

# Designing Trustworthy User Interfaces

Valentin Zieglmeier  
Technical University of Munich  
Munich, Germany  
valentin.zieglmeier@tum.de

Antonia Maria Lehene  
Technical University of Munich  
Munich, Germany  
antonia.lehene@tum.de

## ABSTRACT

Interface design can directly influence trustworthiness of a software. Thereby, it affects users' intention to use a tool. Previous research on user trust has not comprehensively addressed user interface design, though. We lack an understanding of what makes interfaces trustworthy (1), as well as actionable measures to improve trustworthiness (2).

We contribute to this by addressing both gaps. Based on a systematic literature review, we give a thorough overview over the theory on user trust and provide a taxonomy of factors influencing user interface trustworthiness. Then, we derive concrete measures to address these factors in interface design. We use the results to create a proof of concept interface. In a preliminary evaluation, we compare a variant designed to elicit trust with one designed to reduce it. Our results show that the measures we apply can be effective in fostering trust in users.

## CCS CONCEPTS

• **Human-centered computing** → **Human computer interaction (HCI); Graphical user interfaces; User studies.**

## KEYWORDS

User trust, User-centered design, Taxonomy, Systematic literature review, Proof of concept

### ACM Reference Format:

Valentin Zieglmeier and Antonia Maria Lehene. 2021. Designing Trustworthy User Interfaces. In *33rd Australian Conference on Human-Computer Interaction (OzCHI '21)*, November 30–December 2, 2021, Melbourne, VIC, Australia. ACM, New York, NY, USA, 8 pages. <https://doi.org/10.1145/3520495.3520525>

## 1 INTRODUCTION

When creating software tools with user-facing interfaces, one of the central aspects to consider is how they are designed. As this is the component that users are directly exposed to, it can shape their impression of the tool and willingness to use it. How trustworthy the software appears at first glance may play an important role in this. User trust has been shown to influence users' intention to use a software [50]. Furthermore, central trust antecedents, such as credibility, increase intention to use as well [66]. Previous research suggests that trust constructs may even have a higher influence on

intention to use than some usability aspects [87]. Beyond the actual service or underlying implementation, the design of the interface has been shown to play an important role in the trustworthiness of a software tool [72]. Yet, to the best of our knowledge, no comprehensive overview over the relevant trust constructs and how they can be concretely addressed with the design of user interfaces exists today.

Our goal is to derive how (initial) user trust can be achieved and improved through user interface design. For this purpose, general influences on user trust for various usage contexts are summarized. Additionally, we analyze the interactions of these factors, as well as how they can be implemented in user interfaces in order to initiate user trust. In a preliminary empirical study, we assess whether a proof of concept design developed according to our findings can in fact increase user trust as we expect it.

Therefore, this work contributes a theoretical overview over user trust formation and factors in software design, summarizes actionable design variants to improve the trustworthiness of a software tool through its user interface, and provides preliminary evaluation results on the effectiveness of the developed software design variants.

## 2 SYSTEMATIC LITERATURE REVIEW

From literature reviews in the field of user experience and trust [1, 34, 35, 39, 41], we derived central terms used in research on trust in automation. These terms were used to build queries for a systematic literature review covering Scopus and Web of Science. This meant we included works that focus on individual factors related to trust. For each term, we built a query of the form ("user trust") AND (<term> OR <synonyms>) AND NOT ("social media" OR "blockchain"). For the search terms and synonyms we used, refer to Table 1. We explicitly excluded works with the terms "social media" and "blockchain", as we found that these often consider users' trust in each other, rather than in the respective tool. The search covered title, abstract, and keywords. We limited the results to English language journal articles and conference papers in the area of computer science.

In total, 697 works were found. Through a title and abstract review, we filtered for papers related to our research. This left us with 162 remaining works. These, plus 40 works that we added through snowballing, were read and analyzed. The following sections summarize the results from the most relevant of these works.

## 3 FUNDAMENTALS: USER TRUST

To better understand our findings, it is important to grasp what the concept of user trust encompasses. Furthermore, it is instructive to consider how trust is built and maintained, as the trust relationship is dynamic. User trust can be defined using different approaches.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from [permissions@acm.org](mailto:permissions@acm.org).

*OzCHI '21, November 30–December 2, 2021, Melbourne, VIC, Australia*

© 2021 Copyright held by the owner/author(s). Publication rights licensed to ACM.

ACM ISBN 978-1-4503-9598-4/21/11...\$15.00

<https://doi.org/10.1145/3520495.3520525>

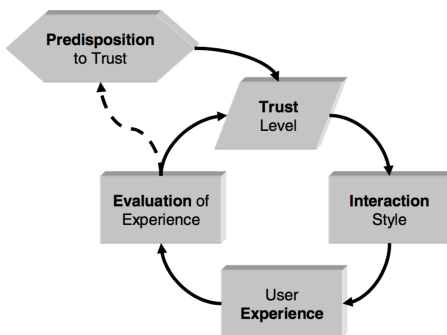
**Table 1: Terms and synonyms used in the search queries.**

Term	Synonyms
interface design	aesthetics
intention to use	tool adoption
perceived credibility	authenticity
functionality	reliability, accuracy
usability	user satisfaction
learnability	learning method
predictability	consistency
perceived security	—
personalization	customization
preference	—
familiarity	previous experience
feedback	communication

In the following, we describe various aspects to understand and classify it.

*Affect-based and cognitive trust.* First, we can differentiate between the type of processing, specifically between affect-based and cognitive trust. Cognitive trust is based on users' perception of system reliability, relating to logical reasoning [16, 91]. Affect-based or emotional trust on the other hand is influenced by their perception of the system's aesthetics and subjective beauty, relating to users' feelings [16, 50, 59]. In general, affect-based trust seems to have greater impact on overall trust [91], but may be indirectly influenced by cognitive trust levels [50].

*Trust life cycle.* Next, we consider the stages in the trust relationship. This can be likened to a life cycle [15], with initial trust transforming into long-term trust with continued use of a system [16]. Trust can be initially fostered, increased, decreased, lost, and regained [16, 68]. In our work, we focus on initial trust, yet it is just as important to maintain continued user trust through the trust life cycle (see Figure 1).

