Security - Visible, Yet Unseen?

How Displaying Security Mechanisms Impacts User Experience and Perceived Security

Verena Distler
University of Luxembourg
HCI Research Group
Esch-sur-Alzette, Luxembourg
verena.distler@uni.lu

Marie-Laure Zollinger
University of Luxembourg
CSC Research Unit
Esch-sur-Alzette, Luxembourg
marie-laure.zollinger@uni.lu

Carine Lallemand
University of Luxembourg
HCI Research Group
Esch-sur-Alzette, Luxembourg
carine.lallemand@uni.lu

Peter B Roenne
University of Luxembourg
Interdisciplinary Centre for Security, Reliability and Trust
Esch-sur-Alzette, Luxembourg
peter.roenne@uni.lu

Peter Y A Ryan
University of Luxembourg
CSC Research Unit &
Interdisciplinary Centre for Security, Reliability and Trust
Esch-sur-Alzette, Luxembourg
peter.ryan@uni.lu

Vincent Koenig
University of Luxembourg
HCI Research Group
Esch-sur-Alzette, Luxembourg
vincent.koenig@uni.lu

ABSTRACT

An unsolved debate in the field of usable security concerns whether security mechanisms should be visible, or black-boxed away from the user for the sake of usability. However, tying this question to pragmatic usability factors only might be simplistic. This study aims at researching the impact of displaying security mechanisms on User Experience (UX) in the context of e-voting. Two versions of an e-voting application were designed and tested using a between-group experimental protocol (N=38). Version D displayed security mechanisms, while version ND did not reveal any security-related information. We collected data on UX using standardised evaluation scales and semi-structured interviews. Version D performed better overall in terms of UX and need fulfilment. Qualitative analysis of the interviews gives further insights into factors impacting perceived security. Our study adds to existing research suggesting a conceptual shift from usability to UX and discusses implications for designing and evaluating secure systems.

CHI 2019, May 4–9, 2019, Glasgow, Scotland Uk

ACM ISBN 978-1-4503-5970-2/19/05…$15.00
https://doi.org/10.1145/3290605.3300835

CCS CONCEPTS

• **Security and privacy → Usability in security and privacy**; *Social aspects of security and privacy*.

KEYWORDS

Usable Security, User Experience, e-voting, security mechanisms, empirical study.

ACM Reference Format:
Verena Distler, Marie-Laure Zollinger, Carine Lallemand, Peter B Roenne, Peter Y A Ryan, and Vincent Koenig. 2019. Security - Visible, Yet Unseen?: How Displaying Security Mechanisms Impacts User Experience and Perceived Security. In *CHI Conference on Human Factors in Computing Systems Proceedings (CHI 2019), May 4–9, 2019, Glasgow, Scotland Uk.* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3290605.3300835

1 INTRODUCTION

Security concerns are becoming increasingly critical and pervasive. In 2018, security breaches continue to increase in cost and size [40] and the average total cost of a data breach amounted to $3.86 million, an increase of 6% from 2017. For critical systems such as election systems, the impact of security breaches goes far beyond financial cost, which has led the US Department of Homeland Security to declare the election system "critical infrastructure" highlighting its crucial importance to national security and economy [7].

Security research is thus of strategic importance, but while technical security has traditionally been well studied, human factors have long played a limited role in security research. There has however been a growing understanding that many security breaches can be linked to "human error"

[8], oftentimes because the system interfaces with its users in an insecure way and violates basic principles of psychology and security economics [17]. The field of usable security addresses this issue.

Research has discussed whether there is an inherent trade-off between security and usability [11] given that security introduces barriers to action, while HCI attempts to remove such obstacles. Automated approaches of security, which remove security decisions from the hands of the users, have thus emerged [13][30]. However, this view has been challenged [45] [31], Norman [31] for example emphasised that appropriate technology can make some systems easier to use while enhancing security. It has also been shown that the lack of knowledge can be a root of security issues [3]. From a UX perspective, security can be an enabling factor and a significant part of UX [33], and the importance of taking into account UX factors has been underlined [10].

In this study, we take a user-centred perspective to security to investigate the impact of communicating security mechanisms on UX. We adopted a mixed-methods approach that combined user tests with semi-directive interviews, investigating both overall User Experience as well as psychological needs fulfilment.

This paper makes the following main contributions to the HCI community:

- Our findings extend existing knowledge on how displaying information on security mechanisms impacts people's UX.
- We identify additional key UX factors that impact perceived security.
- We propose actionable guidelines to support the design of secure systems for researchers and practitioners.

2 RELATED WORK

Different fields of research have adopted different definitions of security. Security can refer to personal security, physical security and computer security [29]. In the context of IT, security can be defined as the limited effects of an attacker trying to make a system fail [35]. This is coherent with many traditional definitions of security which typically refer to security mechanisms such as passwords or encryption [29]. These definitions are mostly concerned with systems or situations, whereas the definition of security in UX Design is concerned with the perceived security humans experience when interacting with such system. A definition that is often used in UX has its origin in psychological needs theories, which define the need for security as "feeling safe and in control of your life rather than feeling uncertain and threatened by your circumstances" [20].

A related concept is privacy, which mostly focuses on either (1) the right to isolation or (2) the right to control information about oneself. Palen and Dourish [34] characterise privacy as "the continual management of boundaries between different spheres of action, and degrees of disclosure within those spheres". These boundaries change with context.

Usable security: towards a stronger inclusion of User Experience

Usability is traditionally concerned with improving "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use." (ISO 9241-11)

In comparison, User Experience (UX) focuses less on task performance and puts a stronger emphasis on emotive, subjective and temporal aspects that play a role when users interact [36]. UX takes into account both hedonic (non-instrumental) and pragmatic (instrumental) qualities of experience [28]. Pragmatic qualities can be seen as similar to the aspects measured by usability. Users' frequent non-compliance with security procedures, combined with their difficulties using security mechanisms, have led some to believe that security and usability are inherently in conflict [9]. Other studies suggest that security and usability are interrelated in a complex way and trade-offs must be balanced [16].

Dunphy and colleagues [12] proposed that ideas from experience-centered design can help researchers in the security domain understand context-specific user behaviours, gain insights into subjective user perceptions of security or privacy and create theories about how technologies fit into people's lives. Studies have also underlined the need to take into account users' values in addition to experiential factors [10]. Pagter and Petersen [33] suggested the strategic use of explicit security actions to design for engaging experiences that are perceived as secure. They demonstrated that security can be a visible, enabling factor for experience, rather than a nuisance.

Studies have also shown that it is important to take into account psychological needs as a part of UX, given that fulfilment of psychological needs has been shown to contribute to a positive UX [18][41]. The most relevant needs were narrowed down to autonomy, competence, relatedness, popularity, stimulation and security [18].

Visibility of security mechanisms and UX

Security mechanisms are often hidden away from the user [11]. While this approach has the advantage that users are not required to understand the underlying security mechanisms, it has been shown that lack of knowledge can be the root of certain security issues [3], and authors have argued that instead of being "transparent", security technologies should be "highly visible, available for inspection and examination seamlessly as a part of work" [11].

