Making Devices Trustworthy: Security and Trust Feedback in the Internet of Things

Christina Hochleitner[1], Cornelia Graf[1], Dominik Unger[1], Manfred Tscheligi[1,2]

[1]CURE - Center for Usability Research & Engineering
Businesspark Marximum
Modecenterstraße 17 / Objekt 2
1100 Wien, Austria
+43 1 743 54 51
{lastname}@cure.at

[2]ICT&S Center
University of Salzburg
Sigmund-Haffner Gasse18
5020 Salzburg, Austria
+43 662 8044 4811
manfred.tscheligi@sbg.ac.at

ABSTRACT

Mobile devices form an essential part of the Internet of Things, where mobile and pervasive devices interconnect to form communication and information systems that enable users to interact with intelligent "things" as part of their daily life. With the increasing potential of mobile phones and the further development of pervasive systems, the overview of information and personal data that is sent by connected things will be complicated to keep, or might even get lost. To counteract this tendency, we present an approach to provide users with underlying security information on a mobile system, in order to establish their trust in the Internet of Things.

Categories and Subject Descriptors

Human Factors, Design

General Terms

Design, Human Factors

Keywords

Trust, Security, User Interface Design

1. INTRODUCTION

The Internet of Things (IoT) aims at connecting a large number of communication and information systems. With the further development of pervasive computing, these systems can be integrated into everyday objects, such as household devices, tools or even humans [31] and animals [16]. Within the near future, the use of IoT systems is expected to become common, similar to the use of mobile phones nowadays. When complex and pervasive systems are interconnected, it is complicated to keep track of how secure a system or connection is and to distinguish which devices are connected within the IoT and which devices are not. Therefore it will become increasingly difficult to keep an overview of the (personal) data that is sent by devices.

Additionally, current security information and properties are often difficult to understand [20]. This issue becomes increasingly important in the field of the IoT, where systems can be hidden in pervasive objects and even small interconnected devices, so-called "things", without displays to provide security information. The potential trust a user can invest is closely connected to a system's security information [4]. As part of our research we investigate trust between humans and computing systems (system-trust), which we define as "a confident expectation in the reliability of an entity's behavior accompanied by the acceptance of vulnerability in a potentially risky situation" [11]. While trust is an action on the user's side, the system has to prove trustworthy in order to evoke the user's trust into the system.

Security functions and privacy implications are vast within the IoT, and in order to create a trustworthy system, they must be assessable by users. Therefore it is important to express underlying security properties to users in a comprehensible way, to allow them to make informed decisions on the trustworthiness of a system. In order to do so, we need to draw on current research on system security and trustworthiness visualization to present feedback on the complex security and privacy concepts to enable user trust in the IoT.

Since smartphones are networked and sending and receiving information (e.g. over the internet and mobile networks), they can already be considered to be part of the IoT. Contrary to networked everyday objects, like smart household appliances, smartphones dispose of advanced feedback methods such as displays, as well as acoustic and haptic feedback possibilities. Therefore we take smartphones as a point of entry in our research on security and trustworthiness feedback in the IoT. Our main goal is to create usable and understandable interfaces within the IoT that inform the user about the underlying security processes and relate to their mental models. To achieve our goal, we base our work on six requirements elicited from literature research. We use these requirements in order to develop secure and trustworthy interaction prototypes for three chosen IoT scenarios: smart home (e.g. re-ordering of prescription medicine), smart office (e.g. connecting to networks) and e-voting (e.g. voting on renovations). We deem these application contexts to be interesting areas where IoT devices are expected to be used in the future.

Within the following sections of this paper, we provide an overview of the current state of the art in trust research in the field of IoT and we present design guidelines for trustworthiness and security. Based on our research, we then highlight important requirements to be addressed when designing trustworthy interaction concepts in an IoT environment. These requirements were the foundation of our approach on providing security and trustworthiness feedback. We explain our approach by demonstrating two prototypical interfaces and describing how the used requirements are addressed by our design. Afterwards we will discuss our future work, which includes the transfer of our currently mobile-phone based concepts to more advanced IoT objects.

