A User-Centered Model for Usable Security and Privacy

Denis Feth(✉), Andreas Maier, and Svenja Polst

Fraunhofer Institute for Experimental Software Engineering,
Kaiserslautern, Germany
{denis.feth, andreas.maier,
svenja.polst}@iese.fraunhofer.de
http://www.iese.fraunhofer.de

Abstract. Security, privacy and usability are vital quality attributes of IT systems and services. Users and legal authorities demand that systems are secure and preserve privacy. At the same time, security and privacy mechanisms should not complicate workflows and must be transparent for the user. In order to master this challenge, a close involvement of the users is necessary—both at development and at run-time. In this paper, we present a user-centered model for usable security and privacy that is aligned with user-centered design guidelines [34] and the Human-Centered Design process [28]. Based on this model, we present an initial method for the design of usable security systems. Through active involvement of the user, the model and the method are meant to help developers to identify and solve shortcomings of their security and privacy mechanisms. We motivate our work and present our results based on an Internet of Things/smart home scenario. Due to the amount of private data and strong data protection laws, both usability and privacy are of major importance in this domain. However, our model and method are not limited to the smart home domain, but can be applied whenever usable security and privacy are of particular interest for a system under development.

Keywords: Usability · Security · Privacy · Security modelling · User-centered design · Continuous improvement

1 Introduction

1.1 Context and Motivation

Security, privacy, and usability are important and inherent quality attributes of IT systems. However, it is often hard to optimize all attributes at the same time [8]. From the users' perspective, systems must be adequately secure and respect their privacy in order to be trustworthy. At the same time, the systems, especially the security mechanisms they provide, must be usable. However, security measures and privacy enhancing technologies are complex by nature and typically complicate workflows. Thus, they frequently have a negative impact on usability [45, 46], e.g. with respect to efficiency.

T. Tryfonas (Ed.): HAS 2017, LNCS 10292, pp. 74–89, 2017.
DOI: 10.1007/978-3-319-58460-7_6

1.2 Ideas and Contributions

We introduce a model that focuses on the user´s privacy as the bridging element of security and usability and which is aligned with the Human-Centered Design process. The U.S. Department of Health and Humans Services [40] defines privacy as "the control over the extent, timing, and circumstances of sharing oneself (physically, behaviorally, or intellectually) with others". As the perception of privacy is highly individual to each user, it will be a major challenge for IT corporations to get their users to understand and trust privacy measures. At the same time, the European Union´s "General Data Protection Regulation" [12] provides for fines up to 4% of the annual worldwide company turnover if the company lacks comprehensive privacy mechanisms. Gartzke and Roebel [22] state that "getting their approach to privacy right while remaining consumer friendly will be absolutely critical to their [both startups and established corporations] future." In that respect, we consider three relevant goals:

1. Adequate privacy enhancing technologies and control mechanisms for the protection of personal data must exist.
2. Control mechanisms must be made transparent for the users and be understood by them.
3. Users have to be capable of building an individual perception of the control mechanism and the preservation of their privacy. This mental model decides whether a user trusts or mistrusts a system.

Through active user involvement, our approach is able to identify and quantify problems with respect to the understanding, application and acceptance of privacy measures following the stated requirements. Our method covers a variety of interdependent aspects to be considered and questions to be answered in terms of usable privacy mechanisms. Besides the requirements stated by Fischer-Hübner et al. [16] (representation of legal requirements, transparency, and trust), we primarily consider the user's mental model and the overall effect on the acceptance of the system. Our model is aligned with the User-Centered Design (UCD) guidelines [34] and the Human-Centered Design (HCD) process [28], and it is a key part of an iterative improvement process. This allows for the evaluation and optimization of privacy with respect to usability at development-time and at run-time [15]. The application of our model and method is meant to help security developers to gain a better understanding of the user's objectives and needs with respect to privacy (e.g., security-relevant information about missing encryption [4]). Thereby, developers will be empowered to optimize privacy enhancing technologies in this respect and improve their acceptance.

To motivate our work in more detail and to provide a base line for subsequent discussions, we use an example from the Internet of Things (IoT) domain. However, both the model and the method are not limited to this domain, but can be applied to each system development process that draws particular attention to usable security and privacy.

At the time being, the work presented here is research in progress and lacks a comprehensive evaluation. We will present our evaluation plan as part of our future work.

1.3 Structure

The paper is structured as follows: We continue with an example scenario in Sect. 2. In Sect. 3, we present our model and its integration into UCD and our iterative improvement process. Related work is presented in Sect. 4 and we conclude the paper in Sect. 5.

2 Usable Security and Privacy in the Internet of Things

The Internet of Things (IoT) offers a plethora of possibilities to customers and service providers. The basic idea is that all kinds of things—including physical objects, sensors, vehicles, buildings—are interconnected with each other and to the Internet. By 2020, there will be approx. 28 billion [10] to 50 billion [13] things. Based on the things and on the data collected by them, services can be offered, optimized and tailored to the user. Famous IoT applications are Smart Home devices (e.g., intelligent heating, smart metering, door locks), wearables (e.g., Smart Watch, intelligent clothing), and connected vehicles (e.g., autonomous vehicles). In summary, the IoT can be described as an "inextricable mixture of hardware, software, data and service" [33].