**Figure 1: Constantine's feedback model of trust in user-system interaction [15].**

*Influences on user trust.* Finally, we zoom out to recognize external influences on user trust that lie outside our control as system designers. *User criteria* are individual factors that differ between

users. These encompass the predisposition or propensity to trust (see Figure 1 and, e.g., [15, 60, 61]), past experiences and familiarity with a software [47, 50], culture [13, 18, 19], and other individual factors such as mental state [41]. Influencing factors extend beyond an individual, also encompassing their *environment*. While these are still somewhat individual, different users may experience them the same way. Examples are the specific task or work environment [41], word of mouth [12], other factors relating to the usage environment [65], or, importantly, the cultural context [13, 14, 18, 19, 23].

## 4 TRUSTWORTHINESS FACTORS IN INTERFACE DESIGN

To understand how to affect user trust through user interface design, we differentiate between trustworthiness factors, or antecedents. We describe factors that can be influenced directly through interface design changes. In previous works, no such overview exists. Therefore, we summarize and combine different taxonomies and classifications of user trust. For each factor in our list, we reference the taxonomies that include it. We selected only those factors for which we found concrete examples in literature describing how they can be addressed through user interface design. Those examples, comprising exemplary instantiations and empirical evaluations, are referenced as well. The result is a robust taxonomy of trustworthiness factors in interface design (see Table 2).

We differentiate between trustworthiness factors by assigning them to the (perceived) purpose, process, and performance of the system [41, 53, 54].

### 4.1 Purpose dimension

The *purpose* of the system depends on its intended use [41]. Trustworthiness factors related to this dimension reflect the impression of the designer's intentions that users get from interacting with the system [44, 54].

*Benevolence.* The trust relationship depends fundamentally on users' belief in benevolence from the trustee, in our case the system [15]. A benevolent system handles user data with care and respects users actions [15].

*Credibility.* Also referred to as honesty or sincerity, this factor refers to the perceived believability of the system [27]. To design a credible system, its interface should be built in accordance to users' expectations and mental models [27].

*Perceived security.* While many factors depend on user perceptions, this one is solely determined by it. Through, e.g., a more complex authentication process [90] or visible data security statements in the interface [43], users' sense of security can be improved.

### 4.2 Process dimension

The *process* dimension describes how the system operates [41]. These factors are defined by users' perception of how appropriate the system design is for its stated purpose [44, 54].

*Integrity.* Reflects users' impression of the values underlying the system design [81], and their belief that the designers acted ethically and fulfill their promises [38]. For example, certification badges or brand images can convey this [81].

**Table 2: Trustworthiness factors identified in literature. *Taxonomies* lists all found taxonomies or theoretical models that include this factor. *Examples* lists exemplary instantiations or empirical evaluations of this factor.**

Dimension	Factor	Taxonomies	Examples
Purpose	Benevolence	[15, 54, 77, 81]	[12, 37, 42, 79]
	Credibility	[27, 85]	[17, 25, 33, 40]
	Perceived security	[48, 49, 82]	[2, 11, 48, 49]
Process	Integrity	[28, 46, 54, 77, 81]	[12, 43, 48, 49]
	Predictability	[15, 28, 35, 54, 77, 81]	[43, 70, 73, 79]
	Transparency	[15, 28, 31, 35, 41, 54, 77]	[5, 33, 64]
	Familiarity	[21, 28, 31, 46, 49]	[7, 30, 45, 71]
	Communication	[28, 35, 41, 62]	[5, 43, 58, 75]
	Usability	[21, 41, 48, 49, 54, 81, 82]	[26, 52, 55, 73]
	Personalization	[8, 49, 77, 82]	[50, 56]
Performance	Competence	[15, 28, 31, 49, 54, 77, 81, 82]	[7, 43, 50, 70]
	Reliability	[28, 31, 35, 41, 46, 54, 68, 77, 81]	[13, 33, 64, 80]
	Validity	[31, 35, 41, 69, 77, 82]	[42, 80]

*Predictability.* A fundamental facet of trustworthiness, reflected in the consistency of the behavior and design of the system [15]. This allows users to predict the system’s future actions [43].

*Transparency.* This means informing the user about the tool, specifically what it does and how it works [41, 74]. Nicely summarized as “the user interface parallel to honesty in human relationships” [15, p. 24].

*Familiarity.* If a system is not necessarily predictable or transparent, users’ familiarity with it can also help them in understanding it [28]. Even if the concrete system is new, following established patterns or designs can foster this [45].

*Communication.* While transparency requires the system to make information easily available and understandable, its communication reflects how it actively engages users [41, 62]. Explicit feedback [5], with short, clear, non-intrusive messages [62] and a positive communication style [58] seem to be preferable.

*Usability.* A multi-faceted construct broadly concerning the quality of the tool in enabling individuals to use it. Multiple usability factors can also elicit trust [43], specifically the ease of use [48], ease of navigation [73], and learnability [3].

*Personalization.* The perception of users how well the system is personalized to their needs [50]. This can be achieved by allowing them to actively customize the tool [81]. Alternatively, it can be accomplished by learning their needs automatically and reacting to them [50], e.g. by providing a list of their most commonly used functions for quick access.

### 4.3 Performance dimension

The *performance* of the system reflects how well the system solves its tasks [41]. Users judge what the system does and if it can help them achieve their goals [44, 54].

*Competence.* The primary performance measure, indicating if a system is capable to achieve its task well. This includes not just the quality of the results, but also the time it takes to deliver them [15].

*Reliability.* The consistency of the functions of the system [41, 44], which can also be beneficial for its predictability. A reliable system

completes its tasks consistently, while a predictable system operates in ways that users expect [41].

*Validity.* The degree to which the tasks are completed by the system as intended by the user [41]. A low reliability will incur a lowered validity as well.