Fourth International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use (IWSSI/SPMU)
June 18, 2012, Newcastle, UK

2. RELATED WORK

Trust is the chicken soup of social life. It brings us all sorts of good things from a willingness to get involved in our communities to higher rates of economic growth, to making daily life more pleasant. Yet, like chicken soup, it appears to work somewhat mysteriously [25].

In the following sections we will provide an overview of current research and related work in the field of trust, security and IoT. We will also highlight important requirements within the presented research.

2.1. Trust in the Internet of Things

As part of our research within the uTRUSTit project [26] we are facing two challenges: trust and IoT, both relatively unknown concepts to most users.

Everyone knows what trust is, but no one really knows how to define it to everyone's satisfaction [19]. While this statement is true, it also applies to increasing the users' trust in the IoT.

2.1.1 Technology intent

In the current research landscape different approaches and results to increase the users' trust are available. For example, Køien investigated human-to-machine trust issues for the IoT [15]. Within his paper, trust is highlighted from different perspectives (software, hardware, devices, and services) and an overview of trust aspects from a human point of view is provided. Based on this research it can be concluded that the IoT components are currently not fully trustworthy, because humans currently do not have the possibility to check the true intent of the device.

2.1.2 Legal frameworks and user control

Hert et al. investigated threats and vulnerabilities affecting privacy and data protection in Ambient Intelligence [9]. Their results show that current legal frameworks are inadequate and new approaches for privacy and data protection are needed. Especially in the IoT, where devices are interoperable, trustworthy data protection mechanisms need to be established for protecting the users' private data. In general, informed consent and control are important from a legal perspective. Nevertheless, easy and safe user control within the IoT is also an important design aspect [3].

In the following section we will present an overview of the current state of the art for creating trustworthiness through design and design approaches for security applications.

2.2. Designing for trustworthiness

In the field of human-computer interaction (HCI) much research deals with trustworthiness of design and how to increase and maintain the user's trust in a system or software. Nielsen describes trust as a long-term proposition, which is very hard to get from users, but very easy to lose [18].

2.2.1 Creation of trust

Based on findings of several studies, Nielsen presents four ways to communicate trustworthiness to the user in a web-environment: quality of the design, up-front disclosure, comprehensible and correct presentation of content and connecting websites through links [18]. Flechais et al. identify several factors, which are affecting the users' aptitude to behave in a trustworthy manner [5]. Based on the identified trust factors design principles, namely simplifying security, promoting a security culture, participative security, group membership/identity and educating employees about security, were presented.

2.2.2 User focus

Wang and Emurian present implications and hints for how to establish online trust through web interface design [27]. Their implications are summarized in a framework with four dimensions (graphic design, structure design, content design, and social-cue design) and are focusing on the user itself for increasing the perceived trustworthiness. As mentioned above, several factors influence the trustworthiness of systems and many of them can be summarized as usable and understandable design. *A usable system will minimize unintentional errors, while a secure system will aim at ensuring that undesirable actions in a system are prevented or mitigated [13]*. Therefore an in-depth knowledge about security design is important for establishing trustworthy technology.

2.3. Designing for security

The research field of HCI security addresses the topic of designing for security.

2.3.1 Understanding the user

The need for "psychological acceptability" in security feedback mechanisms was first described by Saltzer & Schoeder [23]. From their point of view, the user interface has to be usable and match the user's mental model of the security mechanisms. Only then the user will be able to use the mechanisms correctly with a minimal chance of making mistakes. This is a very important statement, because even if a system is absolutely secure from a technical point of view, it is the end-user who operates the system. The importance of including the users' mental model was also outlined by Kelley et al. [14]. Design work that also takes the users' mental model into account is available e.g., for web browser security [8], security feedback dialogs [1] or firewalls [22].

Another important aspect for understanding the user is the establishment of a good communication structure between system and user. Yee introduced design guidelines dealing with the design of software behavior for authorization and communication [29]. According to Yee, good communication could be achieved through an indication of possible consequences.