2.1 Privacy in the Internet of Things

Especially the sheer amount of data that is collected by things is a huge burden for users. In Smart Homes, fewer than 10,000 households can generate 150 million discrete data points every day [14]. This amount of data leads to massive privacy concerns. According to [25], 71% of consumers share the fear that their personal information may get stolen and 64% of customers fear that their data may be collected and sold. Besides the amount of data, this fear is also caused by the sensitivity of the data. The combination of data from different sources allows—at least in theory—the creation of a complete profile of the user. The problem is that users do not have, or at least do not feel like they have, control about their data. Privacy statements are hard to read and understand, and control mechanisms are hardly known or understandable. According to [11], only 15% of EU citizens feel that they have complete control over the data they provide online. 31% even feel they have no control at all. However, the perception of privacy highly differs between countries. While Germans are most concerned about lacking control (only 4% think that they have complete control, 45% think that they have no control at all), Greeks are the least concerned (31% think that they have complete control, only 22% think that they have no control at all).

All of this leads to two conclusions: First, existing control mechanisms are perceived as non-sufficient by users. This might be the case because convincing control mechanisms are missing completely, or because existing mechanisms are not known, understood, or trusted by users. Second, the perception of the quality of privacy and control mechanisms highly differs between different users. A one-for-all solution might thus not be possible and mechanisms need to be tailored to different user groups or even individuals to provide a comprehensive and convincing privacy experience. Companies are starting to realize this problem and are looking for solutions to handle

data transparently and legally. This includes processing data only with explicit user consent and only for permitted purposes. However, it is still unclear how processes, technologies, and user interactions must be designed. Relating to our stated conclusions, we believe that the solutions must be approached iteratively and with close contact to the users whose needs have to be in the focus of the development.

2.2 Application Scenario: Privacy in the Smart Home

For further discussions, consider the following scenario: Uma recently bought a new house that is equipped with several smart home services:

- *Locks and shutters* that open and close automatically or remotely using an app.
- A *heating system* that regulates the room temperature according to Uma's needs and helps to save energy costs. For example, if Uma locks her front door, the heating automatically turns off until she approaches her home again.
- *Lights* that can be controlled remotely and that turn on and off automatically when Uma enters or leaves a room.

Additionally, she already owns some smart devices, which can be perfectly integrated:

- Modern e*ntertainment* systems (e.g., Smart TV) that are connected to Internet services and can be controlled via voice commands and modern apps—a welcome and efficient way of interacting with her TV in Uma's point of view.
- A *baby monitor* that Uma can access remotely to check on her child's safety.

All of these functions are of high value to Uma. However, Uma also has a variety of privacy concerns. The baby monitor and the smart TV continuously record audio and/or video data in sensitive areas. While this is good for the dedicated purposes, all private conversations could also be recorded. Uma wonders how she can be sure that vendors do not store these records and how they are used exactly. Additionally, Uma is concerned that data from smart locks, lights and heating are used to create a detailed profile of her movements.

In order to resolve these concerns, she has to understand how her privacy is protected in order to trust the vendor. However, it is in the nature of IoT systems that they being continuously changed (e.g., via updates) and extended (e.g., new remote control app). With every change, privacy would need to be reassessed.

For IoT developers, this is a challenge, as he does not know which information Uma needs in order to trust/accept his service. In turn, if Uma lacks information, there are seldom suitable ways to get it.

3 A Usable Security and Privacy Model

Especially in the IoT, continuous user involvement and system optimization are very important, as systems, users and contexts continuously change. We divided our model into several (intersecting) sub-models and aligned with to user-centered design [34] and

the Human-Centered Design (HCD) process [28]. HCD is an iterative process aimed at making systems usable and increasing their user experience by taking into account users' needs and requirements.

The process we are following consists of four steps (cf. Fig. 1), namely Context of Use, System Awareness, System Design and Design Evaluation. Each of these will be described in the subsequent sections.

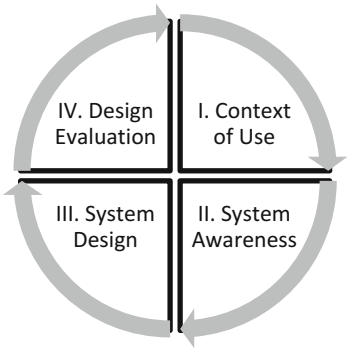

Fig. 1. Design process

3.1 Context of Use

The goal of this step is to understand and to specify the context of use regarding a usable security and privacy system. The context of use is defined by the users and tasks (cf. Fig. 2) and by the environment (cf. Sect. 3.4) [16]. Through the interplay of these aspects, security goals emerge, which can be refined into concrete security requirements. Considering the security requirements in the process of (re-)building a system will contribute to the trustworthiness of the system.