## 5 DESIGNING USER INTERFACES TO ELICIT TRUST

The factors described above are influential when trying to foster user trust. They are, however, fairly abstract concepts. To address them with a user interface, we require concrete and actionable measures. In the following, we describe how to systematically improve trustworthiness of an interface through exemplary measures that directly target these factors in order to elicit trust. We do not cover the factors of the *performance* dimension below, though. While they can be addressed through interface design, we found more effective measures seem to include modifications to the underlying system that are out of scope for this work.

Targeting perceived *benevolence*, the system should be built to be responsive to users and convey a sense of care [15]. For example, caching user input for repeated entry [15] or providing advice when necessary [37] can communicate this.

For *credibility*, the foundational work by Fogg and Tseng serves as a guide. Regarding the interface, they define the display as well as the interaction experience as relevant aspects. Their suggestion is to match users’ expectations of the system [27, p. 85]. This is use case specific and could be evaluated before development through surveys or similar instruments. Generally, choosing text-based (compared to anthropomorphic or audible) interfaces seems to increase credibility for users [10, 84]. Additionally, reducing the complexity of the interface is beneficial [84].

The *perceived security* can be improved through security assurances. A simple, yet effective, measure is to explicitly display details on the security measures, such as that encryption is performed or that data are being verified [20]. While this does not change the actual steps performed in the code, it raises awareness in users

which increases their perceived security [20]. Furthermore, forcing users to re-login after a certain period [90] and informing users that unauthorized accesses are blocked [63, 90] can improve this. These findings can be summarized as actively making users aware of the (ostensible) security measures that are implemented.

For *integrity*, the interface ideally conveys the ethics of the designers. This can be achieved by adding e.g. certification badges or brand images [81] that suggest an ethics code or value system.

The *predictability* of the interface can be achieved following the guidelines set forth by Gram. They suggest deterministic design that maps the observable state directly to system events, with the system providing users with information about its state and the actions they can take. Furthermore, they describe completeness and consistency of information display as important [32, p. 296].

Increasing the *transparency* that users experience can be a vital aspect. As a basic measure, explanatory texts should make clear what functionality exists [9]. Especially for safety-relevant scenarios, the system should also be transparent about the risks and limitations of its functions [17, 51, 70].

Evoking *familiarity* is of course very dependent on the users' previous experience. Still, just by following established design patterns and metaphors, users' familiarity with them can be evoked [45].

Regarding *communication*, short and clear notifications about the status of the system serve to inform users [23, 81]. When designing these messages, etiquette are important [54, 67, 89]. These can be defined as being non-interrupting and patient [67], as well as having a positive tone [36].

The *usability* of a user interface is a more complex topic and its own branch of research. Yet, from works addressing usability as an antecedent of trust specifically, we can derive some concrete suggestions. First, ease of navigation and user guidance are beneficial [23, 73, 76]. Similarly, consistency in design and color schemes improves usability and trustworthiness [19, 23, 81]. For non-intuitive interfaces, learnability was found to be effective [6, 73, 76]. This can mean giving users the opportunity to learn about the functions of the system and encouraging them to explore it [6]. If training is required, tools can directly embed tutorials to ease discovery [83]. Additionally, the ease of use and subjective appeal of the interface can be relevant [29, 78, 86]. Beyond generally aiming to reduce the required cognitive effort, this can mean improving the reaction speed [86], reducing clutter and animations [29], and designing a layout with, e.g., high classical aesthetic appeal [78]. Finally, attractiveness as well as readable typography, covering font choice and text size, are also facets to consider [23, 24].

For *personalization*, various measures can be effective. Allowing customization of the interface to match the user needs [81] is a sensible step, while more advanced systems might try to predict user wishes [50].

## 6 PRELIMINARY EVALUATION

To assess the effectiveness of influencing trust through user interface design, we created a proof of concept interface for a preliminary evaluation. We developed two user interface variants: One variant aimed to follow our recommendations to elicit trust (variant A), the other explicitly disregarded our findings (variant B). Twelve people participated in our study (ten students, two apprentices;

eight female, four male). Each participant was asked to assess both variants. They had to register, then they were led to variant A. After exploring it and answering the questionnaire, they were then shown variant B. Finally, they answered the same questionnaire again to allow us to compare the results. Their responses were recorded on a seven-point Likert scale.

### 6.1 Design variants

We created two interface variants for participants to explore (see Figure 2). Both followed the same basic structure: They started with a login page where users had to authenticate, followed by the main page in form of a dashboard listing various data. The dashboard was designed for the use case of logging data usages [see, e.g., 4, 92], showing how data of the individual were accessed and by whom.

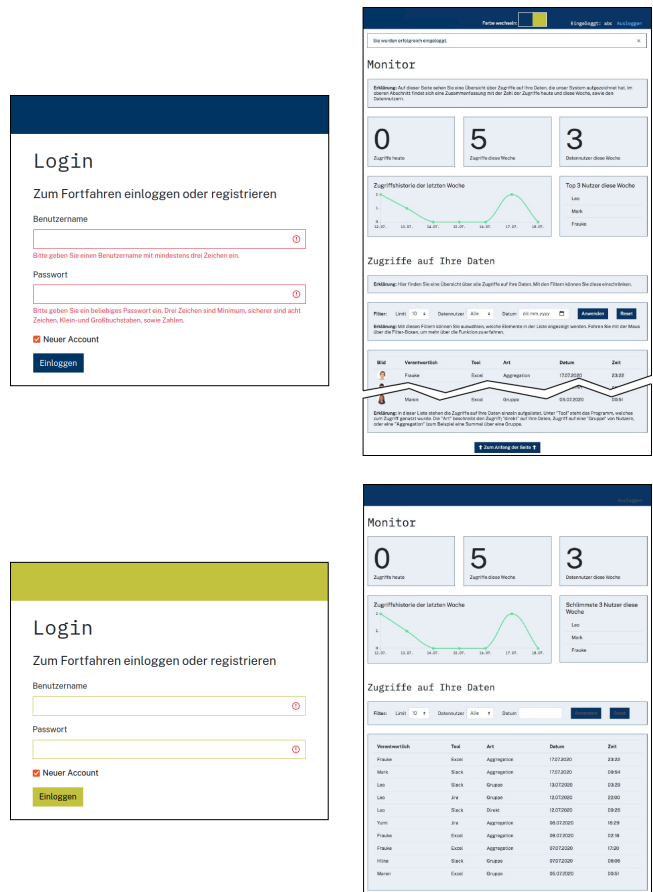


Figure 2: Screenshots of the two interface design variants. Variant A (above) was developed to elicit trust, variant B (below) to reduce it.

