Understanding human need fulfilment to support the design of secure experiences

Verena Distler
University of Luxembourg
Esch-sur-Alzette
verena.distler@uni.lu

ABSTRACT
Technologies are taking an increasingly important and ubiquitous place in our lives. Security concerns are thus becoming even more crucial and pervasive, but usability issues of security artefacts often lead to security breaches. While the field of usable security strives to address this problem, these efforts have been criticized for trying to modify users' behavior to act in a more secure way. Some have concluded that there is an inherent trade-off between usability and security, however, other studies have indicated that security might enhance user experience if approached in a user-centered way and in accordance with user values and needs. Indeed, security is a crucial need in human needs theories whose fulfilment has been shown to contribute to positive experiences. This PhD project will take the position that security can contribute to human needs fulfilment and to a positive User Experience. We will strive to understand human need fulfilment when using technologies in different contexts (e.g., autonomous vehicles on demand, eVoting) and aim at contributing to the design of secure experiences which are aligned to users' values and needs.

Author Keywords
User Experience; Human Needs; Security; Privacy.

ACM Classification Keywords
H.5.m. Information interfaces and presentation (e.g., HCI): Miscellaneous;

INTRODUCTION
Technologies are increasingly pervasive in our everyday lives. The relevance and scope of security and privacy infractions thereby increases. While privacy refers to the ability of individuals to maintain control of their personal information [13], security is a broad term which can refer to personal security, physical security, and computer security [6]. Pieters' definition of security refers to the limited effects of an attacker trying to make a system fail [9], which is in line with many traditional definitions of computer security which is often thought of as software security mechanisms like passwords or encryption [6]. However, in UX Design, perceived security is defined as feeling safe and in control of your life, rather than feeling uncertain and threatened by your circumstances [4]. Maslow [5] defined security and safety needs as the second most important needs after physiological needs, also highlighting that the need for security and safety translates differently for each individual. It is also noteworthy that privacy and security are highly context dependent, as pointed out for example by Palen and Dourish [8] who define privacy as "the continual management of boundaries between different spheres of action, and degrees of disclosure within those spheres.". The authors highlight that these boundaries move dynamically with changing contexts.

Various efforts have been undertaken to improve privacy and security, namely in the field of usable security. Yee [15] created guidelines for usable secure systems, and Whitten and Tygar [14] have pointed out five problematic properties of security, such as the unmotivated user property (security as a secondary goal) or the weakest link property (the security of a computer is only as strong as its weakest component). They underline that security mechanisms are only effective when used in a correct way.

The field of usable security has been criticized for taking a techno-centered approach, focusing mainly on adapting user behavior to behaving securely (e.g., [2]). Moreover, blaming users to be "the weakest links" when a security breach occurs is a frequent and bad practice [11]. As Gollmann et al. state [3], if users are left to be weak points in a system's functioning, the system interfaces with its users in an insecure way and violates basic principles of psychology and security economics. Security has often been found to be an obstacle to users' goals due to unusable interfaces, which has led some to conclude that there might be an inherent trade-off between usability and security. However, others explain these "usable security" problems with a mismatch between the values that security experts believe users to have, and their actual values, sometimes

This work was selected for presentation at the NordiCHI'18 Doctoral Consortium, September 29, 2018.

leading to useless, counter-productive or harmful security artefacts [2].

Mathiasen and Bødker [6] demonstrated that in situations which might be considered usable secure according to Whitten & Tygar [14], meaning that the participant behaves in the intended, secure way, they might still end up feeling annoyed and in lack of control. Even though the situation can be considered "usable secure", they are not having a secure experience. In their study, in certain some instances, the security technology added to users' uncertainty. This is in line with Dodier-Lazaro et al. [2] who criticize the paternalistic character of many usable security initiatives, and point out the aforementioned discrepancy between how security is valued by security experts and how it is valued by users. They state that security mechanisms must respect users' values (e.g., costs, productivity, credibility). Pagter & Petersen [7] were among the first to look beyond the usability of security artefacts, and studied the experience of security of hotel guests. They introduced the concept of falsifiable security, where users can double-check if the situation is secure, an action which might be seen as an equivalent of double-checking locking a door. They point out that security can be an enabling factor and a significant part of the experience which is provided to people.

The experience of security is not only system-related, but context-dependent and user-related factors play a role. User Experience (UX) helps us address all of these facets of security, given that it allows for understanding user, context and system-related factors of experiences. UX also enables us to look at problems through the lens of psychological need fulfilment which has been shown to be a driver of positive experiences [4]. Perceived security and control is one of the most important human needs [12], and it therefore does not come as a surprise that creating experiences that, amongst others, also fulfil the need for security and control might be perceived as positive.