2.3.2 Usable design

In 2002, Yee presented a set of ten key design principles for making security systems more usable [30]. The bottom line of his principles is that the natural way of interaction should be the secure way. Therefore, users should be able to interact with systems without the need to think about detailed security processes. This approach also answers to the so-called "secondary task" problem [13], [33]. The combination of known wizard-like interfaces and security mechanisms is recommended by Herzog et al. [10]. Similar to Herzog et al. Kelley et al. suggest using familiar approaches for displaying privacy information [14]. Their approach adopts nutrition labels from groceries for presenting privacy and security information to end-users.

2.4. Design requirements

We have used current literature as described above to elicit important guidelines when creating trustworthy interfaces for an IoT environment. The following list summarizes these requirements and states the literature that has influenced its creation:

1. Communicate technology intent [15]: Users need to know the technology's intentions, in order to make the right decisions for protecting their data. According to [15] the awareness of the technology's intent is a precondition for the development of trust towards the system.

2. Create adequate legal frameworks [9]: In an IoT environment legal data protection mechanisms need to be established. Currently available legal measures are insufficient and have to be adapted to the new requirements, such as those originating from an IoT environment.

3. Create trust [18]: Design should be used to create trustworthy interfaces and communicate real trustworthiness to the user. Since trust is a long-term proposition [18] trustworthiness communicated through design-approaches as introduced in [5] will establish trust over time.

4. Focus on the user and create intuitive design [13], [27]: Security, design and technology needs to be built around the user and his needs. The technology should make the life of the user easier, e.g., through more efficient behavior.

5. Use interaction concepts to address the users' mental models [1], [8], [10], [14], [22], [23], [30]: The interface should be created to support the users' mental models and the interaction needs to be intuitive and natural. Thus, the interfaces and interaction concepts should fit the users' thought processes and known interaction paradigms should be employed.

6. Communicate consequences [29]: The communication of consequences helps the user to understand potential risks. This will enable users to make informed decisions.

Based on the described requirements we developed a first approach of mobile interaction prototypes that foster the user's trust in the IoT. The novelty of this approach is the combination of literature-based requirements of the topics trust, security and IoT to create usable, secure and intuitive interfaces that allow for a user's informed consent.

3. TRUSTWORTHINESS FEEDBACK IN THE IOT

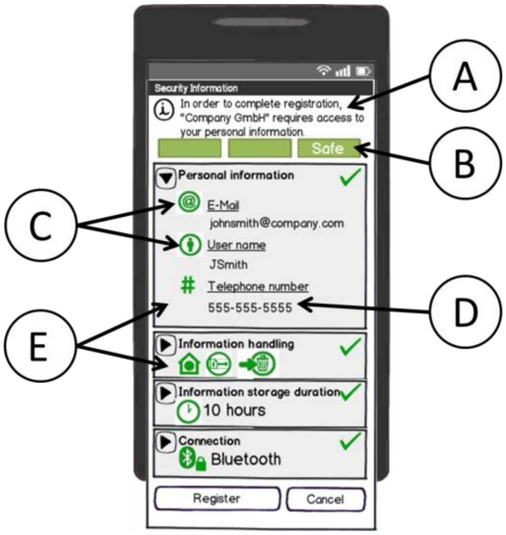
Within our research we aim at providing users with understandable security and trustworthiness feedback. In order to do so, we follow up on the research and requirements in the previous section. We have developed two prototypes visualizing security information. Our overall goal, in accordance with de Saint-Exupery [3] is to provide the users with a possibility to control their personal information. As a starting point for our research in the field of the IoT, we have chosen to investigate feedback possibilities on mobile devices (especially on smartphones and tablets) in a first iteration and then apply them to more advanced pervasive systems, such as networked washing machines, lamps or other household appliances. In the following sections we will present the developed interaction prototypes and how we addressed the requirements during the interface development for smart phones and tablets.