To target personalization, variant A offered a color scheme picker, while variant B did not. For transparency and communication, a message was displayed after successful login, with a status bar showing the logged-in user. Both were missing from variant B. A more positive communication style for variant A meant that it listed

the “best” users, instead of the “worst”, when showing who accessed the data most frequently. Improving predictability, a detailed description of available functions was shown only for variant A. Also, the same color scheme was used for the login page and dashboard, whereas for variant B it switched from yellow to blue. Finally, we targeted usability. To improve ease of navigation, variant A had a button at the bottom to return “back to top” that B did not have. Additionally, the “Log out” button on variant A was made easier to notice with brighter text. For ease of use and subjective appeal, the colors of text on buttons for variant B in general were made less legible compared to A, with a reduced contrast to the background color. Furthermore, a semaphore informing users how strong the password they selected was and if it was valid was shown on variant A, but not on B.

## 6.2 Questionnaire

Participants answered ten questions related to our design changes, with their responses being recorded on a seven-point Likert scale. Lower values on the scale indicate lower levels of agreement. We used questions developed and validated in previous works to evaluate trust.

Covering the induced familiarity and predictability, we asked:

- FP: I am familiar with how the system works [from 50].

For transparency, learnability, and communication, we asked:

- TLC: I find the system easy to learn to use [from 23].

Regarding their perceived security, we asked:

- PS: I think the authentication is very secure, that is, it protects me against attacks [from 93].

Addressing usability directly, we asked:

- U1: I find the system easy to use [from 17].
- U2: I can find easily what I am looking for on the interface [from 73].

To assess their faith in the system generally, we asked:

- F1: I believe advice from the system even when I don't know for certain that it is correct [from 57].
- F2: When I am uncertain about a decision I believe the system rather than myself [from 57].
- F3: If I am not sure about a decision, I have faith that the system will provide the best solution [from 57].

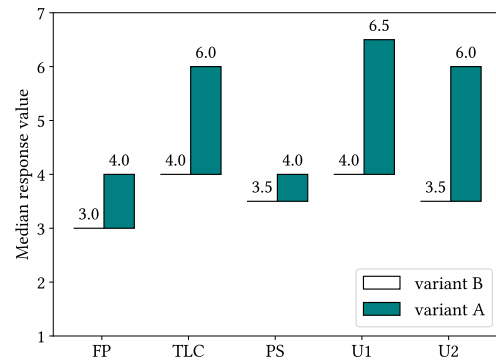
In addition, we asked participants about their trust and the perceived trustworthiness of the system directly:

- T1: I trust the system [from 17, 59].
- T2: I believe the system to be trustworthy [from 17, 22, 33].

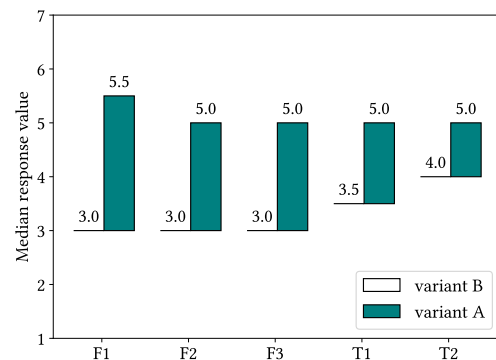
## 6.3 Results

We analyze the results by comparing the median value of all responses for variant A (eliciting trust) to variant B. We use the median instead of averaging the response values, as that can be problematic for ordinal data such as Likert responses. It prevents outliers from affecting the result while still allowing us to summarize the responses in a single value. For visualization, we use bar graphs [88].

For most trustworthiness factors, we find a clear increase in the median level of agreement (see Figure 3(a)). On average, the median



(a) Questions targeting trustworthiness factors.



(b) Questions targeting faith and trust broadly.

**Figure 3: Questionnaire results ( $n = 12$ ). The median of all responses for variant A (trust-eliciting) and variant B is compared.**

increased by 1.7 points, with the lowest increase (0.5) for question PS and the highest (2.5) for questions U1 and U2. This suggests that our changes had the greatest impact on usability. Considering questions FP and TLC, we find an interesting difference: participants seemingly did not understand how the system worked when they first used it, but may have found they could learn to do so. The low difference for question PS seems plausible, as our modifications did not explicitly target perceived security and both variants used the same authentication process.

Considering the overarching goal of trust and the related construct of faith, we also find noticeable increases in the median level of agreement (see Figure 3(b)). The average increase is 1.8 points, with the lowest (1) for question T2 and the highest (2.5) for question F1. For variant A, we can see that the median is stable at 5, except for F1 with 5.5. This means that participants did not overwhelmingly agree with the questions, but showed a clear tendency towards agreement. The lower increase for question T2 is not due to variant A being less trustworthy, but due to variant B seemingly also eliciting some trust in participants. In all, this suggests that our changes had the impact we aimed for.

## 7 DISCUSSION

At first glance, aiming to elicit trust in users solely through interface design may seem counterintuitive. Surely, confidence in a system should arise from actual and verifiable properties of the system. Yet at the same time, it seems clear that laypeople will not be able to verify such system properties in many cases. Therefore, their trust is required even then, e.g. in a third party auditor or the developers. Instead, we believe that trust in software is important to consider on its own. Based on our findings, initial trust in a tool can be fundamentally influenced by user interface design. That means that deliberate design is beneficial and in some cases necessary to elicit trust in the developed tool.