Definition of the System Context. The first step in defining the context of use is to create a description of the information system context. Information systems are defined as the total of all components, interacting to fulfill a certain functionality [32], including applications, services, information technology assets, or other information handling components [29]. The information system has to fulfill privacy goals to protect a user's privacy. Privacy goals can stem from legal regulations or from the user. To comply with legal regulations, system developers have to identify the assets that have to be protected according to legal regulations. Assets are resources that are of real or ideal value for at least one stakeholder [32].

For users, personally identifiable information and their privacy are assets. These assets are exposed to threats—potential causes of an unwanted incident, which may result in harm to a system or organization [29]. With the rising number and increasing severity of threats, the risk for these assets to get harmed increases. To keep the risk low, security mechanisms including privacy-enhancing technology have to be built into the system. These mechanisms fulfills security goals, including the privacy goals. A security goal describes a property of a component or system that has to be fulfilled to protect a

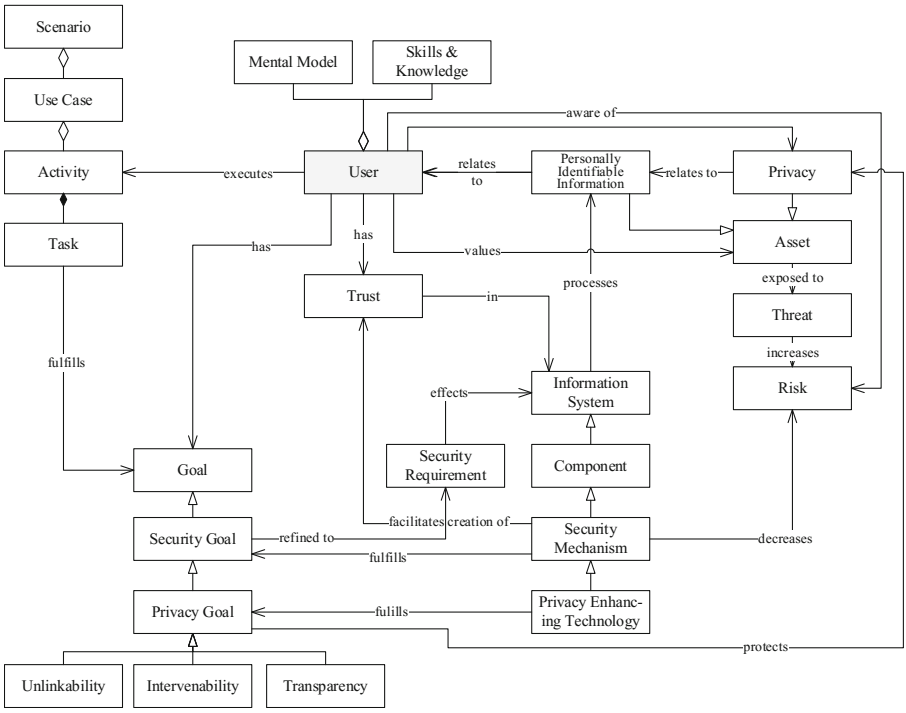

Fig. 2. Model Pt. 1: system context & awareness

user's concrete assets [32] from concrete threats. In the ISO 27000 standard [29] Confidentiality, Integrity, Availability, Authenticity, Non-Repudiation, and Authorization are the main security goals that must be investigated to derive corresponding security requirements. Additionally, the overall system goals are based on the system's security goals in terms of a usable security and privacy system.

Regarding the scenario, Uma is interested in using the information system "Smart Home". Uma has to understand how her privacy is protected. She knows that the information system processes data that concern her privacy, e.g., audio data recorded by the baby monitor. However, she knows that there are legal regulations that force the company to use mechanisms to protect Uma´s privacy. For instance, the company must not save or share recorded data. However, in order to trust the system, Uma needs to know how the system adapts certain security mechanisms. In addition, she must be able to control specific smart products, including their security features, if necessary. For this reason, the system needs to provide appropriate usability, which has to be implemented according to Uma's individual needs, preferences, skills, and knowledge.

Creation of Personas. In the next step, we have to create personas of all user groups in order to better understand the users and their privacy goals. If a system is not designed for and with the users, it will offer a poor user experience due to missing trust in the system and will counteract efficient and effective work. Therefore, the user is an

essential element in our model. The HCD approach defined in ISO 9241-210 [28] provides guidance on how to build a usable system around the user.

First, we need to identify primary and secondary stakeholders. In terms of privacy, we have to consider the users as primary stakeholders. For each stakeholder group, we then identify the relevant characteristics and describe their relationships to the system, their goals and constraints. In our context, it is especially relevant to understand the security and privacy goals of the stakeholders. In particular, the privacy goals [35] have to be considered:

- *Unlinkability* assures that personal data cannot be elicited, processed and used for purposes other than those stated.
- *Intervenability* assures that a system provides means for every affected person to enforce their legal rights.
- *Transparency* assures that information about the processing of personally identifiable information is available, verifiable, and assessable.