3.1. The Trust Feedback Toolkit

As part of the uTRUSTit project [26], the so-called trust feedback toolkit (TFT) is being developed. This generic toolkit is designed to be embedded in smartphone and IoT applications and has a similar functionality to the privacy manager in Zhou et al. [32]. Other than the privacy manager, the TFT does not only provide privacy settings for each application, it also provides feedback on incoming and outgoing connections. The TFT will be able to interface with common software applications and provide information about the system's security and trustworthiness status to the users. Summarizing the TFT is the technical basis that processes security and application input in order to create interaction workflows that answer to the requirements as presented in Section 2.

The following two exemplary application scenarios from a smart home environment demonstrate the functionality of the TFT. Amongst other, these scenarios have been implemented and are currently subject to user evaluations. The two main actors within the scenarios, Sara and Paul, are part of the uTRUSTit personas [24], archetypical users, representing our target group [2].

Example 1: Sara, a business woman in her thirties connects her mobile device to an office infrastructure, she hasn't connected to before. Before connecting, Sara wants to be informed about the security of the network (e.g. WiFi) and the information being sent from her mobile. Therefore the mobile application shows the available connections. The TFT augments this information by indicating the security state of each available connection and the recommended connection. Upon choosing one connection, the mobile application forwards this process to the TFT that, as a consequence, displays information about the system's security state, as well as information being transmitted and how this information will be handled and used by the receiver (Figure 1). Hence, Sara is given information in order to make an informed decision about her personal data. This decision is then forwarded to the application by the TFT and the process continues accordingly.



Security Information

In order to complete registration, "Company GmbH" requires access to your personal information.

Personal information ✓

E-Mail
johnsmith@company.com

User name
JSmith

Telephone number
555-555-5555

Information handling ✓

Information storage duration ✓
10 hours

Connection ✓
Bluetooth

Figure 1. Security information about the connection and the information to be transmitted displayed by the TFT. A) The top area providing a security summary and instructions. B) The security bar. C) Privacy icons indicating the type of information disclosed. D) The information being transmitted. E) The accordion menu in expanded (above) and collapsed state (below).

Example 2: With the increasing number of pervasive devices connected to the IoT, it is increasingly difficult for Paul, an elderly man who is living alone, to keep an overview of what devices are connected and transmitting information. To obtain this information Paul launches the IoT overview application either on his smartphone or on his tablet. This application interfaces with provide an overview of all "things" connected to the IoT within

Paul's environment (e.g. his home) and transmitting information (Figure 2). The application indicates per connected "thing" what information is transmitted. In case of a smartphone all applications that are currently transmitting information are listed with their according security status. Additionally, Paul has the possibility to control the information being sent and the transmission channels being used. Hence, Paul is not only able to get an overview of the activities of the things in his environment that are connected to the IoT, but also to exercise control over information transmitted and devices connected.

3.2. Designing for trust

As mentioned before, we have based the created interfaces on requirements elicited from research, as well as on our own experience in designing trustworthy and privacy-enhancing systems as part of projects like PrimeLife [6], [7]. To achieve our objective of creating trustworthy and secure user interfaces, we have addressed the requirements, as introduced in Section 2, during our interface design process. The following paragraphs provide examples, based on the two screens presented in Figure 1 and 2, on how we addressed the requirements.