The results from our preliminary evaluation seem to confirm our hypothesis. With very few adjustments to a proof of concept interface compared to our control, we found a noticeable increase in perceived trustworthiness by users. Our evaluation is limited, though. Only twelve participants were part of the study, and they were shown both interface variants. That means that we can neither exclude the influence of individual characteristics, nor an exaggerated effect by participants being able to compare the variants. For future work, we therefore suggest expanding on these ideas and conducting a more robust and in-depth evaluation. In addition to expanding the set of participants, assessing their individual predisposition to trust before the evaluation may help in understanding some differences in the responses. Finally, of course, we hope our work will serve to guide and support the design of trustworthy user interfaces.

## ACKNOWLEDGMENTS

This work was supported by the German Federal Ministry of Education and Research (BMBF) under grant no. 5091121.

## REFERENCES

- [1] Raja Naeem Akram, Hsiao-Hwa Chen, Javier Lopez, Damien Sauveron, and Laurence T. Yang. 2018. Security, privacy and trust of user-centric solutions. *Future Generation Computer Systems* 80 (2018), 417–420.
- [2] Mansour Naser Alraja, Murtaza Mohiuddin Junaid Farooque, and Basel Khashab. 2019. The Effect of Security, Privacy, Familiarity, and Trust on Users' Attitudes Toward the Use of the IoT-Based Healthcare: The Mediation Role of Risk Perception. *IEEE Access* 7 (2019), 111341–111354.
- [3] Rui Alves and Nuno Jardim Nunes. 2016. Ceiling and Threshold of PaaS Tools: The Role of Learnability in Tool Adoption. In *Human-Centered and Error-Resilient Systems Development*, Cristian Bogdan, Jan Gulliksen, Stefan Sauer, Peter Forbrig, Marco Winckler, Chris Johnson, Philippe Palanque, Regina Bernhaupt, and Filip Kis (Eds.). Springer, Cham., 335–347.
- [4] Julio Angulo, Simone Fischer-Hübner, Tobias Pulls, and Erik Wästlund. 2015. Usable transparency with the Data Track: a tool for visualizing data disclosures. In *Proceedings of the 33<sup>rd</sup> ACM Conference Extended Abstracts on Human Factors in Computing Systems*. ACM, 1803–1808.
- [5] Stavros Antifakos, Nicky Kern, Bernt Schiele, and Adrian Schwaninger. 2005. Towards Improving Trust in Context-Aware Systems by Displaying System Confidence. In *Proceedings of the 7<sup>th</sup> International Conference on Human Computer Interaction with Mobile Devices & Services*. ACM, 9–14.
- [6] Beth F. Wheeler Atkinson, Troy O. Bennett, G. Susanne Bahr, and Melissa M. Walwanis Nelson. 2007. Development of a Multiple Heuristics Evaluation Table (MHET) to Support Software Development and Usability Analysis. In *Universal Access in Human Computer Interaction. Coping with Diversity*, Constantine Stephanidis (Ed.), Vol. 4554. Springer, Berlin, Heidelberg, 563–572.
- [7] Grace M. Begany, Ning Sa, and Xiaojun Yuan. 2015. Factors Affecting User Perception of a Spoken Language vs. Textual Search Interface: A Content Analysis. *Interacting with Computers* 28, 2 (2015), 170–180.
- [8] Regina Bernhaupt. 2010. Usability and user experience evaluation methods. In *Mass Customization for Personalized Communication Environments: Integrating Human Factors*, Constantinos Mourlas and Panagiotis Germanakos (Eds.). IGI Global, Chapter 13, 232–243.
- [9] Emilie Bigras, Marc-Antoine Jutras, Sylvain Sénécal, Pierre-Majorique Léger, Chrystel Black, Nicolas Robitaille, Karine Grande, and Christian Hudon. 2018. In AI We Trust: Characteristics Influencing Assortment Planners' Perceptions of AI Based Recommendation Agents. In *HCI in Business, Government, and Organizations*, Fiona Fui-Hoon Nah and Bo Sophia Xiao (Eds.). Springer, Cham., 3–16.
- [10] Judee K. Burgoon, Joseph A. Bonito, Bjorn Bengtsson, Carl Cederberg, Magnus Lundberg, and Lisa Allsop. 2000. Interactivity in human-computer interaction: a study of credibility, understanding, and influence. *Computers in Human Behavior* 16, 6 (2000), 553–574.
- [11] Yu-Hui Chen and Stuart J. Barnes. 2007. Initial trust and online buyer behaviour. *Industrial Management and Data Systems* 107, 1 (2007), 21–36.
- [12] Christy M. K. Cheung and Matthew K. O. Lee. 2008. Online consumer reviews: Does negative electronic word-of-mouth hurt more?. In *Proceedings of the 14<sup>th</sup> Americas Conference on Information Systems*, Vol. 5. 3242–3251.
- [13] Shih-Yi Chien, Michael Lewis, Katia Sycara, Jyi-Shane Liu, and Asiye Kumru. 2018. The Effect of Culture on Trust in Automation: Reliability and Workload. *ACM Transactions on Interactive Intelligent Systems* 8, 4 (2018).
- [14] Shih-Yi Chien, Zehleh Semmani-Azad, Michael Lewis, and Katia Sycara. 2014. Towards the Development of an Inter-cultural Scale to Measure Trust in Automation. In *Cross-Cultural Design*, P. L. Patrick Rau (Ed.). Springer, Cham., 35–46.
- [15] Larry L. Constantine. 2006. Trusted Interaction: User Control and System Responsibilities in Interaction Design for Information Systems. In *Advanced Information Systems Engineering*, Eric Dubois and Klaus Pohl (Eds.). Springer, Berlin, Heidelberg, 20–30.
- [16] Cynthia L. Corritore, Beverly Kracher, and Susan Wiedenbeck. 2003. On-line trust concepts, evolving themes, a model. *International Journal of Human-Computer Studies* 58, 6 (2003), 737–758.
- [17] Cynthia L. Corritore, Robert P. Marble, Susan Wiedenbeck, Beverly Kracher, and Ashwin Chandran. 2005. Measuring online trust of websites: Credibility, perceived ease of use, and risk. In *Proceedings of the 11<sup>th</sup> Americas Conference on Information Systems*, Vol. 5. AIS, 2419–2427.
- [18] Dianne Cyr. 2013. Website Design, Trust and Culture: An Eight Country Investigation. *Electronic Commerce Research and Applications* 12, 6 (2013), 373–385.
- [19] Dianne Cyr, Milena Head, and Hector Larios. 2010. Colour appeal in website design within and across cultures: A multi-method evaluation. *International Journal of Human-Computer Studies* 68, 1 (2010), 1–21.
- [20] Verena Distler, Marie-Laure Zollinger, Carine Lallemand, Peter B. Roenne, Peter Y. A. Ryan, and Vincent Koenig. 2019. Security - visible, yet unseen?. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, 1–13.
- [21] Yongqin Du and Jin Zhao. 2009. An Empirical Study of End-User Trust in a Web Information System. In *Proceedings of the 2009 International Conference on Information Management, Innovation Management and Industrial Engineering*, Vol. 2. 561–564.
- [22] Andrea Everard and Dennis F. Galletta. 2006. How Presentation Flaws Affect Perceived Site Quality, Trust, and Intention to Purchase from an Online Store. *Journal of Management Information Systems* 22, 3 (2006), 55–95.
- [23] C. M. Nadeem Faisal, Martin Gonzalez-Rodriguez, Daniel Fernandez-Lanvin, and Javier de Andres-Suarez. 2017. Web Design Attributes in Building User Trust, Satisfaction, and Loyalty for a High Uncertainty Avoidance Culture. *IEEE Transactions on Human-Machine Systems* 47, 6 (2017), 847–859.
- [24] Julie Fisher, Frada Burstein, Kathy Lynch, and Kate Lazarenko. 2008. "Usability plus usefulness = trust": an exploratory study of Australian health web sites. *Internet Research* 18, 5 (2008), 477–498.
- [25] Andrew J. Flanagin and Miriam J. Metzger. 2007. The role of site features, user attributes, and information verification behaviors on the perceived credibility of web-based information. *New Media & Society* 9, 2 (2007), 319–342.
- [26] Carlos Flavián, Miguel Guinali, and Raquel Gurrea. 2006. The role played by perceived usability, satisfaction and consumer trust on website loyalty. *Information & Management* 43, 1 (2006), 1–14.
- [27] Brian J. Fogg and Hsiang Tseng. 1999. The Elements of Computer Credibility. In *Proceedings of the 1999 SIGCHI Conference on Human Factors in Computing Systems*. ACM, 80–87.
- [28] Bronwyn French, Andreas Duenser, and Andrew Heathcote. 2018. *Trust in automation - a literature review*. Technical Report EP184082. CSIRO.
- [29] Yuan Gao. 2005. Factors influencing user trust in online games. *Electronic Library* 23, 5 (2005), 533–538.
- [30] David Gefen. 2000. E-commerce: the role of familiarity and trust. *Omega* 28, 6 (2000), 725–737.
- [31] P. Goillau, C. Kelly, M. Boardman, and Emmanuelle Jeannot. 2003. *Guidelines for trust in future ATM systems: measures*. Technical Report HRS/HSP-005-GUI-02. European Air Traffic Management Programme.
- [32] Christian Gram. 1996. A software engineering view of user interface design. In *Proceedings of the 1995 IFIP International Conference on Engineering for Human-Computer Interaction*. Springer, 293–306.