As privacy is complex and individual, the users' capabilities and experiences (skills and knowledge) have to be taken into account. It has to be clear what their understanding of privacy is, whether they are aware of risks, and whether they have security requirements. In addition, we have to include user experience aspects by considering the users' attitudes, habits, personalities, strengths, limitations, preferences, and expectations.

In our scenario, stakeholder groups include residents and guests. The residents are the users of the system. Uma is a representative of the group of residents. She likes to live in a house where technology makes life more convenient. She often forgets to turn off the light when she suddenly has to care for her child. Therefore, she expects her house to take care of switching the lights off when she leaves the house. Turning lights on and off could be an indication of being at home. She needs to be sure that nobody with bad intention (e.g. a potential burglar) can access the data. As she knows something about information security, all three privacy goals are highly important to her.

Creation of Use Cases. Once we know the system context and the goals of its users, we can start to define use cases. Use case specifications describe all activities that have to be performed with the help of the system under development. They describe ideal standard procedures embedded into a realistic sequence of interactions from the personas' points of view. Every task in a use case needs to be characterized with respect to its impact on usability, accessibility, as well as security and privacy. Furthermore, it needs to be refined into activities the user needs to execute. Several use cases are integrated into a scenario, which again can be used to identify missing use cases. The results of this step can be recorded in activity descriptions, use case specifications, use case diagrams, and scenario descriptions.

Regarding the scenario, Uma wants to set up a movie mode for her smart home in order to watch movies in a suitable atmosphere. Therefore, she defines a set of system reactions that are executed when she starts a movie. For example, the shutters close, the lights dim and the baby monitor is set on maximum volume. However, Uma likes to keep her choice of movies secret. Therefore, a requirement to the smart TV is that it does not forward the selection of movies to 3rd party vendors (e.g., the vendor of the baby monitor).

3.2 System Awareness

The goal of this step is to create concepts to make the user aware of important things in the system. Especially for the security and privacy, this is an important aspect with respect to transparency and user involvement. Usable security guidelines, like the ones collected by the USecureD project [41], Yee [45] and the usable security principles by Whitten [42], Garfinkel [20], by Furnell [19], and by Herzog and Shahmehri [24] can help to accomplish this step.

Conceptual System Model. The first step is to develop a conceptual model of the system that cap-tures the important parts of the operation of the device and that is appropriate and understandable for the user [16]. This means that the conceptual model of the system has to be mapped to the user's mental model of the system. At this point, it is important to pay particular attention to the security goals that have to be fulfilled by the system and the privacy goals of the user. This step helps to cover the basic security and privacy mechanisms (cf. Fig. 2, and Sect. 1.2, Goal 1).

Regarding the scenario, Uma is concerned that data from smart locks, lights, and heating can be used to create a detailed movement profile of herself. Therefore, the system must ensure that data cannot be used by unauthorized persons in any way. It must provide security mechanisms that prevent unauthorized access while keeping the use of the smart home functionality comfortable at the same time. Additionally, the smart home functionality must be controllable with respect to Uma's skills and knowledge. Since Uma is skillful in using mobile apps on her smartphone, the system should provide a mobile app to control the smart home. Data conveyed from the mobile app to the system must be encrypted to prevent the system from being controlled by unauthorized persons. However, Uma must not be annoyed when using the mobile app by being forced to enter a password whenever she uses the mobile app. In her mental model of the system, the system behaves like another person. Therefore, she wants to talk to her smart home. Thus, the mobile app should be designed in a way that allows for natural interaction. Among other things, this requires a speech recognition component.

Obviously, there are many interdependencies to consider. The user's mental model has to be consistent with the behavior of the system. Thus, every internal and external component of the system has to match to the user's skills and knowledge. This includes all security mechanisms and privacy-enhancing technologies. The user needs to understand how the security mechanisms achieve the security goal(s) and the privacy goal(s).

Continuous Visibility of System States and User Actions. For each dialog step, the system must ensure that the user's currently possible actions, alternative actions, and results of actions are visible [34]. In this step, the focus is particularly on security-relevant information and user actions that mitigate risks in this step. This step contributes to the fulfillment of transparency (cf. Sect. 1.2, Goals 2 & 3). To that end, it has to be analyzed which security-relevant information is important for being conveyed to the user at which time and at which level of detail. However, individual perception and trust in privacy and control mechanisms can highly vary between, but also within

user groups. If security and privacy measures require user interactions, the user needs to be made aware of possible actions and the results of actions.

Regarding the scenario, Uma is informed about every change in the smart home elements. Whenever a light is switched on or off, a heater is adjusted, or a door is opened, closed, locked or unlocked, Uma gets informed both on her smartphone and via an LED and an acoustic signal located directly on the corresponding element. The mobile smart home control app is designed like her apartment. Therefore, Uma has a very good overview of each room and the smart elements in the rooms. The status of each smart element is continuously presented and only functions that make sense can be performed. For example, when a light is switched on, Uma can only switch it off instead of being able to switch it on a second time. The app only allows controlling those smart elements that can be controlled without any security risk. For example, the mobile app allows unlocking the front door only when Uma is located within a radius of 200 m.