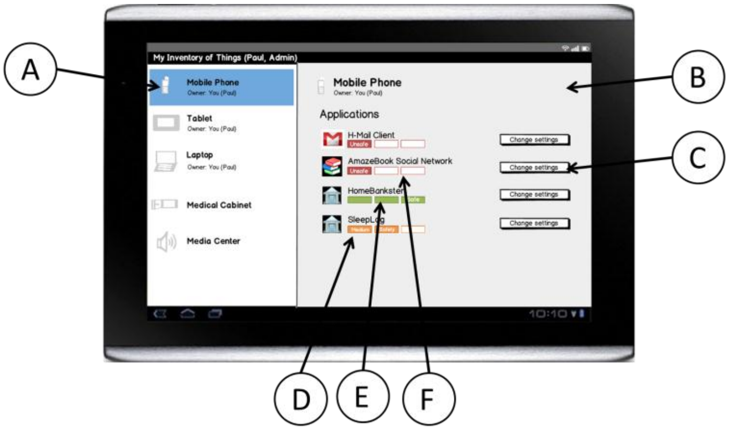


Figure 2. Overview of the devices connected to the IoT and according security information. A) Overview of devices connected to the IoT. B) The detailed information per device. C) The possibility to change settings. The security bar indicating D) medium, E) good and F) poor security.

1. Communicate technology intent. It is our goal to enable the user to grasp the situation and main context of each transaction within a glance. Therefore we provide a summary and instructions on the top part of the mobile phone application (Figure 1, part A). This area immediately provides users with a context in the form of a small info icon and a short text that informs them about the process at hand (Figure 1, parts A and B). Thus, the user is able get an overview of the security state of the transaction or the applications running on the tablet (Figure 1 and 2). The displayed information is structured according to the concept of progressive disclosure, an interaction design technique that aims to reduce clutter, confusion and cognitive workload for the users [17].

2. Create adequate legal frameworks. Hert et al. have voiced the need for new legal frameworks to answer the users' complex privacy and data protection needs [9]. This certainly applies to the field of the IoT, where even more aspects have to be taken into consideration. As part of the uTRUSTit project, we aspire to analyze the current legal landscape and provide input on shortcomings and potentials for improvements. During the development of interaction prototypes we consult with our legal partners in order to create legally compliant interfaces. Additionally, the developed interaction prototypes are evaluated from a legal perspective.

3. Create trust. In order to evoke trust in the user, we communicate trustworthiness by providing well-structured and concise information. The developed interfaces are informing the users about security and privacy issues, such as unsecure connections. The reliable presentation and an up-front disclosure of security information will increase the users' trust in the system. An example of up-front disclosure can be seen in Figure 2. On the left hand side the users see a list of devices that are connected (Figure 2, part A) including additional ownership information (if this applies to the specific element). Detailed information about the individual devices can be easily obtained by just tapping on the item on the list, which will open a detailed view in the right panel (Figure 2, part B). This detailed view will vary according to the selected device. In accordance with Exupery et al. [3], the users can exercise control over the transmitted information of all devices by selecting "change settings" (Figure 2, part C).

Another approach to create trust is the development of a well-formed information system, for example by simplifying security. We have addressed this requirement by using privacy icons (Figure 1, part C) and by providing comprehensible representations of the system's security status, such as the security bar (Figure 1, part B and 2, parts D-F). The security bar is a visual summary of all security information combined. The idea is to provide the users with a learnable traffic light system that can be quickly processed and understood. The bar has three distinguishable states: safe (green, Figure 2, part E), medium (orange, Figure 2, part D) or unsafe (red, Figure 2, part F). This gives the user a visual clue that makes it possible to quickly assess the situation.

The design intention of the privacy icons (Figure 1, part C) is for the users to progressively discover the information they seek through the icons. Most of the icons used were selected according to previous tests conducted for the PrimeLife project [12]. While even well designed icons might not be fully self-explanatory, they can still be learned through usage and can improve the speed of comprehension while increasing information density. This is essential on mobile devices with little screen estate.

4. Focus on the user and create intuitive design. As part of our chosen user-centered design process we have developed representative archetypical users, called "personas" [2]. Through the use of personas we are able to align all interaction prototypes to the requirements of the target group users. This alignment includes the graphic design, the content of the interfaces, the structure and presentation of the information and the social-clue design. As described in the scenarios above, the screen in Figure 1 is rather targeted at younger persons that are used to interacting with complex technologies. Figure 2, on the other hand addresses potential issues of elderly users (in this case, Paul). This can be seen in the larger font types, the more visual appearance of the interface and the different wording. Additionally, the screen layout for the uTRUSTit IoT overview application (Figure 2) is more loosened up, due to the larger screen estate (on a tablet) but follows the same basic ideas and principles.