The effectiveness of displaying security mechanisms has been questioned, Schechter and colleagues [38] showed for instance that users mostly did not correctly interpret the lack of security indicators, such as HTTPS indicators or authentication images. In their study, even though the website showed increasingly important signs that it was not secure, no participant adopted "secure behaviour" and withheld their password. Their work thus seems to indicate that security indicators do not necessarily modify users' behaviour. Ferreira and colleagues [15] showed that context and beliefs play a role in users' security decisions regarding visible security indicators.

Fahl et al. [14] studied the usability and perceived security linked to encrypting Facebook messages, investigating different combinations of manual and automatic encryption and key management. Studies outside the scope of security indicate that the degree of visibility of a system's functioning might impact trust. Kizilcec [24] studied the impact of algorithmic transparency on trust in the context of peer-assessment. Participants who had received a lower grade than expected trusted the grading algorithm less, unless the algorithm was explained to them. On the contrary, when too much information on the algorithm was provided, trust was eroded.

Security and UX of e-voting

Paper voting systems have several shortcomings, some of which are of pragmatic nature (e.g., waiting times [42]), others are linked to security weaknesses. To respond to security-related and pragmatic concerns, researchers have developed end-to-end verifiable e-voting schemes (e.g., [37] [4]).

Privacy, in the context of e-voting, is defined by ballot-secrecy, receipt-freeness and coercion-resistance. Ballot-secrecy means that the system must not reveal the vote for a given voter. Receipt-freeness indicates that there is no information, or receipt, that can directly prove a vote. Coercion-resistance means that a voter is able to cast a vote freely, even if a coercer can interact with the voter before, during and after casting.

Verifiability, on the other hand, should enable voters to check that their vote was cast-as-intended, recorded-as-cast and tallied-as-recorded. There is a distinction between individual verifiability, which means that voters can verify their own votes, and universal verifiability, which allows any observer of the election to verify the correctness of the result of the election.

In response to these security requirements, various voting systems have been developed. While these methods may solve some security problems that are associated to traditional paper voting, they also introduce some added complexity to the voting process [2]. Acemyan et al. [2] compared the usability of three voting systems, and found out that they were exceptionally difficult to use. In the first step of using the voting systems, casting a vote, only 58% of the participants were able to successfully cast a vote across all three systems. Overall satisfaction was low. For the second step of these voting systems, the verification phase, completion rates were even lower. The authors emphasise the importance of voting systems to be not only secure, but also usable.

Other studies have pointed towards a correlation between perceived security and acceptance of a voting method [44], thus pointing towards the relevance of investigating fulfillment of the need for security.

Going beyond usability, the UX of e-voting systems has only been studied to a limited extent. In this paper, we study the impact of displaying security mechanisms on User Experience in the context of e-voting. This use case is illustrative of an application in a high-stakes environment, yet nevertheless targeted at the general population. Some might view voting as a rare occasion, yet it is a frequent interaction considering all types of elections (e.g., citizenship, in a work or school context, associations). E-voting can thus be a regular, high-stakes interaction for most people. We use it here as a representative of security-relevant technologies and will discuss the underlying implications of our findings for the design of such systems.

3 RESEARCH OBJECTIVES

An important debate in the field of usable security concerns whether security mechanisms should be made visible to users or rather stay invisible to improve systems' usability. Knowing more about the impact of making security elements visible in different contexts will inform the design of security-relevant technologies to trigger optimal experiences. This study thus aims to address this challenge by adopting a more comprehensive UX perspective beyond usability concerns only. The present study addresses the following research questions:

RQ1: What is the impact of displaying encryption-related security mechanisms on UX?
RQ2: What is the impact of displaying verifiability-related security mechanisms on UX?

Building on RQ1 and RQ2, we will derive actionable guidelines to support the design of secure experiences.

4 METHODOLOGY

Participants

38 participants took part in our study (19 male, 19 female). In order to ensure that all participants had comparable prior voting experiences, only persons who held the voting right

and had participated in at least one political election were selected.

The average age was 35.4 years (Min=19, Max=73, SD=12.45). Participants were recruited in online groups on social networks of nearby cities where users exchange practical information. We recruited a diverse sample of laypersons who were unknown to the researchers. 13% held no diploma or a diploma below the A-levels, 29% had obtained the A-Levels degree, 21% held a college degree, 18% a Bachelor's degree, 16% a Master's degree and 3% had a PhD.

There were 19 participants per group. Groups were assigned to ensure high similarity between conditions (age, gender, education), thus controlling for extraneous variables.

Procedure

We conducted 38 user tests and semi-structured interviews in summer 2018. Each session took approximately 1 hour. Participants gave informed consent and were compensated for their time.

The sessions were split up into 4 phases:

(1) **Voting phase:** Participants cast a vote via the application.

(2) **Post-voting UX evaluation:** The UX of phase (1) is evaluated through:
   (a) *two questionnaires:* UEQ [27] and UX needs scale [26].
   (b) *a semi-structured interview.*

(3) **Verification phase:** Participants verify that their vote has been taken into account using the same app.

(4) **Post-verification UX evaluation:** The UX of phase (3) is assessed using the same procedure as in phase (2).

Both the interview and questionnaires were administered twice i.e., once after the voting phase (T1), and once after the verification phase (T2). This repeated measure allows to explore users' thoughts about the voting and the verification phase in a separate manner given that verification has no direct equivalent in paper voting.

We combined questionnaires and interviews in order to gather both structured data (following a UX framework and allowing us to compare UX across versions D/ND and phases T1/T2) and deep insights formulated in users' own words.

In order to improve the ecological validity of our lab study, we introduced a scenario which participants should envision themselves in. This in-sitro approach consists in the recreation of elements of a real use situation in a lab setting, thus increasing the level of realism of lab studies [25]. We asked participants to imagine that the next national elections were about to take place, and that they had decided to vote online. They received some basic information regarding the candidates they could choose from for their election, as well as "official" letters which were personalized to each participant giving them the login details for the application. All sessions were facilitated by one of two trained facilitators in order to ensure high consistency with regards to the facilitation style. All participants casted their vote successfully and no major issues were encountered by participants in the two groups.

Special attention was paid to security priming, which is a common bias in usable security studies [16]. We attempted to avoid priming our participants by explaining that the goal of the study was merely to understand the UX of the application. In the interviews, no reference to security was made until the very end of the study.

Material

Standardized UX Scales. We used two standardized questionnaires as a measure of UX: the User Experience Questionnaire (UEQ, [27]) and the psychological needs scale (original questionnaire [41] adapted by Lallemand and Koenig [26]).