Transparency and Guidance. In this step, we have to ensure that the user knows the current state of the system and that the interaction follows natural mappings between intentions and required actions and between actions and resulting effects. Simply speaking, the user shall always know what is currently happening on the system's side. This step contributes to Goals 2 and 3 (cf. Sect. 1.2).

Security-relevant, meaningful information needs to be conveyed in the user's language [16] at an appropriate abstraction level. For each action on security-relevant information, it needs to be decided whether this action should be made transparent for the user. A variety of aspects contribute to this decision. For example, the presented information might differ according to the user group. Some information is not understandable to certain user groups and leads to an opposite effect. In addition, making internal information public might lead to security risks. Finally, we have to decide whether information is presented to the user only upon demand or also actively to make the user aware of certain risks.

In addition to transparency, there needs to be guidance on the mitigation of risks and the use of security mechanisms that require user actions. The user needs to know immediately what to do and not suffer from confusion or information gaps.

Regarding the scenario, Uma is concerned about third parties hacking into her system. Due to the system's transparency concerning the current system state and the implemented security mechanisms, Uma gains trust in the system's security regarding unauthorized access. Whenever the system identifies an unauthorized access, Uma is immediately informed and guided through a security mechanism that asks her to authorize the access and to identify herself as an authorized user.

3.3 System Design

This section corresponds to the step 'Producing design solutions' of the HCD process provided by ISO 9241-210 [28], but we draw particular attention to the security mechanisms of the system under development. This section deals with the identification and implementation of appropriate user interface patterns, the creation of an

appropriate interaction design, and the creation of prototypes (cf. Fig. 3), which are important for evaluating the proper operation of the security mechanisms as well as their usable operability in the next step.

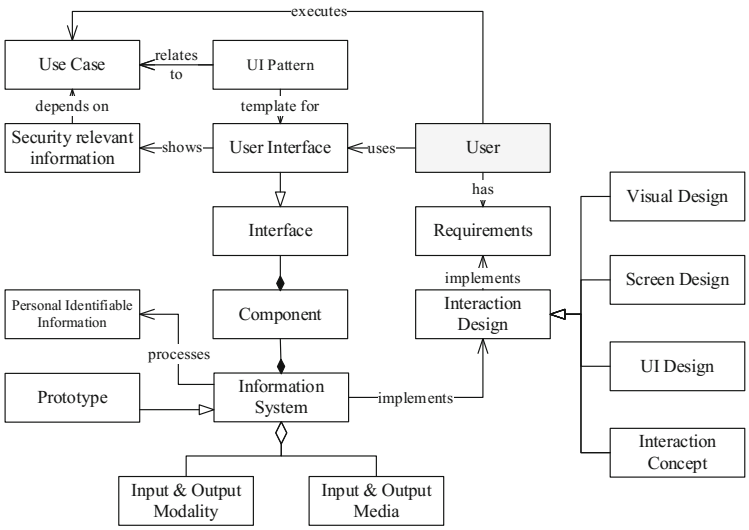

Fig. 3. Model Pt. 2: system design

Selection of User Interface Patterns. To support the performance of tasks, it is useful to draw on fast and proven solutions for particular human-system interactions given in use case specifications. We have to pay particular attention to usable security patterns from pattern libraries (e.g., [41]) to identify fast and proven solutions for particular human-system interactions. This is especially true for the usable security and privacy issues described in the use cases and scenarios created in step 1.

Creation of Interaction Design. Based on the personas, use cases, scenarios, and user interface patterns, we have to illustrate interaction ideas as interaction concepts, user interface design, and screen design. A Usability Walkthrough is an adequate instrument for the early evaluation of the usable security and privacy of the interaction ideas, user interface design, and the screen design. This can be performed before the actual evaluation of the system takes place.

Creation of Prototypes. Finally, we have to create interactive and realistic prototypes of interaction designs to facilitate discussing ideas with stakeholders, especially the end-users of the system. Compliance with conceptual usability criteria can and should be checked at this stage. We have to design user tasks, user-system interactions and the user interface to meet user requirements, especially those user requirements that concern usable security and privacy. We then create the essential design concept and the essential outcomes as well as appropriate input and output modalities and appropriate media for conveying information.

3.4 Design Evaluation

The evaluation of the design corresponds to the HCD phase "Evaluating the design" [28] and closes the iterative cycle of the method for the design of a usable security and privacy system. Through systematic feedback collection and analysis, issues are identified and rated. This information serves as input for improvements in the next iteration of the method.

Collection of Feedback. The main goal of this phase is to collect feedback about issues and uncertainties users face with respect to security or privacy. To put the feedback into context, it is enriched with additional information about the system state and the user's current situation (cf. Fig. 4). Information about the user context and information about the system context must eventually be linked to form a complete picture. To take into account the usability of the security and privacy system, a usability evaluation should be performed. During the usability evaluation, check if usability criteria that are relevant for smooth and engaging use of the system as described in the scenario and use cases are met.