Our focus on the users' needs and requirements is, for example, displayed in the concept of progressive disclosure [17], which is adapted to the targeted user groups. Furthermore, all actions that a user can undertake within these interfaces are easily revocable and the users are warned in case their decisions might be harmful to their privacy and security. To ease understanding and to alert the user about potentially risky situations, the visual cues are supported by multi-modal (acoustic and haptic) feedback.

5. Use interaction concepts to address the users' mental models. Kelley et al. [14] and Saltzer and Schroeder [23] stress the importance of fitting interfaces to the users' understanding and thought processes. For the here presented interfaces we have conducted several steps of research to understand the end-users' mental models. First of all, we have created the personas, based on user research on trust in the IoT. Additionally, we have researched existing literature and conducted focus groups with users of the respective target groups. The results of our user research have influenced design decisions, such as the security bar (Figure 1, part B and 2, part D to F).

Further possibilities to address the users' mental models through design are natural means of interaction. According to the principles of Yee [30] we use the most secure approaches as default values. In case the user decides to use e.g. unsecure channels for connection, he will be warned about potential risks of this decision. The users explicitly have to confirm that they want to make themselves vulnerable to attacks.

Familiar interaction approaches are recommended by Herzog et al. [10] and Kelley et al. [14]. In order to use known interaction paradigms, we have made use of design patterns as presented in [28]. An example of such a design pattern is the accordion control element that can be expanded and collapsed by tapping one of the logical sections: personal information, information handling, information storage and connection (Figure 1, part E). Another familiar interaction approach used within the here presented interfaces is the traffic light approach of the security bar and the employed icons, c.f., Privacy Bird [20]. For the security states "medium" and "unsafe" (Figure 2, parts E and F) there will be a strong color coded connection between the bar and specific security icons that cause the lower rating. After opening a section (Figure 1, part E) users are presented with detailed security information and icon labels. Warning icons replace the check icons of the section that does not have the security state "safe".

6. Communicate consequences. To establish a good communication between the user and the system, as recommended by Yee [29], we provide a detailed overview of what information is sent (Figure 1, part D). Additionally we provide the users with information about consequences of e.g. connecting to unsecure networks.

4. DISCUSSION

The interaction prototypes described in this paper have been implemented for usage on a smart phone and a tablet. The resulting prototypes are currently subject to end-user evaluations. Through the evaluations we expect to obtain feedback on the quality of the implemented interfaces and the extent the requirements have been satisfied. As mentioned in the requirements targeting legal frameworks, we are also conducting evaluations from a legal perspective. Since the legal landscape concerning IoT and security is still in development, we anticipate further research to be required and improvements to be made.

For the interfaces presented here we have sought a trade-off between providing too much information to the user (i.e. overwhelming the user) and providing too little information (i.e. taking control from the user). When there is too much information present, the interfaces get cluttered and the user loses the overview of the important security information. This is expected to cause disinterest in the user and feeds into the "secondary task" problem as described in [13], [33]. Too little information might cause the user to feel patronized by the system and again causes reluctance in using such applications. These issues also apply to multi-modal information. To foster the different display-based needs of users that also depend on their personal backgrounds, attitudes and intentions, we use the personas approach. As demonstrated in the scenarios including Sara and Paul, both have different requirements concerning the displayed information, as well as the employed wording.

Nevertheless, the information displayed does not only depend on the recipient, but also on the device, it is displayed on. No matter where the information is displayed (in this case smartphone and tablet), its content has to be equal on all devices. This requires very generic interfaces that work in different contexts and with different types of devices.

Another research question we have encountered during the development of the interaction prototypes was connected to single display elements and multi-modal feedback mechanisms. Especially the used traffic light system (Figure 1 and 2) has provoked mixed reviews in early feedback sessions. Several iterations of the security bar have been developed and feedback indicates that the presentation should put more emphasis on the unsafe state, without disregarding potential accessibility problems.

