURE WORK

The main contribution is the proposed method and the report of the successful application of the method. Furthermore, I emphasize the need for investigating secure and insecure experiences. Future work should engage more informants, new ways of recording user stories according to this method, and new applications of the method. Results of future data analysis should inform analysts' future investigations or interviews, and future designs of new security sensible systems.

5. ACKNOWLEDGMENTS

ITSCI is a project financed by the Danish Strategic Research Council (NABIIT). It is managed by Ivan Damgaard. I thank Ivan, the industrial partners in the project, the project group (Susanne Bødker, Kaj Grønbæk, Marianne Graves Petersen, Gert Mikkelsen), as well as Clemens Klokmose and Pär-Ola Zander for valuable discussions.

6. REFERENCES

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

[2] Dourish, P., Grinter, E., Delgado de la Flor, J., and Joseph, M. 2004. Security in the wild: user strategies for managing security as an everyday, practical problem. Personal Ubiquitous Comput. 8, 6 (Nov. 2004), 391-401. DOI= http://dx.doi.org/10.1007/s00779-004-0308-5

[3] Grossman, J. 2006. Feeling secure. interactions 13, 3 (May. 2006), 50. DOI= http://doi.acm.org/10.1145/1125864.1125892

[4] Mathiasen, N. R. and Bødker, S. Threats or threads -from usable security to secure experience? (in preparation).

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

[6] 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.

[7] Smetters, D. K. and Grinter, R. E. 2002. Moving from the design of usable security technologies to the design of useful secure applications. In Proceedings of the 2002 Workshop on New Security Paradigms (Virginia Beach, Virginia, September 23 - 26, 2002). NSPW '02. ACM, New York, NY, 82-89. DOI= http://doi.acm.org/10.1145/844102.844117

[8] Whitten, A. & Tygar, J. D. Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In 8th USENIX Security Symposium, pages 169 -- 184. Usenix, 1999.

[i] Tygar and Whitten 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" [8]. To check if some system adheres to (1) – (4) one should inspect system users' behavior.

[ii] These three ways are more generally three ways of bringing users into the design process than it is testing.