The UEQ measures overall attractiveness, pragmatic (instrumental) and hedonic (non-instrumental) qualities of experience. The pragmatic qualities subscales include perspicuity, dependability, efficiency. Hedonic qualities include stimulation and novelty subscales. The items are presented in the format of 26 contrasted pairs of words separated by a 7-points scale (ranging from -3 to 3) as exemplified here:

Attractive ○ ○ ○ ○ ○ ○ ○ Unattractive

The UX needs are a further UX measure which focuses on the fulfilment of psychological needs. Multiple studies show that fulfilment of psychological needs might be a driver of positive experience [41][19]. The 30-items scale measures the fulfilment of the needs for competence, autonomy, security, pleasure, relatedness, influence and self-actualizing. While we were mostly interested in the needs of security, competence and autonomy, we administered the questionnaire including all needs in order to avoid security priming. We asked the participants to rate the fulfilment of their psychological needs using a 5-points Likert scale (from 1 Not at all to 5 Extremely). After having checked the reliability of each UX need subscale, we computed mean scale values for each need by averaging the respective items for each participant. Statistical analyses have been conducted using SPSS v24. Effect sizes are reported following Cohen's convention.

Interviews. The questions in the first interview (at T1, after the voting phase) concerned the overall impression participants had, any difficulties they might have encountered, and how they perceived the e-voting experience compared to

paper voting. Trust in the application was also discussed. A free discussion followed, with the participant explaining their rationale. In the second interview (at T2, after the verification phase), participants were asked the same questions again, with additional questions pertaining to the verification phase. Questions regarding the perceived security were only asked at the very end of the session (in the end of the evaluation phase at T2) in order not to bias participants' earlier responses to refer mainly to security. A bottom-up content analysis of recurring topics followed, which were subsequently organised in an affinity diagram. The categories that were obtained using the bottom-up analysis were closely related to the UX frameworks as deployed in the questionnaires, namely hedonic and pragmatic qualities, with additional factors identified, namely contextual factors and past experiences. Our objective was to understand how these factors impacted perceived security.

The e-voting smartphone application. We developed an Android application for the existing e-voting protocol Selene [37]. Selene is an end-to-end verifiable voting scheme that avoids voters having to handle an encrypted ballot and instead provides each person with a unique tracking number. This number allows voters to verify that their vote has been counted in a list of all votes. It thus takes a different approach from most voting schemes, which require users to handle an encrypted ballot in order to verify that their vote has been included in the tally.

Using the technical specifications of Selene, we created low- and high-fidelity prototypes, which we iteratively tested on end users and improved following a user-centered design process. In order to study the visibility of security mechanisms, two versions of the app were developed (screenshots in the additional material):

- *Version D* displays the employed security mechanisms (e.g., encryption or decryption) to the user through waiting screens (e.g., "currently encrypting your vote") and additional explanations as shown in Figure 1 and Figure 2.
- *Version ND* does not display any security mechanisms to the user. There were no waiting screens that informed users of the ongoing encryption. No explanations were given regarding the technical security mechanisms in place.

There were thus two main instances of security mechanisms that were made visible in the application: encryption/decryption processes (between-subject design, only in version D) and verification (within-subject design, present in both versions yet with more explanations in version D), in addition to the authentication phase.

5 RESULTS

Impact of displaying security mechanisms on UX

User Experience Questionnaire. Both versions of our application scored above average on the UEQ (according to [39]) with average means of 1.12 (SD = 0.82) for version D and 1.05 (SD = 0.86) for version ND as shown in Table 1. Overall, respondents assessed version D (with visible security mechanisms) as slightly better than version ND. As shown in Figure 1, version D (at T1, M = 0.95, SD = 0.72) scored higher on hedonic aspects than version ND (M = 0.60, SD = 0.98) with a small effect size (d = 0.41). Version ND at T1 scored slightly higher for pragmatic aspects (M = 1.64, SD = 1.41) than version D (M = 1.50, SD = 1.26), yet with a negligible effect size.

At the subscale level, results indicate that *Perspicuity* (e.g., *understandable/not understandable, difficult to learn/easy to learn*) was experienced higher in version ND (M = 2.16, SD = 1.29) than in version D (M = 1.90, SD = 1.30, d = -.23). The hedonic subscale *Perceived Novelty* was significantly higher (t(36)=2.20, p=.035) in version D (M = 1.31, SD = 1.09, version ND: M = 0.33, SD = 1.30) with a moderate effect size (d = 0.67).

Psychological Needs Questionnaire. This section focuses on the needs for *Competence, Autonomy* and *Security*. While these were the needs we were mainly interested in, we still collected data for all needs to avoid security priming.

Our participants assessed the fulfilment of their need for *Security* as higher in version D (M = 3.80, SD = 0.71) than in version ND (M = 3.51, SD = 1.00) with a small effect size (d = 0.34). Similarly, the need for *Competence* was perceived higher in version D (M = 3.85, SD = 0.68) than in version ND (M = 3.54, SD = 1.35, d = 0.29). Both in version D and ND of the app, the feeling of *Competence* was higher after the voting phase than after the verification phase. The levels of perceived *Autonomy* were very similar for both versions (Version D: M = 4.05, SD = 0.69, Version ND: M = 4.13, SD = 0.81). No notable differences between versions were found regarding the fulfilment of *pleasure, relatedness and influence*. At the item level, the item "I felt I understood how things worked" (part of *Security* scale) was significantly higher in version D (M = 4.32, SD = 1) than in version ND (M = 3.63, SD = 1.07, t(36) = 2.04, p =.049).

In order to explore the relationships between the need for security and the other UX factors, we computed Pearson's correlation coefficients.

We first explored the links between the fulfilment of the need for Security and the need for *Competence* (feeling capable and effective in one's actions) and found an overall moderate correlation for both version D and ND combined, ($r(36)$ = .62, p = .001). While the two needs were not correlated in version D, they were strongly correlated in ND,