We adopt a broad definition of security, which includes contextual, user-related and system-related factors. We posit that security mechanisms can improve the UX of systems. We will study how security can contribute to a positive UX and "secure experiences" by taking a human needs centered approach, while also taking into consideration contextual and system-related factors.

RESEARCH OBJECTIVES

In this PhD project, we will view security as an enabling factor with the potential of providing even more positive experiences if security contributes to human need fulfilment. The objective of this PhD project is thus twofold:

Our first objective will be to understand users' need fulfilment when using security-relevant technologies in various contexts (e.g., eVoting and autonomous mobility on demand). We will place a particular focus on the need for security and control.

Secondly, by understanding psychological need fulfilment when using technologies, we will aim at better aligning security to users' needs and values in the objective of creating positive secure experiences.

1) EXPLORATORY STUDIES: EVALUATING HUMAN NEEDS AND ACCEPTANCE FACTORS IN VARIOUS CONTEXTS (SMART THERMOSTAT, EHEALTH RECORDS, SOCIAL MEDIA, OFFICE SURVEILLANCE)

This phase of the PhD project has the objective of exploring the link between human needs and acceptance factors in the context of privacy and security-relevant technologies. The results will serve as a base for addressing human needs fulfilment in the contexts described thereafter.

We conducted a first study (under review) which explores factors that influence privacy trade-offs in different use contexts. We used four scenarios (derived from [10]) which describe situations with potential privacy trade-offs, namely office surveillance cameras, smart thermostats, social networks and online health platforms. In each scenario, our participants were confronted with a situation where a technology might provide them with potential benefits in exchange for privacy or security shortcomings. By conducting eight focus groups with 32 participants, we found out that the factors influencing the acceptability of privacy trade-offs go beyond security and privacy. The feeling of control over the data shared had an important impact, as well as perceived usefulness, previous experiences and voluntariness of use.

Ongoing studies also include an online questionnaire which will use the aforementioned scenarios with the objective of reaching a more international audience. Beyond evaluating the acceptability of these scenarios, we will include technology acceptance items and study the influence of psychological needs on the acceptability of the privacy and security trade-offs.

2) UNDERSTANDING PERCEIVED SECURITY AND CONTROL OF ENCRYPTION PROCESSES IN THE CONTEXT OF EVOTING

The overarching goal of this study is to understand how different visualizations of cryptography can influence human needs fulfilment, with a focus on the need for security and control. This work has a three-fold aim.

The first objective will be to understand users' security-related values and awareness of security threats in the context of eVoting. For this purpose, we have conducted four exploratory focus groups with 16 participants, which evaluate the contextual acceptability of eVoting (e.g. in the context of municipal elections, regional elections, national elections), general opinions of eVoting and voting in general, and the awareness of security threats.

Secondly, we will strive to understand the impact of varying levels of transparency of the encryption process on the need of perceived security and control. We will create different versions of a prototype of an eVoting application,

with varying levels of transparency of the encryption process for the user. The encryption might for example be completely automated and invisible to the user. On the other hand, the encryption process might also be more visible to the user, and require some interaction. We will conduct user testing with approximately 10 users per condition (encryption is invisible, encryption is slightly more visible, encryption is highly visible). Our objective will be to understand the impact of the varying levels of visibility of encryption to the user's need fulfilment, and in particular on perceived security and control.

The third objective of this study will be to explore how to best align the actual (expert-evaluated) security and user-perceived security of the application. We will be closely collaborating with a team of cybersecurity experts and cryptographers in the eVoting domain who will provide us with the necessary insights to assess the "actual" (expert-evaluated) security at each step of the voting process. Comparing the user-perceived security (as studied in the previous step) and the expert-evaluated security, we will be able to iteratively adapt the design of the eVoting application in order to align user-perceived security to the actual security. We will then conduct user tests of this new eVoting application prototype.

3) UNDERSTANDING PERCEIVED SAFETY AND CONTROL IN AUTONOMOUS VEHICLES ON DEMAND

This study's objective is to understand the perceived security and control when using autonomous vehicles.