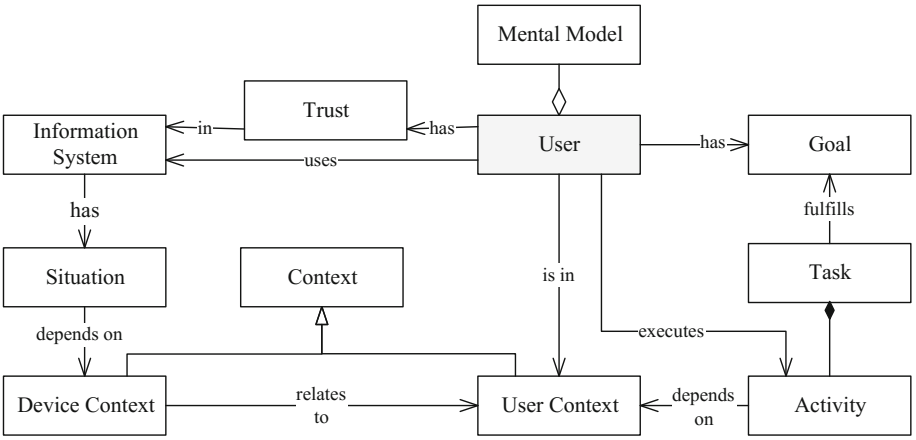

Fig. 4. Model Pt. 3: user context at runtime

For the purpose of a usability evaluation, an evaluation should be performed according to usability heuristics. This evaluation is performed by experts who check if usability criteria are violated. The experts should perform a walkthrough and check the suitability of the design decisions for daily use. Ultimately, the system is evaluated by real end-users. Here, particular hypotheses are proposed. The end-users follow the scenarios created in step 3.1. In laboratory environments, the test can be documented with video and audio records.

In the field, users execute (or want to execute) certain activities to fulfill one or more goals in a certain context. For example, if Uma is at home, she can perform several activities that belong to that context: relaxing, cooking, watching TV, and so on. The status of the devices (i.e., things) she is using includes information about their

internal states and their environment. Similar to the relationship between activity and user context, device context and situation would always match in an ideal world. However, due to technical limitations, several distinct device situations lead to the same device context. Further details about this kind of context modeling and its application can be found in [30]. The main goals is to collect feedback about issues and uncertainties users face with respect to security or privacy. To put the feedback into context, it is enriched with additional information about the system state and the user's current situation. Information about the user context and information about the system context finally have to be linked to form a complete picture.

If usability issues are found, these issues should be prioritized according to their severity, especially regarding on their impact on system usage, security, and privacy. The most severe usability issues should be solved first. Appropriate solutions can be found in the descriptions of the patterns and corresponding design solutions identified and created in the previous steps.

Analysis. At this point, we combine static information from the system design with feedback we collected from users of the system or prototype. As user feedback is typically vague and informal, a *root cause* has to be identified, i.e., we have to map feedback to one or more security or privacy measures. The effect of the issue on the user has to be *rated* in order to assess the severity of the issue and its influence on system acceptance. To that end, we have to combine information about the currently performed activity, the context of use, the user's mental model, and the system state.

The continuous collection and analysis of these mappings allows for iterative improvement and tailoring of the solution. This phase is especially challenging, as usability issues are typically the result of a combination of different aspects. In order to utilize and automate the rating, our model has to be extended by corresponding metrics, which is part of our future work (cf. Sect. 5).

4 Related Work

Since the mid-1990s, huge efforts have been made to develop approaches for aligning usability and security. Unfortunately, the number of security incidents caused by unusable security measures or usable, but insecure systems is still high [18]. In [21] Garfinkel and Lipfort summarize the history and challenges of the "usable security" domain.

Whereas some guidelines and checklists exist for the design and evaluation of a usable security system, only few general requirements on a usable security system can be found in the scientific literature. For the harmonization of security and usability, Fischer-Hübner et al. [16] formulate three major requirements:

- Legal data protection requirements must be represented in a user-friendly manner in order to increase the user's comprehension, consciousness, and controllability.
- *Through a system's transparency, t*he user must understand security and privacy mechanisms and concepts in order to create a mental model that supports him in achieving his goals.

- A user has to be able to create trust in security mechanisms and be aware of the risks that might be caused by missing security mechanisms. The user must be able to perceive these risks. Important criteria are the conveyance and the comprehension of the plausibility of the security mechanisms.

Existing literature on usable security shows that the user is an important and active part of modern security chains. The research field of usable security and privacy has been approached both in a theoretical fashion and in the form of case studies. Famous case studies analyze the usability of email encryption with PGP [42, 44], of file sharing with Kazaa [23], and of authentication mechanisms and password policies [6, 9, 26, 30]. However, case studies are specific to one system, system class, or application domain and can hardly be generalized. On the other hand, theoretical work [1, 7] is typically more abstract and hard to apply in practice.