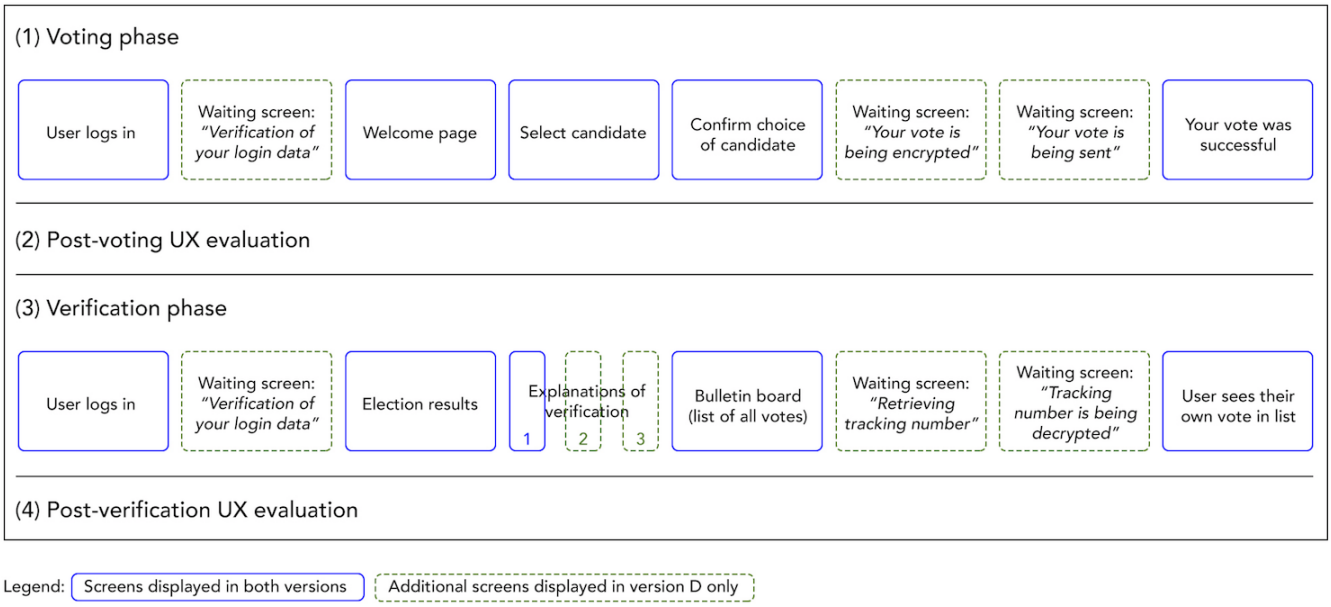

Figure 1: A conceptual overview of the differences between version D and ND of the app.

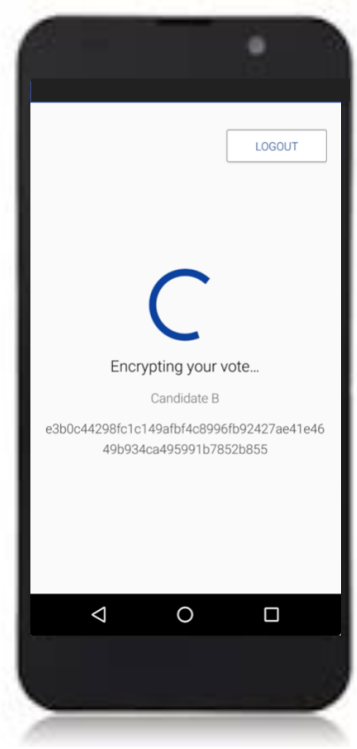

Figure 2: One of the screens displaying the security mechanisms of the app in version D during phase 1 (voting phase). No such informative screens were shown in version ND.

	Vers. D		Vers. ND			
	M	*SD*	*M*	*SD*	*d*	*p*
UEQ/Overall	1.12	0.82	1.05	0.86	0.08	0.810
UEQ/Hedonic	0.95	0.72	0.60	0.98	0.41	0.214
UEQ/Pragmatic	1.50	1.26	1.64	1.41	-0.11	0.741
UEQ/Attr.	1.18	0.69	1.18	0.92	0	0.997
Needs/Competence	3.85	0.68	3.54	1.35	0.29	0.371
Needs/Autonomy	4.05	0.69	4.13	0.81	-0.10	0.748
Needs/Security	3.80	0.71	3.51	1.00	0.34	0.304

Table 1: Summary of questionnaire results for both UEQ and needs questionnaire.

(r(17) = .73, p = .001) and especially at T2 ($r(17)$ = .87, p = .001). No significant correlation was found between *Security* and *Autonomy* for both versions D and ND, nor for *Security* and *Pragmatic Quality* or *Security* and *Attractiveness*. Last, *Security* and *Hedonic Quality* were moderately correlated at T2 only for version ND ($r(17)$ = .49, p = .033). Regarding demographic factors, age was negatively correlated with all UX factors (Hedonic qualities: $r(36)$ = -.30, p =.068, pragmatic qualities: $r(36)$ = -.35, p =.031, attractiveness: r(36) = -.37, p = .024). Age was also negatively correlated with perceived security yet in version D only ($r(17)$= -.42, p = .077). No significant correlation was found between age and the need for security in version ND. In version ND, age was negatively correlated with competence ($r(17)$ = -.43, p = .077). No statistically significant difference was found with regards to participants' education level.

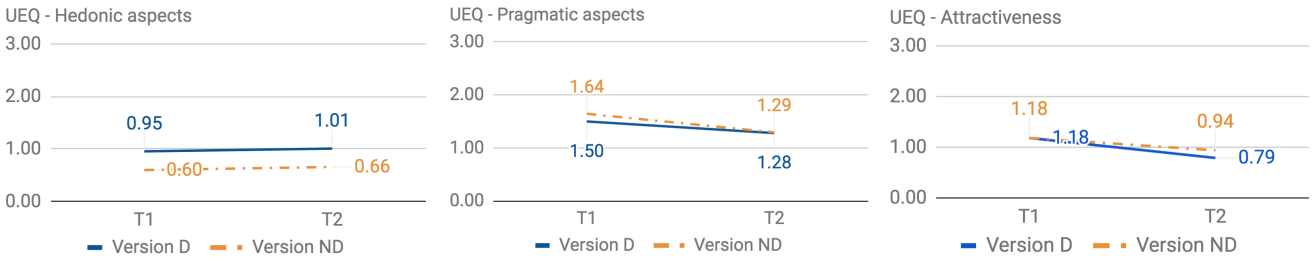

Figure 3: Results of User Experience Questionnaire (Version D: display of security mechanisms, Version ND: no display of security information. For statistically non-significant results, effect size was reported)

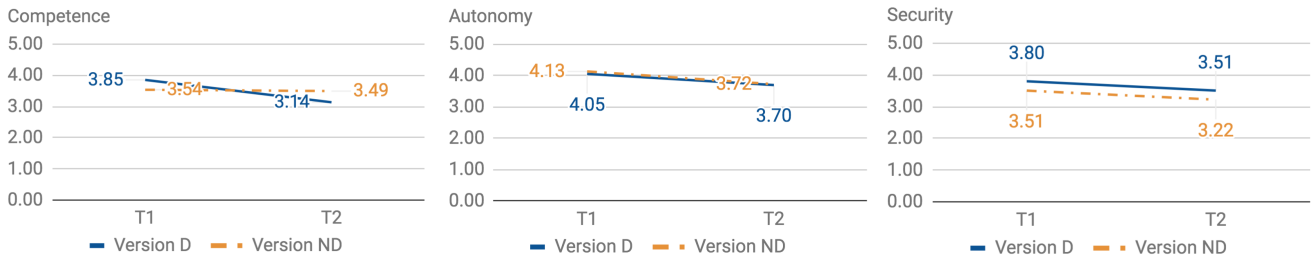

Figure 4: Results of psychological needs questionnaire (Version D: display of security mechanisms, Version ND: no display of security information)

UX factors impacting perceived security of e-voting

The results of the interviews were analysed using a content analysis of recurring topics and shed light on additional factors impacting the UX with a special focus on aspects pertaining to the perceived security of participants. No notable differences emerged between the participant groups who had used version D and those who had used version ND. We thus report these findings with no distinction of the experimental group participants belonged to. We studied three instances of visible security: the display of encryption, verification and the authentication phase. We will first report these findings, before describing additional factors that played an important role in the experience: general security concerns, the impact of pragmatic qualities, contextual factors and past experiences.