We have conducted a first study [1] on the acceptance of Autonomous Mobility on Demand (AMoD), where we first evaluated acceptability of AMoD (before having used it), and then we placed participants in a realistic AMoD experience. After this first use of AMoD, we again evaluated their (after-use) acceptance of AMoD. We have found out that the psychological needs, and specifically the need for security and control, play an important role for users when they evaluate the acceptance of an autonomous vehicle along with pragmatic factors. This opens up room for new questions regarding the specific needs that have to be fulfilled in the context of AMoD in order to create a secure experience which is aligned to users' values (e.g., efficiency).

At present, we are evaluating different collaboration possibilities with manufacturers of autonomous vehicles and shuttles, and we can therefore not provide any details on the vehicle used yet. Similar to the aforementioned study, we will place participants in a realistic AMoD experience with the goal of understanding their perceived security and control before, during and after the ride. An interesting aspect of this study lies in the relevance of physical security (safety) in the context of autonomous mobility, which is linked to the software security of the vehicle. To the best of our knowledge, no studies on the human needs fulfilment in this specific context of autonomous mobility exist, and we hope to contribute to closing this research gap. As a result of this study, we hope that we will be able to make design recommendations for AMoD, with the objective of creating a secure AMoD experience which responds to users' needs and corresponds to their values.

CONCLUSION

Usability issues of security-relevant technologies lead to security breaches. In this PhD project, we will go beyond the techno-centered approach often used in the field of usable security. Instead of trying to adapt the users' behavior in order to make them act in a more secure way, we take a step back and adopt the stance that security might actually enhance user experience and help address user needs. We will strive to understand human need fulfillment when using technologies in contexts such as eVoting and autonomous mobility on demand. Our objective will be to (1) understand human need fulfilment when using various security-relevant technologies (2) better align security to users' needs and values in the objective of creating positive secure experiences. Our contributions will include theory building on factors influencing human need fulfilment when designing secure experiences. On a methodological level, we will contribute to the development of methods aimed at evaluating psychological need fulfilment when using security artefacts. The pragmatic implications of our work should include recommendations which inform the design of secure experiences.

REFERENCES

[1] Distler, V., Lallemand, C. and Bellet, T. 2018. Acceptability and Acceptance of Autonomous Mobility on Demand: The Impact of an Immersive Experience. (2018), 1–10.

[2] Dodier-Lazaro, S., Sasse, M.A., Abu-Salma, R. and Becker, I. 2017. From Paternalistic to User-Centred Security: Putting Users First with Value-Sensitive Design. *Workshop on Values in Computing. 09 May 2017* (2017), 7.

[3] Gollmann, D., Herley, C., Koenig, V., Pieters, W. and Sasse, M.A. 2015. Socio-Technical Security Metrics (Dagstuhl Seminar 14491). *Dagstuhl reports*. 4, 12 (2015), 28.

[4] Hassenzahl, M., Eckoldt, K., Diefenbach, S., Laschke, M., Len, E. and Kim, J. 2013. Designing moments of meaning and pleasure. Experience design and happiness. *International Journal of Design*. 7, 3 (2013).

[5] Maslow, A.H. 1943. A theory of human motivation. *Psychological review*. 50, 4 (1943), 370.

[6] Mathiasen, N.R. and Bødker, S. 2008. Threats or threads: from usable security to secure experience? *Proceedings of the 5th Nordic conference on Human-computer interaction: building bridges* (2008), 283–289.

[7] 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? *International Conference on Financial Cryptography and Data Security* (2007), 383–388.

[8] Palen, L. and Dourish, P. 2003. Unpacking "Privacy" for a Networked World. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (2003), 129–136.

[9] Pieters, W. 2006. Acceptance of voting technology: between confidence and trust. *Trust Management, 4th International Conference, iTrust 2006, Pisa, Italy, May 16-19, 2006* (2006), 283–297.

[10] Rainie, Lee and Duggan 2015. Privacy and Information Sharing. Pew Research Center.

[11] Schneier, B. 2000. *Secrets & Lies: Digital Security in a Networked World*. Wiley Publishing, Inc.

[12] Sheldon, K.M., Elliot, A.J., Kim, Y. and Kasser, T. 2001. What is satisfying about satisfying events? Testing 10 candidate psychological needs. *Journal of personality and social psychology*. 80, 2 (2001), 325.

[13] Westin, A.F. 1968. Privacy and freedom. *Washington and Lee Law Review*. 25, 1 (1968), 166.

[14] Whitten, A. and Tygar, J.D. 1999. A Usability Evaluation of PGP 5.0. *Proceedings of the 8th USENIX Security Symposium* (1999), 169–183.

[15] Yee, K.-P. 2002. User interaction design for secure systems. *International Conference on Information and Communications Security* (2002), 278–290.