5. CONCLUSION AND FUTURE WORK

5.1. Conclusion

In this work we have presented and addressed requirements on trustworthy and secure IoT design and developed a first set of interaction prototypes for providing trust feedback information (trustworthiness of a connection, overview of connected devices) to end-users. The goal of our approach is to present trustworthiness issues in an understandable way to end-users to increase their security and protect their data in the interconnectedness of the IoT. Through this interconnectedness the exchange of private data between things will increase in the future and therefore protection mechanisms need to become more usable and understandable for end-users. The provided security and trustworthiness information will support users in their decision whether or not to share their private data.

5.2. Future work

As previously mentioned the developed prototypes are currently being evaluated by end-users. To be able to simulate the functionality of the TFT and its interaction with devices within an advanced IoT environment at an early stage of the project, an immersive three-dimensional virtual environment was created. For the simulation of the system's functionality, two scenarios (a smart home and a smart office environment) were developed. Within both scenarios, users interact with virtual objects (things in the IoT) through a touch-enabled smartphone or a tablet computer. These devices allow the users to interact with their environment and experience the TFT in a realistic surrounding.

The results of the evaluation using the immersive virtual environment will provide feedback on the usability, user experience and efficiency of the developed trust and security interaction prototypes. The gathered knowledge will be used to further refine the mobile-based interfaces and implement feedback mechanisms for pervasive systems that do not dispose of a display. For the latter, the feedback needs to be provided using either limited visual cues or haptic and acoustic channels.

Additionally we want to gather further insights into the users' mental models of trust in the IoT and conduct research in this area, as suggested by Saltzer & Schoeder [23].

6. ACKNOWLEDGMENTS

This work was partially funded by the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement number 258360 (uTRUSTit; see http://www.utrustit.eu/).

7. REFERENCES

[1] Bravo-Lillo, C., Cranor, L.F., Downs, J.S., Komanduri,S., Sleeper, M.: Improving Computer Security Dialogs (2011). In: Interact 2011 pp. 18-35

[2] Cooper, A. The Inmates Are Running the Asylum. Indianapolis. (1999). In, USA: Macmillan Publishing Co., Inc.

[3] de Saint-Exupery, A.: Internet of Things Strategic Research Roadmap (2009). Strategic Research Agenda [SRA]. Available at: http://ec.europa.eu/information_society/policy/rfid/documents/in_cerp.pdf

[4] Dourish, P. and Mazmanian, M. Media as Material: Information Representations as Material Foundations for Organizational Practice. Working Paper for the *Third International Symposium on Process Organization Studies,* Corfu, Greece (June 2011).

[5] Flechais, I., Riegelsberger, J., Sasse, M.A.: Divide and conquer: the role of trust and assurance in the design of secure socio-technical systems (2005). In: NSPW '05. ACM, pp 33-41.

[6] Graf, C., Wolkerstorfer, P., Geven, A., Tscheligi, M.: A Pattern Collection for Privacy Enhancing Technology v (2010). In: Patterns '10.

[7] Graf, C., Wolkerstorfer, P., Hochleitner, C., Wästlund, E., Tscheligi, M.: HCI for PrimeLife Prototypes (2011). In: Privacy and Identity Management for Life. Springer. Pp221-232.

[8] Hawkey, K., Inkpen, K.M.: PrivateBits: managing visual privacy in web browsers (2007). In: GI '07. ACM, pp. 215-223.

[9] Hert, P., Gutwirth, S., Moscibroda, A., Wright, D., Fuster, G.G.: Legal safeguards for privacy and data protection in ambient intelligence (2009). In: Personal Ubiquitous Comput. 13, 435-444.

[10] Herzog, A., Shahmehri, N.: User help techniques for usable security (2007). In: CHIMIT '07. Article 11.

[11] Hochleitner, C., Döbelt, S., Busch, M. and Tscheligi, M.: The Materiality of Trust – Materializing Trust in the Physical World (2012). In: Material to Materiality, Workshop at CHI 2012 (to be published).