- [33] Stephan Hammer, Michael Wißner, and Elisabeth André. 2015. Trust-based decision-making for smart and adaptive environments. *User Modeling and User-Adapted Interaction* 25 (2015), 267–293.
- [34] Peter A. Hancock, Deborah R. Billings, and Kristin E. Schaefer. 2011. Can You Trust Your Robot? *Ergonomics in Design* 19, 3 (2011), 24–29.
- [35] Peter A. Hancock, Deborah R. Billings, Kristin E. Schaefer, Jessie Y. C. Chen, Ewart J. de Visser, and Raja Parasuraman. 2011. A Meta-Analysis of Factors Affecting Trust in Human-Robot Interaction. *Human Factors* 53, 5 (2011), 517–527.
- [36] Jan Hartmann, Antonella De Angeli, and Alistair Sutcliffe. 2008. Framing the User Experience: Information Biases on Website Quality Judgement. In *Proceedings of the 2008 SIGCHI Conference on Human Factors in Computing Systems*. ACM, 855–864.
- [37] Tracy Harwood and Tony Garry. 2017. Internet of Things: Understanding trust in techno-service systems. *Journal of Service Management* 28, 3 (2017), 442–475.
- [38] Zahid Hasan, Alina Krischkowsky, and Manfred Tscheligi. 2012. Modelling user-centered-trust (UCT) in software systems: interplay of trust, affect and acceptance model. In *Proceedings of the 5<sup>th</sup> International Conference on Trust and Trustworthy Computing*. Springer, 92–109.
- [39] Marc Hassenzahl and Noam Tractinsky. 2006. User experience – a research agenda. *Behaviour & Information Technology* 25, 2 (2006), 91–97.
- [40] Milena M. Head and Khaled Hassanein. 2002. Trust in e-Commerce: Evaluating the Impact of Third-Party Seals. *Quarterly Journal of Electronic Commerce* 3, 3 (2002), 307–325.
- [41] Kevin Anthony Hoff and Masooda Bashir. 2015. Trust in Automation: Integrating Empirical Evidence on Factors That Influence Trust. *Human Factors* 57, 3 (2015), 407–434.
- [42] Robert R. Hoffman, Matthew Johnson, Jeffrey M. Bradshaw, and Al Underbrink. 2013. Trust in Automation. *IEEE Intelligent Systems* 28, 1 (2013), 84–88.
- [43] Axel Hoffmann, Holger Hoffmann, and Matthias Söllner. 2013. Fostering Initial Trust in Applications - Developing and Evaluating Requirement Patterns for Application Websites. In *Proceedings of the 21<sup>st</sup> European Conference on Information Systems*. AIS.
- [44] Holger Hoffmann and Matthias Söllner. 2014. Incorporating Behavioral Trust Theory into System Development for Ubiquitous Applications. *Personal Ubiquitous Comput.* 18, 1 (2014), 117–128.
- [45] Andreas Holzinger, Gig Searle, and Michaela Wernbacher. 2011. The effect of previous exposure to technology on acceptance and its importance in usability and accessibility engineering. *Universal Access in the Information Society* 10, 3 (2011), 245–260.
- [46] Jiun-Yin Jian, Ann M. Bisantz, and Colin G. Drury. 2000. Foundations for an empirically determined scale of trust in automated systems. *International Journal of Cognitive Ergonomics* 4, 1 (2000), 53–71.
- [47] Catholijn M. Jonker, Joost J. P. Schalken, Jan Theeuwes, and Jan Treur. 2004. Human Experiments in Trust Dynamics. In *Trust Management*, Christian Jensen, Stefan Poslad, and Theo Dimitrakos (Eds.). Springer, Berlin, Heidelberg, 206–220.
- [48] Myoung-Soo Kim and Jae-Hyeon Ahn. 2007. Management of Trust in the E-Marketplace: The Role of the Buyer's Experience in Building Trust. *Journal of Information Technology* 22, 2 (2007), 119–132.
- [49] Iacovos Kirlappos, M. Angela Sasse, and Nigel Harvey. 2012. Why Trust Seals Don't Work: A Study of User Perceptions and Behavior. In *Proceedings of the 5<sup>th</sup> International Conference on Trust and Trustworthy Computing*. Springer, Berlin, Heidelberg, 308–324.
- [50] Sherrie Y. X. Komiak and Izak Benbasat. 2006. The effects of personalization and familiarity on trust and adoption of recommendation agents. *MIS Quarterly* 30, 4 (2006), 941–960.
- [51] Alexander Kunze, Stephen J. Summerskill, Russell Marshall, and Ashleigh J. Filtness. 2019. Automation transparency: implications of uncertainty communication for human-automation interaction and interfaces. *Ergonomics* 62, 3 (2019), 345–360.
- [52] Dongwon Lee, Junghoon Moon, Yong Jin Kim, and Mun Y. Yi. 2015. Antecedents and consequences of mobile phone usability: Linking simplicity and interactivity to satisfaction, trust, and brand loyalty. *Information & Management* 52, 3 (2015), 295–304.
- [53] John Lee and Neville Moray. 1992. Trust, control strategies and allocation of function in human-machine systems. *Ergonomics* 35, 10 (1992), 1243–1270.
- [54] John D. Lee and Katrina A. See. 2004. Trust in Automation: Designing for Appropriate Reliance. *Human Factors* 46, 1 (2004), 50–80.
- [55] Kun Chang Lee and Namho Chung. 2009. Understanding factors affecting trust in and satisfaction with mobile banking in Korea: A modified DeLone and McLean's model perspective. *Interacting with Computers* 21, 5 (2009), 385–392.
- [56] Yanan Li and Yong Wang. 2013. Social Influence from Personalized Recommendations to Trusting Beliefs of Websites: Intermediate Role of Social Presence. In *Human-Computer Interaction – INTERACT 2013*, Paula Kotzé, Gary Marsden, Gitte Lindgaard, Janet Wesson, and Marco Winckler (Eds.). Springer, Berlin, Heidelberg, 632–639.