This gap is closed by design principles for usable, yet secure systems [20, 24, 39, 44, 45]. These principles focus on the development of usable security systems by supporting developers and emphasizing the importance of considering the user. However, they do not adopt the user's viewpoint or active involvement of users in the development process. However, it is crucial to both consideronsidering both the user's viewpoint and to involve users in the development process, as the user is an important, but often weak, link in the usable security HCI chain [3, 5, 37, 44, 46]. We consider design principles to be complementary to our work. By quantifying the effect and acceptance of design principles in different contexts, a knowledge base can be built that supports developers.

Looking specifically at the IoT, a survey on security and privacy issues and corresponding mitigation techniques is provided by Tank et al. [38]. Related work is provided by Ismail et al. [27], who propose a framework for evaluating transparency in cloud applications. This framework is comparable to parts of our model, but not integrated into design and optimization processes.

5 Summary and Conclusion

The preservation of privacy is becoming more and more important. Demands in terms of privacy are coming both from legal regulations and from users themselves. However, the implementation of a secure and privacy-preserving, yet usable system is a challenge for software and service providers. This challenge can be solved only by actively involving the users. Especially in the IoT, where systems are changing frequently, it is important to continue this involvement also at run-time. Unfortunately, corresponding user-centered design approaches do not explicitly include security and privacy. In this paper, we presented a usable security and privacy model and a corresponding method, both of which focus on the user as the central element. Not only does this focus separate our approach from other existing approaches, but we believe that it is also the only way to help elaborate and quantify the users' privacy needs and their perception of privacy- enhancing technologies. Based on the model and the method, developers are supported in optimizing appropriate usable security and privacy mechanisms.

In its current state, the model is quite abstract and cannot be applied directly to full extent. Thus, the next important step is to derive attributes and metrics for each model element. Based on that, measures have to be researched to provide the required data at development time and at run-time. In addition, a technical implementation, for example by using the Eclipse Modeling Framework (EMF), is necessary to support the use of the model. Finally, the evaluation with respect to applicability and generalizability remains to be done. We are planning to evaluate the model´s applicability together with a large German IT company by collecting and analyzing feedback from their users. Additionally, we are planning expert reviews from different domains to generalize our model.

The work presented here is a first step towards the consideration and integration of privacy into UCD and HCD. In the future, this will become a vital aspect, which will not be limited to the IoT. The provision of comprehensive and understandable security and privacy mechanisms will be a major prerequisite to achieving compliance and high user acceptance by enhancing user experience through increased trustworthiness of the system.

Acknowledgements. The research presented in this paper is supported by the German Ministry of Education and Research (BMBF) project Software Campus (grant number 01IS12053). The sole responsibility for the content of this document lies with the authors.

References

1. Adams, A., Sasse, A.: Users are not the enemy. Commun. ACM **42**(12), 40–46 (1999)
2. Al-Saleh, M.: Fine-grained reasoning about the security and usability trade-off in modern security tools. Dissertation, The University of New Mexico (2011)
3. Blythe, J., Koppel, R., Smith, S.W.: Circumvention of security: good users do bad things. IEEE Secur. Priv. **11**(5), 80–83 (2013)
4. Botha, R.A., Furnell, S.M., Clarke, N.L.: From desktop to mobile: examining the security experience. Comput. Secur. **28**, 130–137 (2009)
5. Caputo, D.D., Pfleeger, S.L., Sasse, A., Ammann, P., Offutt, J., Deng, L.: Barriers to usable security? Three organizational case studies. IEEE Secur. Priv. **14**(5), 22–32 (2016)
6. Choong, Y.-Y., Theofanos, M.: What 4,500+ people can tell you – employees' attitudes toward organizational password policy do matter. In: Human Aspects of Information Security, Privacy, and Trust, pp. 299–310 (2015)
7. Cranor, L., Garfinkel, S.: Security and Usability. O'Reilly Media, Inc., Sebastopol (2005)
8. Cranor, L., Garfinkel, S.: Secure or usable? IEEE Secur. Priv. **2**(5), 16–18 (2004)
9. Eljetlawi, A.M., Ithnin, N.: Graphical password: comprehensive study of the usability features of the recognition base graphical password methods. In: Proceedings of the 3rd International Convergence and Hybrid Information Technology ICCIT 2008, vol. 2, pp. 1137–1143 (2008)
10. Ericsson: Ericsson Mobility Report – on the pulse of the networked society (2015)
11. European Commission: Special Eurobarometer 431 - Data Protection (2015)
12. European Union: Regulation (EU) 2016/679 of the European parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016)