Impact of displaying encryption. Many participants who had used *version D* of the application did not consciously see or pay attention to the security mechanisms displayed to them. Most of those who did notice the mechanisms however felt reassured: "I like seeing that there is encryption, it is good to remind people that their data is secure and not hacked, and there is no HTTPS like in a browser." (P35). "When I see 'encryption ongoing', that's reassuring." (P17).

One participant who had used version D explicitly stated that they would choose seeing security-related information if they had a choice: "If I had the possibility to choose if I want to have access to this transparency for both encryption and verification, I would choose this [transparent] version." (P32) The same participant even pushed for more transparency: "I like when it's open source, like this everyone can see if it is secure".

In *version ND*, some participants perceived the process as too quick and easy. This left them with a feeling of uneasiness although they did not necessarily link it to the lack of security information. Few participants specifically referred to a lack of feedback in version ND, but P5 for instance found that there was not enough information: "I feel like user feedback is missing, usually I like having some little things telling me that it is secure."

Impact of the verification phase. The verification phase is an unknown concept to most end-users, with no direct equivalent in real-life. In the application, there was a list of all votes that had been counted for the election. These votes are completely anonymous, only the user of the app can see their own vote for verification. The application explained vote verification to participants in an understandable way, which was validated in pre-tests. The results regarding verification were contradictory. Many participants expressed that vote verification was positive. "This might be better than the current voting system where my vote completely disappears. It is reassuring." (P29), but many also did not see any advantage to verifying: "I am confused, I don't know

what this is good for. A confirmation that my vote has been counted would have been sufficient." (P30).

Interestingly, verification, a mechanism designed to increase vote security, decreased many participants' perceived security: "I am less confident now [after the verification phase]." (P26)

While many participants simply did not see any use to vote verification, some expressed strong concerns regarding vote anonymity during this phase. Even though they had understood that their vote was still private, the fact of seeing all anonymized votes in a list gave them the impression that their vote was suddenly less confidential. One participant compared seeing the anonymized list of votes to opening the curtain of a voting booth, revealing the person's back, strongly emphasising that "just seeing a little bit is already too much. There is information one does not want to have." (P32)

Some participants compared the verification phase to the counting of votes in paper voting: "When I go to see the counting of votes, I know that the persons counting did it correctly. Here [with verification on the app] I don't have this certainty. On the internet, I am not convinced." (P24)

The importance of the authentication phase. Many participants described the authentication phase as critical for their perceived security, and interestingly, many participants believed that a secure authentication phase was sufficient to create security: "As soon as there were the login codes, I felt secure. Like online with the credit card icon, I felt secure." (P27)

Some participants suggested alternative authentication methods, such as using a digital fingerprint or two factor authentication to improve the overall security of the application. "In order to improve my trust, maybe there should be a log in with a digital fingerprint. I don't see anything else." (P25) These insights show that a carefully designed authentication phase can impact the perceived security of an entire application.

While the focus of this study was to examine the impact of displaying these instances of security, qualitative analysis showed that the participants' general security concerns played a role in their perception of the security mechanisms and the e-voting application as a whole. Moreover, pragmatic qualities, contextual factors and past experiences contributed to their experience. We will describe these results in the following.

Security concerns. When asked whether they had any security concerns while using the e-voting application, many participants reported not having any: "About the security? No, nothing has come to my mind." (P27) When prompted, they were unsure of security risks and described a general feeling of vulnerability when using technologies. A large number of participants mentioned some general security concerns, such as hacking, which they perceived as inherent to technologies in general and thus not something that can be avoided: "Yes, of course it is always possible to be hacked. That's not something I think about." (P16). Most participants were unsure of the security risks linked to using smartphone apps. "Security questions? No. But it remains technology. Can there be leaks on an application? I think it might be hacked?" (P23)

Other security concerns either referred to human threats such as others voting instead of the legitimate person ("What if someone votes instead of me?" (P19)) or general technical threats linked to using the internet or smartphones; "For sure this is quicker, but I am not a fan of the internet. I think it's vulnerable, even if it is secure." (P24). "Nothing is ever secure, nowhere." (P28)

Pragmatic qualities. Our qualitative analysis showed that pragmatic aspects play an important role in the experience of e-voting. Our participants found the application practical, easy to use and understandable, with an appropriate design. "It was very quick and clear, you couldn't fall off track. It does its job." (P3). They mentioned that e-voting in general might increase the vote turnout, and that it might mitigate some of the security problems of paper voting. On the negative side, our participants expressed concern for certain population groups: "I am very engaged with elderly people and I see the difficulties they have with IT. When I put myself in their shoes, it is complicated. Except if someone is next to them to help them vote on their phone, but what about vote secrecy?" (P19)

Interestingly, some participants stated that the ease of use gave them the impression that the application was trustworthy: "Given that it's easy to use I would trust it more." (P32)

Pragmatic qualities did not only have a positive impact however. Surprisingly, participants found that the e-voting application was too easy to use: "It's easy but frustrating, you don't have to go anywhere, you just push a button and that's it. It is too quick." (P30) And lastly, there were also participants who stated that even though they did not really trust the app, they would still use it for practical reasons.

Contextual factors. Some contextual factors impacted our participants' UX when e-voting. First, many participants mentioned that receiving their login ID and password in letters gave them a feeling of security: "Receiving this by paper mail is reassuring." (P2) Some however mentioned security concerns regarding paper mail, for example with regards to roommates or family members who might access their login details. Many participants were also reassured by the fact that the application had been issued by a governmental

authority "I didn't wonder about security. If it is an app from the government, I thought that it must be secure".

Past experiences. Participants consistently compared e-voting to paper voting. The symbolic value of casting a paper vote was important to them: "It's symbolic to go into the voting booth. I miss the symbolic aspect with e-voting, I think it would be a pity if we all voted on our phones." (P23). Participants mentioned that they liked the personal contact when paper voting ("At the polling station we talk about our opinions, we discuss with people" (P27)). However, other participants mentioned that e-voting offered relief of the social pressure they experience at polling stations:

"This is extremely anonymous, there is no pressure like at the polling station with the people behind you. On the smartphone, you can hardly be judged. This makes me feel more in security when voting." (P15)

Participants also often referred to past experiences in other domains when evaluating the UX of the e-voting application. Banking apps were often used as an example for secure applications that everyone uses. Again, the organisation issuing the application was an important factor impacting perceived security: "If the app is from this bank, then it must be secure." (P11) Some participants also explained that they were aware of potential security failures of banking apps, but underlined that the practical aspects of using a banking app were predominant: "I use the banking app, but I know that I am not safe. There are people who get hacked. When something like this exists and it's practical, one uses it." (P16)

This is similar to the trust participants expressed in the e-voting application, which was grounded in its practicality and ease of use.