- [57] Maria Madsen and Shirley Gregor. 2000. Measuring human-computer trust. In *Proceedings of the 11<sup>th</sup> Australasian Conference on Information Systems*. 6–8.
- [58] Maral Mayeh, T. Ramayah, and Alok Mishra. 2016. The role of absorptive capacity, communication and trust in ERP adoption. *Journal of Systems and Software* 119 (2016), 58–69.
- [59] Stephanie M. Merritt. 2011. Affective Processes in Human-Automation Interactions. *Human Factors* 53, 4 (2011), 356–370.
- [60] Stephanie M. Merritt, Heather Heimbaugh, Jennifer LaChapell, and Deborah Lee. 2013. I Trust It, but I Don't Know Why: Effects of Implicit Attitudes Toward Automation on Trust in an Automated System. *Human Factors* 55, 3 (2013), 520–534.
- [61] Stephanie M. Merritt and Daniel R. Ilgen. 2008. Not All Trust Is Created Equal: Dispositional and History-Based Trust in Human-Automation Interactions. *Human Factors* 50, 2 (2008), 194–210.
- [62] Alexander G. Mirmig, Sandra Troesterer, Elke Beck, and Manfred Tscheligi. 2014. To trust or not to trust. In *Proceedings of the 2014 International Conference on Human-Centred Software Engineering*. 164–181.
- [63] Anthony D. Miyazaki and Ana Fernandez. 2000. Internet Privacy and Security: An Examination of Online Retailer Disclosures. *Journal of Public Policy & Marketing* 19, 1 (2000), 54–61.
- [64] Kenya Freeman Oduor and Christopher S. Campbell. 2007. Deciding When to Trust Automation in a Policy-Based City Management Game: Policity. In *Proceedings of the 2007 Symposium on Computer Human Interaction for the Management of Information Technology*. ACM, 2–es.
- [65] Kristin E. Oleson, Deborah R. Billings, Vivien Kocsis, Jessie Y. C. Chen, and Peter A. Hancock. 2011. Antecedents of trust in human-robot collaborations. In *Proceedings of the 2011 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support*. 175–178.
- [66] Chong-Shyong Ong, Jung-Yu Lai, and Yi-Shun Wang. 2004. Factors Affecting Engineers' Acceptance of Asynchronous e-Learning Systems in High-Tech Companies. *Information & Management* 41, 6 (2004), 795–804.
- [67] Raja Parasuraman and Christopher A. Miller. 2004. Trust and Etiquette in High-Criticality Automated Systems. *Commun. ACM* 47, 4 (2004), 51–55.
- [68] Raja Parasuraman and Victor Riley. 1997. Humans and Automation: Use, Misuse, Disuse, Abuse. *Human Factors* 39, 2 (1997), 230–253.
- [69] Jarutas Pattanaphanchai, Kieron O'Hara, and Wendy Hall. 2013. Trustworthiness Criteria for Supporting Users to Assess the Credibility of Web Information. In *Proceedings of the 22<sup>nd</sup> International Conference on World Wide Web*. ACM, 1123–1130.
- [70] LeeAnn Perkins, Janet E. Miller, Ali Hashemi, and Gary Burns. 2010. Designing for human-centered systems: Situational risk as a factor of trust in automation. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 54, 25 (2010), 2130–2134.
- [71] Antti Pirhonen. 2005. Supporting a User Facing a Novel Application: Learnability in OBE. *Personal and Ubiquitous Computing* 9, 4 (2005), 218–226.
- [72] Pearl Pu and Li Chen. 2007. Trust-inspiring explanation interfaces for recommender systems. *Knowledge-Based Systems* 20, 6 (2007), 542–556.
- [73] Marie Christine Roy, Olivier Dewit, and Benoit A. Aubert. 2001. The impact of interface usability on trust in Web retailers. *Internet Research: Electronic Networking Applications and Policy* 11, 5 (2001), 388–398.
- [74] Sebastian Schnorf, Martin Ortlieb, and Nikhil Sharma. 2014. Trust, Transparency & Control in Inferred User Interest Models. In *CHI '14 Extended Abstracts on Human Factors in Computing Systems*. ACM, 2449–2454.
- [75] Stephen R. Serge, Jonathan A. Stevens, and Latika Infert. 2015. Make It Usable: Highlighting the Importance of Improving the Intuitiveness and Usability of a Computer-Based Training Simulation. In *Proceedings of the 2015 Winter Simulation Conference*. IEEE, 1056–1067.
- [76] Elizabeth Sillence, Pam Briggs, Lesley Fishwick, and Peter Harris. 2004. Trust and Mistrust of Online Health Sites. In *Proceedings of the 2004 SIGCHI Conference on Human Factors in Computing Systems*. ACM, 663–670.
- [77] Matthias Söllner, Axel Hoffmann, Holger Hoffmann, and Jan Marco Leimeister. 2011. Towards a theory of explanation and prediction for the formation of trust in IT artifacts. In *Proceedings of the 10<sup>th</sup> Annual Workshop on HCI Research in MIS*. AIS, 1–5.
- [78] Andreas Sonderegger, Juergen Sauer, and Janine Eichenberger. 2014. Expressive and classical aesthetics: two distinct concepts with highly similar effect patterns in user-artefact interaction. *Behaviour & Information Technology* 33, 11 (2014), 1180–1191.
- [79] Sónia Sousa, Ilya Šmorgun, David Lamas, and Arman Arakelyan. 2014. A design space for trust-enabling interaction design. In *Proceedings of the 2014 International Conference on Multimedia, Interaction, Design and Innovation*. ACM, 1–8.
- [80] Nash S. Stanton, Stuart A. Ragsdale, and Ernesto A. Bustamante. 2009. The Effects of System Technology and Probability Type on Trust, Compliance, and Reliance. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 53, 18 (2009), 1368–1372.
- [81] Alistair Sutcliffe. 2006. Trust: From Cognition to Conceptual Models and Design. In *Advanced Information Systems Engineering*, Eric Dubois and Klaus Pohl (Eds.).