[12] Holtz, L., Nocun, K., Hansen, M..: Towards Displaying Privacy Information with Icons (2011). In: Privacy and Identity Management for Life, pp. 338-348.

[13] Kainda, R., Flechais, I., Roscoe, A.W.: Security and Usability: Analysis and Evaluation (2010). In: ARES '10. IEEE, pp 275 - 282.

[14] Kelley, P.G., Bresee, J., Cranor, L.F., Reeder, R.W.: A "nutrition label" for privacy (2009). In: SOUPS '09. Art. 4.

[15] Køien, G.M. Reflections on Trust in Devices: An Informal Survey of Human Trust in an Internet-of-Things Context (2011). In: Wirel. Pers. Commun. 61, 3 (December 2011), 495-510.

[16] Lee, P., Cheok, D., James, S., Debra, L, Jie, W., Chuang, W., and Farbiz, F. A mobile pet wearable computer and mixed reality system for human-poultry interaction through the internet (2006). In: *Personal Ubiquitous Comput.* 10, 5. 2006), pp. 301-317.

[17] Marx, A. Using metaphor effectively in user interface design. (1994). In: CHI '94, Catherine Plaisant (Ed.). ACM, New York, NY, USA, 379-380.

[18] Nielsen, J.: Trust or Bust: Communicating Trustworthiness in Web Design (1999). Available at: http://www.useit.com/alertbox/990307.html

[19] Patrick, A.S., Briggs, P., Marsh, S.: Designing Systems that People Will Trust (2005). In: Cranor, L.F., Garfinkel S.: Security and usability: designing secure systems that people can use. O'Reilly Media.

[20] Privacy Bird: http://www.privacybird.org/

[21] Raja, F., Hawkey, K., Jaferian, P., Beznosov, K., Booth, K. S.: It's Too Complicated, So I Turned It Off! Expectations, Perceptions, and Misconceptions of Personal Firewalls (2010). In: SafeConfig '10.

[22] Raja, F., Hawkey, K., Hsu, S., Wang, K.-L. C., Beznosov, K.: A brick wall, a locked door, and a bandit: a physical security metaphor for firewall warnings (2011). In: SOUPS '11. ACM, pp 1-20.

[23] Saltzer, J.H., Schroeder, M.D.: The Protection of Information in Computer Systems (1975). In: Proceedings of the IEEE, vol. 63, no. 9. pp. 1278-1308.

[24] Schulz, T, Graf, C., Hochleitner, C. and Fuglerud, K. S. D2.1 Personas, uTRUSTit deliverable, March 2011

[25] Uslaner, E.M.: The Moral Foundations of Trust (2002). Cambridge University Press, Cambridge.

[26] uTRUSTit Website 2010 - 2013: www.utrustit.eu

[27] Wang, Y.D., Emurian, H.H.: An overview of online trust: Concepts, elements, and implications (2005). In: Computers in Human Behavior . pp105-125

[28] Welie, M.v.: Pattern Library - Accordion (2008) – available at: http://www.welie.com/patterns/

[29] Yee, K.-P.: Guidelines and Strategies for Secure Interaction Design (2005). In: Cranor, L.F. and Garfinkle, S. eds. Security and Usability: Designing Secure Systems That People Can Use, O'Reilly 2005, pp. 247-274.

[30] Yee, K.-P.: User Interaction Design for Secure Systems (2002). http://zesty.ca/sid/uidss-may-28.pdf

[31] Zhong, Y., and Liu, L. Remote Neonatal Pain Assessment System Based on Internet of Things. In: ITHINGSCPSCOM '11. IEEE Computer Society, pp. 629-633.

[32] Zhou, Y., Zhang, X., Jiang, X. and Freeh, V.W. Taming information-stealing smartphone applications (on Android) (2011). In: TRUST'11, pp. 93-10.

[33] Zurko, M.E.: User-Centered Security: Stepping Up to the Grand Challenge (2005). In: ACSAC '05. IEEE, pp. 187-202.