13. Evans, D.: The internet of things - how the next evolution of the internet is changing everything (2011)
14. Federal State Commission: IoT Privacy & Security in a Connected World (2015)
15. Feth, D.: User-centric security: optimization of the security-usability trade-off. In: Proceedings of the 2015 10th Joint Meeting on Foundations of Software Engineering - ESEC/FSE 2015, pp. 1034–1037 (2015)
16. Fischer-Hübner, S., Iacono, L., Möller, S.: Usable security und privacy. Datenschutz und Datensicherheit - DuD **34**, 773–782 (2010)
17. Fogg, B.: A behavior model for persuasive design. In: Proceedings of the 4th International Conference on Persuasive Technology 2009, pp. 40:1–40:7 (2009)
18. Furnell, S.: Making security usable: are things improving? Comput. Secur. **26**(6), 434–443 (2007)
19. Furnell, S., Jusoh, A., Katsabas, D.: The challenges of understanding and using security: a survey of end-users. Comput. Secur. **25**(1), 27–35 (2006)
20. Garfinkel, S.: Design principles and patterns for computer systems that are simultaneously secure and usable. Gene **31**, 234–239 (2005)
21. Garfinkel, S., Lipford, H.R.: Usable security: history, themes, and challenges. Synth. Lect. Inf. Secur. Priv. Trust **5**(2), 1–124 (2014)
22. Gartzke, U., Roebel, M.: Balancing privacy and user experience: the challenge of the digital age (2016). http://techonomy.com/2016/01/balancing-privacy-and-user-experience-the-challenge-of-the-digital-age/
23. Good, N., Krekelberg, A.: Usability and privacy: a study of KaZaA P2P file-sharing. In: Proceedings of the Conference on Human Factors in Computing Systems CHI, no. 5, p. 137 (2003)
24. Herzog, A., Shahmehri, N.: Usable set-up of runtime security policies. In: Proceedings of the International Symposium on Human Aspects of Information Security and Assurance (HAISA 2007), Plymouth, UK, 10 July 2007, pp. 99–113 (2007)
25. IControl Networks: 2015 State of the Smart Home Report (2015)
26. Inglesant, P., Sasse, M.A.: The true cost of unusable password policies: password use in the wild, pp. 383–392 (2010)
27. Ismail, U., Islam, S., Ouedraogo, M., Weippl, E.: A framework for security transparency in cloud computing. Futur. Internet **8**(1), 5 (2016)
28. ISO 9241-210: Ergonomics of human-system interaction—Part 210: Human-centred design for interactive systems (2010)
29. ISO 27000 Series: Information security management systems
30. Jermyn, I., Mayer, A., Monrose, F., Reiter, M.K., Rubin, A.D.: The design and analysis of graphical passwords. In: Proceedings of the 8th USENIX Security Symposium, 23–36 August 1999
31. Jung, C., Eitel, A., Feth, D., Rudolph, M.: Dealing with uncertainty in context-aware mobile applications. In: Mobility 2015, p. 9 (2015)
32. Kompetenzzentrum für angewandte Sicherheitstechnologie: "Begriffsdefinitionen in KASTEL". https://www.kastel.kit.edu/651.php
33. Noto, G., Diega, L., Walden, I.: Contracting for the 'Internet of Things': looking into the Nest. Queen Mary School of Law, Legal Studies Research Paper No. 219/2016 (2016)
34. Norman, D.: The design of everyday things. Doubled Currency (1988)
35. Rost, M., Pfitzmann, A.: Datenschutz-Schutzziele – revisited. Datenschutz und Datensicherheit (DuD) **33**(6), 353–358 (2009)
36. Rudolph, M.: User-friendly and tailored policy administration points. In: 1st International Conference on Information Systems Security and Privacy (2015)

37. Sasse, A., Brostoff, S., Weirich, D.: Transforming the 'Weakest Link': a human/computer interaction approach to usable and effective security. BT Technol. J. **19**(3), 122–131 (2001)
38. Tank, B., Upadhyay, H., Patel, H.: A survey on IoT privacy issues and mitigation techniques. In: Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies - ICTCS 2016, pp. 1–4 (2016)
39. Quay-de la Vallee, H., Walsh, J.M., Zimrin, W., Fisler, K., Krishnamurthi, S.: Usable security as a static-analysis problem. In: Proceedings of the 2013 ACM International Symposium on New Ideas, New Paradigms, and Reflections on Programming & Software - Onward! 2013, pp. 1–16 (2013)
40. U.S. Department of Health and Human Services: "Institutional Review Board Guidebook". https://archive.hhs.gov/ohrp/irb/irb_guidebook.htm
41. USecureD Project. https://www.usecured.de
42. Whitten, A.: Making security usable. Comput. Secur. **26**, 434–443 (2004)
43. Whitten, A., Tygar, J.D.: Usability of security: a case study. Comput. Sci. 1–41 (1998)
44. Whitten, A., Tygar, J.: Why Johnny can't encrypt: a usability evaluation of PGP 5.0. In: Proceedings of the 8th Conference on USENIX Security Symposium - Volume 8, p. 14. USENIX Association, August 1999
45. Yee, K.-P.: Aligning security and usability. IEEE Secur. Priv. Mag. **2**(5), 48–55 (2004)
46. Zurko, M.E., Simon, R.T.: User-centered security. In: Proceedings of the 1996 Workshop on New Security Paradigms - NSPW 1996, pp. 27–33 (1996)