Other examples participants compared e-voting to were official administrative procedures which they completed online, such as tax returns: "I already do a lot of things online, my tax returns for example. It saves a tremendous amount of time. When it's easy to use, it suits me fine." (P27)

6 DISCUSSION

Why designing for usability alone is insufficient: How displaying security mechanisms impacts UX

The first research question of the present study had the objective of investigating how displaying security mechanisms impacts User Experience. Both versions showed good scores for pragmatic quality, and it is noteworthy that all of our participants were able to successfully cast their vote compared to 58% for the e-voting systems tested by Acemyan and colleagues [2]. While these studies are comparable to a limited extent (e.g., slight differences in study design, contextual factors might have changed during four years), it is noteworthy that the voting applications tested in their study were not designed in a user-centred approach, pointing towards the value of adopting a UX process when creating e-voting applications.

In version ND, participants had less information to process since no security information was given to them. While this might have advantages for the efficiency and overall usability of a system, usability can also have downsides, as one of our participants explained: "Voting becomes banal. It is very quick, I am not for it." (P23). Making the process quicker and smoother might cause perceived security to decrease. Indeed, the need for security was slightly less fulfilled in version ND and the interviews show that the security mechanisms felt reassuring to participants. While many participants using version D of the app did not report seeing the security mechanisms, we hypothesise that the presence of security information, combined with the additional waiting time it introduced had a positive impact on the hedonic quality of the experience and on perceived security. Lower usability due to more visible encryption might thus be correlated with higher perceived security. This hypothesis is in line with a study by Fahl and colleagues [14] who found the highest usability in the versions of their prototype that included either no display of security, where encryption was completely automated, or a combination of manual encryption and automatic key management. Similarly to our study yet not assessed using the same metrics, "security feeling" was highest in the versions with the lowest usability scores, which included some extent of manual encryption or key management.

Previous studies have investigated the usability of e-voting systems [2][5][44], but there is a dearth of research that takes into account UX in the context of e-voting. While usability is an important indicator and prerequisite for such systems, our study and related work thus indicate that the goal of making security-relevant technologies more usable alone is insufficient to create a positive UX. Dependent on the experience designers want to create, adopting a usability perspective alone might even be detrimental to the objective, given that usability does not take into account critical factors such as perceived security. Moreover, while a lack of usability will result in users' dissatisfaction, a good level of usability will not necessarily trigger satisfaction. This is what is commonly referred to as a hygiene factor as compared to motivational factors [21][20].

The UX approach might provide insights into context-specific user behaviour, into subjective perceptions of security and privacy and create theories about how technologies fit into people's lives [12]. While the SUS [6] scale is most commonly used in the usable security community, more recent UX scales like the UEQ [27] allow researchers and practitioners to understand hedonic qualities of experience,

in addition to the pragmatic quality (comparable with the measure supported by the SUS).

Ideas from experience-centered design might help researchers in usable security gain a deeper understanding of context-dependent behaviors and subjective user perceptions [12] due to a stronger focus on emotive, subjective and temporal aspects [36]. Beyond supporting the inclusion of UX-criteria in usable security studies, we believe that a conceptual change away from usability to UX would allow for a more holistic understanding of security-relevant experiences.

Transparency: a double-edged sword for UX

Including transparency is necessary to provide people with the means to understand the security implications of the configuration of technologies at their disposal, and it should be expressed in terms that correspond to users' activities and needs at the time [11]. Dourish et al. [11] suggest that security technologies should be highly visible and available for inspection.

In the present study, we investigated the impact of making security mechanisms visible on UX. There were three instances of security that were made visible in our application: two main instances of the display of encryption-related processes and the verification phase, in addition to the authentication phase.

The verification phase was studied as a security mechanism that is required in e-voting with the objective of making the voting process verifiably secure both at the individual and the universal level. As stated by Olembo and Volkamer [32], "user interaction for verifiability is required in verifiable e-voting systems, and therefore understanding is critical." (p. 173) Verification thus requires user interaction which is an important difference between these types of transparency given that the display of the encryption-related processes does not require any interaction.

The first way of providing transparency, the display of encryption and decryption processes, was embodied in version D of the application. As described above, this version showed overall more positive results in terms of UX and needs fulfilment, even though many participants reported not consciously having processed the display of the security mechanisms. This result is similar to Fahl and colleagues [14], in whose study manual key management (also implying a more visible security mechanism) equaled lower usability scores, but also higher perceived security. The authors suggested that the complexity of a mechanism might increase a user's perceived security, and that an entirely invisible and effortless protection mechanism might not generate a feeling of security. It is also noteworthy that participants using version D felt like they understood how things worked significantly better than in version ND, pointing to a potential improvement of understanding of the functioning of the app.

The second research question concerned the impact of displaying verifiability-related security mechanisms on UX. The verification phase yielded ambivalent reactions, even though the explanations were carefully worded and pre-tested. Overall, UX was assessed as better before the verification phase, and many participants did not understand the utility of seeing their own vote within the entire list of votes on the bulletin board. Some participants reported feeling more insecure, while others felt reassured that their vote had been counted towards the election result. The verification phase introduces some friction to the process by requiring an additional interaction of the user which is not directly aligned with their objective at the time of use. Verification has no direct equivalent in real life users can base their understanding on, it has been considered an "unnatural concept" for users [44]. The verification process is however necessary from a security standpoint, it is thus important to design this process in a way that supports UX and perceived security.

Referring back to Dourish and colleagues [11], more research is needed to investigate how verification can be communicated even better for those participants for whom seeing the list of votes was a perceived mismatch with their need at the time, which was to check that their vote (and their vote only) had been recorded correctly.

A discrepancy was noteworthy in this context. Introducing a certain degree of complexity by displaying the encryption and decryption process had a negative impact on pragmatic aspects, but a positive impact on overall UX. This result is promising given that it indicates that displaying security mechanisms such as encryption, while not necessarily improving usability, might improve overall UX. Displaying information about encryption might also contribute to users' understanding of encryption processes who often have misconceptions about the latter [1]. The verification phase, in contrast, had a negative effect on UX, and it had, according to the interviews, the shortcoming of not being aligned with the users goals at the moment. This example demonstrates that transparency needs to be provided in a meaningful and purposeful way that is aligned with users' goals.

7 LIMITATIONS AND FUTURE WORK

The present study has also shown some limitations. While great efforts were made to maximize the validity of our study (e.g., use of scenarios and elements simulating a real election such as official personalised letters), the fact that it took place in a lab setting might have increased participants' feeling of security [43][38] and partially biased the evaluation of UX on specific aspects (e.g., social factors) which are harder to assess in a controlled environment [26].