- Springer, Berlin, Heidelberg, 3–17.
- [82] Monideepa Tarafdar and Jie Zhang. 2005. Analyzing the Influence of Web Site Design Parameters on Web Site Usability. *Information Resources Management Journal* 18, 4 (2005), 62–80.
- [83] Bruce Tognazzini. 2014. First Principles of Interaction Design. <https://asktog.com/atc/principles-of-interaction-design/> Visited on 2020-07-09.
- [84] Kai-Ti Tseng and Yuan-Chi Tseng. 2014. The Correlation between Visual Complexity and User Trust in On-line Shopping: Implications for Design. In *Human-Computer Interaction. Applications and Services*, Masaaki Kurosu (Ed.). Springer, Cham., 90–99.
- [85] Shawn Tseng and B. J. Fogg. 1999. Credibility and Computing Technology. *Commun. ACM* 42, 5 (1999), 39–44.
- [86] Natalia Vila and Inés Kuster. 2011. Consumer feelings and behaviours towards well designed websites. *Information & Management* 48, 4 (2011), 166–177.
- [87] Yi-Shun Wang, Hsin-Hui Lin, and Pin Luarn. 2006. Predicting consumer intention to use mobile service. *Information Systems Journal* 16, 2 (2006), 157–179.
- [88] Jessica K. Witt. 2019. Introducing hat graphs. *Cognitive Research: Principles and Implications* 4, 1 (2019), 1–17.
- [89] Jie Xu, Kim Le, Annika Deitermann, and Enid Montague. 2014. How different types of users develop trust in technology: A qualitative analysis of the antecedents of active and passive user trust in a shared technology. *Applied Ergonomics* 45, 6 (2014), 1495–1503.
- [90] Mehmet M. Yenisey, A. Ant Ozok, and Gavriel Salvendy. 2005. Perceived security determinants in e-commerce among Turkish university students. *Behaviour & Information Technology* 24, 4 (2005), 259–274.
- [91] Beste F. Yuksel, Penny Collisson, and Mary Czerwinski. 2016. Brains or Beauty: How to Engender Trust in User-Agent Interactions. *ACM Transactions on Internet Technology* 17, 2 (2016).
- [92] Valentin Zieglmeier and Alexander Pretschner. 2021. Trustworthy transparency by design. arXiv:2103.10769 [cs.SE]
- [93] Verena Zimmermann and Nina Gerber. 2020. The password is dead, long live the password – A laboratory study on user perceptions of authentication schemes. *International Journal of Human-Computer Studies* 133 (2020), 26–44.