In our study we used two versions of the same smartphone application. Future studies should investigate the impact of a larger diversity of visualisations of security mechanisms on UX. Another aspect that was not addressed by our study are cultural aspects that might impact UX, including perceived security (e.g., for countries where voting is linked to higher risks). Similarly to previous literature [32], our study takes a western perspective and future studies should investigate cultural differences linked to e-voting perceptions.

8 RECOMMENDATIONS FOR THE DESIGN OF SECURITY-RELEVANT TECHNOLOGIES

We suggest the following recommendations for researchers and designers who have the objective of improving the UX and perceived security of security-relevant technologies.

Do not assume users necessarily have security concerns: Users do not necessarily have many concerns regarding IT security. One should therefore avoid the security-priming bias by not prompting participants to think about security topics.

Be aware that users do not always have the required knowledge to assess a system's security level: Many users have a limited knowledge of security but have a general feeling that new technologies can bear security risks, often referring to the general risk of "hacking". Design teams should explore users' security knowledge and iteratively test security-relevant processes on the target population.

Take advantage of users' beliefs about the authentication phase for enhancing technical security: Users often refer to the perceived security of the authentication phase (when applicable) as a proxy for overall security and seem to be willing to invest more efforts at this stage to safeguard their security. Designers might thus introduce additional authentication security measures if necessary (e.g., biometrics, 2 Factor Authentication).

Include contextual factors as essential aspect of experience / security design: When forming an opinion of the perceived security of an application, users take context into account. The experience of any system starts before the interaction and users rely on related information (e.g., which organisation or authority issued the app) to make the choice of using a system or not. Exploring users' needs through contextual inquiry [22] and synthesizing them through user journey maps [23] safeguards the integration of contextual factors during the design process.

Benchmark comparable experiences likely to act as users' reference points: Users also use past experiences to make sense of their current experience. One should therefore carefully investigate potentially related experiences to understand the elements that impact perceived security. Some of these elements may then be transferred to one's project.

Use transparency in a purposeful way and consider the relevance of trade-offs between usability and other experience related factors: Transparency (in the sense of displaying security mechanisms) can shape perceived security either for the sake of a more optimal experience or for adding friction when user awareness of security is critical. One should adopt a larger conceptual model when designing security relevant technologies, not limited to usability. Design and evaluation methods should support this more comprehensive perspective: an example of this would be replacing usability scales such as SUS or QUIS with more recent UX scales (e.g., UEQ used in the present study) when assessing systems' qualities.

9 CONCLUSION

The present study aims to address the debate of whether security mechanisms should be visible to users using a more comprehensive UX approach that goes beyond usability alone. It makes three main contributions. First, it builds on existing knowledge on how displaying information on security mechanisms impacts people's UX . Second, it identifies UX factors that impact perceived security. The results have shown that factors impacting UX and perceived security go beyond usability aspects, which supports the inclusion of such factors into usable security studies. Our study adds to existing research suggesting that a conceptual shift from usability to User Experience might bring substantial added value to the field of usable security. Our third contribution thus consists in suggesting a number of recommendations for design and research in usable security. The results of this study are thus promising, and we expect the results to contribute to future studies which investigate to what extent displaying information on security mechanisms can be an enabling factor to UX.

ACKNOWLEDGMENTS

We thank the anonymous reviewers for their constructive feedback. We acknowledge support from the National Research Fund (FNR) under grant number PRIDE15/10621687. PBR was partly supported by the FNR INTER-Sequoia project which is joint with the ANR project SEQUOIA ANR-14-CE28-0030-01. MLZ was supported by the INTER-SeVoTe project.

REFERENCES

[1] Ruba Abu-Salma, Elissa M Redmiles, Blase Ur, and Miranda Wei. 2018. Exploring User Mental Models of End-to-End Encrypted Communication Tools. In *Proceedings of the 8th USENIX Workshop on Free and Open Communications on the Internet (FOCI)*. Baltimore, MD, 8.

[2] Claudia Z. Acemyan, Philip Kortum, Michael D. Byrne, and Dan S. Wallach. 2014. Usability of voter verifiable, end-to-end voting systems: Baseline data for Helios, Prêt à Voter, and Scantegrity II. *The USENIX Journal of Election Technology and Systems* 2, 3 (2014), 26–56.

[3] Anne Adams and Martina Angela Sasse. 1999. Users are not the enemy. *Commun. ACM* 42, 12 (Dec. 1999), 40–46. https://doi.org/10.1145/322796.322806

[4] Ben Adida. 2008. Helios: Web-based Open-Audit Voting. 335–348.

[5] Benjamin B Bederson, Paul S Herrnson, Richard G Niemi, Bongshin Lee, and Robert M Sherman. 2003. Electronic Voting System Usability Issues. *NEW HORIZONS* 5 (2003), 8.

[6] John Brooke. 1996. SUS-A quick and dirty usability scale. *Usability evaluation in industry* 189, 194 (1996), 4–7.

[7] US Election Assistance Commission. [n. d.]. Elections - Critical Infrastructure - Elections as Critical Infrastructure. https://www.eac.gov/election-officials/elections-critical-infrastructure/

[8] Lorrie Cranor and Simson Garfinkel. 2005. *Security and Usability*. O'Reilly Media, Inc.

[9] L. F. Cranor and S. Garfinkel. 2004. Guest Editors' Introduction: Secure or Usable? *IEEE Security Privacy* 2, 5 (Sept. 2004), 16–18. https://doi.org/10.1109/MSP.2004.69

[10] Steve Dodier-Lazaro, M Angela Sasse, Ruba Abu-Salma, and Ingolf Becker. 2017. From Paternalistic to User-Centred Security: Putting Users First with Value-Sensitive Design. In *Workshop on Values in Computing. 09 May 2017*. 7.

[11] P Dourish, R. E Grinter, J. D de la Flor, and M Joseph. 2004. Security in the Wild: User Strategies for Managing Security as an Everyday, Practical Problem. *Personal and Ubiquitous Computing* 8 (2004).

[12] Paul Dunphy, John Vines, Lizzie Coles-Kemp, Rachel Clarke, Vasilis Vlachokyriakos, Peter Wright, John McCarthy, and Patrick Olivier. 2014. Understanding the Experience-Centeredness of Privacy and Security Technologies. ACM Press, 83–94. https://doi.org/10.1145/2683467.2683475

[13] W. Keith Edwards, Erika Shehan Poole, and Jennifer Stoll. 2008. Security automation considered harmful?. In *Proceedings of the 2007 Workshop on New Security Paradigms - NSPW '07*. ACM Press, New Hampshire, 33. https://doi.org/10.1145/1600176.1600182

[14] Sascha Fahl, Marian Harbach, Thomas Muders, Matthew Smith, and Uwe Sander. 2012. Helping Johnny 2.0 to encrypt his Facebook conversations. In *Proceedings of the Eighth Symposium on Usable Privacy and Security - SOUPS '12*. ACM Press, Washington, D.C., 1. https://doi.org/10.1145/2335356.2335371

[15] Ana Ferreira, Jean-Louis Huynen, Vincent Koenig, Gabriele Lenzini, and Salvador Rivas. 2015. Do Graphical Cues Effectively Inform Users? In *Human Aspects of Information Security, Privacy, and Trust*, Theo Tryfonas and Ioannis Askoxylakis (Eds.). Vol. 9190. Springer International Publishing, Cham, 323–334. https://doi.org/10.1007/978-3-319-20376-8_29

[16] Simson Garfinkel and Heather Richter Lipford. 2014. *Usable Security : History, Themes, and Challenges*. Morgan & Claypool Publishers, San Rafael, United States.

[17] Dieter Gollmann, Cormac Herley, Vincent Koenig, Wolter Pieters, and Martina Angela Sasse. 2015. Socio-Technical Security Metrics (Dagstuhl Seminar 14491). *Dagstuhl reports* 4, 12 (2015), 28.

[18] Marc Hassenzahl. 2008. User experience (UX): towards an experiential perspective on product quality. In *Proceedings of the 20th Conference on l'Interaction Homme-Machine*. ACM, 11–15.

[19] Marc Hassenzahl, Sarah Diefenbach, and Anja Göritz. 2010. Needs, affect, and interactive products - Facets of user experience. *Interacting with Computers* 22, 5 (Sept. 2010), 353–362. https://doi.org/10.1016/j.intcom.2010.04.002

[20] Marc Hassenzahl, Kai Eckoldt, Sarah Diefenbach, Matthias Laschke, Eva Len, and Joonhwan Kim. 2013. Designing moments of meaning and pleasure. Experience design and happiness. *International Journal of Design* 7, 3 (2013).

[21] Frederick Herzberg. 1976. One More Time: How Do You Motivate Employees? In *Job Satisfaction - A Reader*, Michael M. Gruneberg (Ed.). Palgrave Macmillan UK, London, 17–32. https://doi.org/10.1007/978-1-349-02701-9_2

[22] Karen Holtzblatt and Hugh Beyer. 2016. *Contextual design: Design for life*. Morgan Kaufmann.

[23] James Kalbach. 2016. *Mapping experiences: A complete guide to creating value through journeys, blueprints, and diagrams*. " O'Reilly Media, Inc.".

[24] René F. Kizilcec. 2016. How Much Information?: Effects of Transparency on Trust in an Algorithmic Interface. ACM Press, 2390–2395. https://doi.org/10.1145/2858036.2858402

[25] Jesper Kjeldskov and Mikael B. Skov. 2007. Studying Usability In Sitro: Simulating Real World Phenomena in Controlled Environments. *International Journal of Human-Computer Interaction* 22, 1-2 (April 2007), 7–36. https://doi.org/10.1080/10447310709336953

[26] Carine Lallemand and Vincent Koenig. 2017. Lab Testing Beyond Usability: Challenges and Recommendations for Assessing User Experiences. *Journal of Usability Studies* 12, 3 (2017), 133–154.

[27] Bettina Laugwitz, Theo Held, and Martin Schrepp. 2008. Construction and Evaluation of a User Experience Questionnaire. In *HCI and Usability for Education and Work*, Andreas Holzinger (Ed.). Vol. 5298. Springer Berlin Heidelberg, Berlin, Heidelberg, 63–76. https://doi.org/10.1007/978-3-540-89350-9_6

[28] Sascha Mahlke. 2008. *User experience of interaction with technical systems*. Doctoral dissertation.

[29] Niels Raabjerg Mathiasen and Susanne Bodker. 2008. Threats or threads: from usable security to secure experience?. In *Proceedings of the 5th Nordic conference on Human-computer interaction: building bridges*. ACM, 283–289.

[30] Raydel Montesino and Stefan Fenz. 2011. Information Security Automation: How Far Can We Go?. In *2011 Sixth International Conference on Availability, Reliability and Security*. IEEE, Vienna, Austria, 280–285. https://doi.org/10.1109/ARES.2011.48

[31] Donald A. Norman. 2009. When security gets in the way. *interactions* 16, 6 (Nov. 2009), 60. https://doi.org/10.1145/1620693.1620708

[32] Maina Olembo and Melanie Volkamer (Eds.). 2013. *Human-Centered System Design for Electronic Governance: Lessons for Interface Design, User Studies, and Usability Criteria*. IGI Global. https://doi.org/10.4018/978-1-4666-3640-8

[33] Jakob Illeborg Pagter and Marianne Graves Petersen. 2007. A Sense of Security in Pervasive Computing - Is the Light on When the Refrigerator Door Is Closed?. In *International Conference on Financial Cryptography and Data Security*. Springer, 383–388.

[34] Leysia Palen and Paul Dourish. 2003. Unpacking "Privacy" for a Networked World. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 129–136.

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

[36] V Roto, E Law, A Vermeeren, and J Hoonhout. 2011. User Experience White Paper. In *Result from Dagstuhl Seminar on Demarcating User Experience, September 15 - 18, 2010*. 12.

[37] Peter YA Ryan, Peter B. Rønne, and Vincenzo Iovino. 2016. Selene: Voting with transparent verifiability and coercion-mitigation. In *International Conference on Financial Cryptography and Data Security*. Springer, 176–192.

[38] Stuart E. Schechter, Rachna Dhamija, Andy Ozment, and Ian Fischer. 2007. The Emperor's New Security Indicators. IEEE, 51–65. https://doi.org/10.1109/SP.2007.35

[39] Martin Schrepp. 2018. User Experience Questionnaire Handbook. (2018), 15.

[40] IBM Security Services. 2018. *The 2018 Cost of a Data Breach Study by the Ponemon Institute.* Technical Report.

[41] Kennon M. Sheldon, Andrew J. Elliot, Youngmee Kim, and Tim Kasser. 2001. What is satisfying about satisfying events? Testing 10 candidate psychological needs. *Journal of personality and social psychology* 80, 2 (2001), 325.

[42] S.W. Smith. 2003. Humans in the loop: Human-computer interaction and security. *IEEE Security & Privacy Magazine* 1, 3 (May 2003), 75–79. https://doi.org/10.1109/MSECP.2003.1203228

[43] Andreas Sotirakopoulos, Kirstie Hawkey, and Konstantin Beznosov. 2011. On the challenges in usable security lab studies: lessons learned from replicating a study on SSL warnings. In *Proceedings of the Seventh Symposium on Usable Privacy and Security*. ACM, 3.

[44] Marco Winckler, Regina Bernhaupt, Philippe Palanque, David Lundin, Kieran Leach, Peter Ryan, Eugenio Alberdi, and Lorenzo Strigini. 2009. Assessing the usability of open verifiable e-voting systems: a trial with the system Prêt à Voter. In *Proceedings of ICE-GOV*. https://www.irit.fr/page-perso/Marco.Winckler/publications/2009-ICEGOV.pdf

[45] Ka-Ping Yee. 2002. User interaction design for secure systems. In *International Conference on Information and Communications Security*. Springer, 278–290.