Challenges in Security and Privacy for Mobile Users in Intelligent Environments

Bachelorarbeit

zur Erlangung des akademischen Grades „Bachelor of Science (B. Sc.)“ im Studiengang Wirtschaftswissenschaft der Wirtschaftswissenschaftlichen Fakultät der Leibniz Universität Hannover

vorgelegt von

Name: Oehmigen Vorname: Elisa

[redacted] [redacted] [redacted]

Prüfer: Prof. Dr. M. H. Breitner

Hannover, den 09.08.2017

Table of Contents

Table of Contents .... **I**

List of Figures .... **II**

List of Tables .... **III**

List of Abbreviations .... **IV**

1 Introduction **1**

2 Literature Review **2**

3 Theoretical Foundation **5**

3.1 User Mobility 5

3.2 Intelligent Environments 12

3.2.1 Conceptual Delimitation and Definition 12

3.2.2 Elements and Organisation 14

3.2.3 Areas of Application 16

3.3 Ethical, Legal and Social Issues 18

3.3.1 Information and Mobile Security 18

3.3.2 Individual Information Privacy 20

3.3.3 Challenges and Threats 23

4 Research Method – Expert Interviews **27**

4.1 Operationalization 27

4.2 Execution of explorative Expert Interviews 30

4.3 Evaluation 30

5 Results and Discussion **33**

6 Conclusions **35**

7 Limitations and Further Research **37**

References ....

Appendices **39**

1 Introduction

Information and communication technologies have become an indispensable part of today since we benefit from several technological innovations and a variety of everyday devices in different kinds of situations (see Augusto et al., 2013, p. 1; Gebauer, 2008, p. 1; Kollmann, 2016, p. 1). In particular, the Internet has penetrated both our daily and professional life radically and created a global knowledge society (see Donath & Jüptner, 2009, p. 6). A further significant technological development in recent years is the move towards a more mobile society (see Becher et al., 2011, p. 96; Bergman et al., 2013, p. 3). By using mobile systems people are nowadays able to access data and information at any time and anywhere they want to, as a result of which the offline and online worlds have merged (see Kollmann, 2016, p. 44).

Despite these technological advances during recent years, developments may go one step further in the near future. By introducing the term “Ubiquitous Computing” 25 years ago, Mark Weiser (1991) already had the vision of intelligent environments in the form of invisible computers which would lead to a new era and quality of life through increases in efficiency. This phenomenon is very complex, on account of which it demands that researchers have knowledge in a variety of fields: perceive and mobile computing, sensor networks, artificial intelligence, robotics, multimedia computing, middle ware and agent based software (see Cook & Das, 2007, p. 53; Donath & Jüptner, 2009, p. 12 f.). Due to cheaper and faster communication and computer capabilities more and more objects and structures will be embedded in our physical surroundings soon and a new human-machine relationship will be created (see Kang et al., 2016, p. 1). This growing networking may ease our daily and work life in many ways, but also implicates several social challenges for the future in terms of security, privacy and trust.

Information that was once private and secure is now shared, for example via applications and Geo-tracking Systems. For this reason, huge amounts of intimate data involving our interests, traits and beliefs are saved on various devices in this digital age (see Acquisti et al., 2015, p. 509; Gubbi et al., 2013, p. 1). This implies that the monitoring of sensitive information is ubiquitous. Even if the convenience, functionality and immediacy of access to data, communication, applications and web services may sound completely positive at first, it also implies a lack of defence against criminal attacks and other threats (see Ciaramitaro, 2012, p. 10).

Increased networking does not stop short of any area of our life, as a result of which concerns about information privacy and security have been raised (see Bélanger & Crossler, 2011, p. 1017). On account of these concerns this research paper aims to analyse and illustrate challenges to security and the privacy of mobile users in intelligent environments through a critical analysis of information systems (IS) literature as well as by methods of interviews with experts. As a direct result, some advances in security and privacy in intelligent environments will be presented in addition to recommendations for future actions. Consequently, in this research paper the following research question arises:

Do mobile users have to worry a lot about data security and privacy in intelligent environments?

First of all, with regard to structure and filter relevant articles as a basis for this research paper, a systematic literature review according to Webster and Watson (2002) is conducted in chapter 2. Because of the wide variety of the main terms of the title, “security and privacy”, “mobile users”, and “intelligent environments” in Chapter 3, these theoretical foundations will be defined, analysed and described in detail. Afterwards, in Chapter 4, interviews with experts are conducted to gain additional insight into the topic and uncover research gaps by means of specialised knowledge and also to establish practical relevance and experiences. Finally, results are presented and discussed before conclusions are drawn. Last but not least, this research paper involves some essential limitations that have to be taken into account and made clear in addition to further research recommendations.

2 Literature Review

First of all, a systematic literature review is conducted in order to filter out the most important and relevant articles as well as to present an overview of the sate of research into security and privacy for mobile users in intelligent environments. To ensure a well-structured procedure, the concept-centric approach according to Webster and Watson (2002, pp. xiii-xiv) is used.

Through their article “Analyzing the Past to Prepare for the Future: Writing a Literature Review“, Webster and Watson (2002, pp. xiii-xiv) provide a guideline on how to write and structure a literature review clearly in academic projects. In this connection, they highlight the importance of such an approach by stating that a review “creates a firm foundation for advancing knowledge” (see Webster & Watson, 2002, p. xiii). In the course of identifying esvices he/she wants to use or not. Most apps today ask the user to approve whether it is allowed to use the camera, microphone etc. In Particular, the Telekom Smart Home, an intelligent environment, adapts its functions to the individual needs. Users are, for example, able to decide whether the alarm system should contact the house owner via SMS in the case of a burglary or if it should inform someone in a different way. Everything could by regulated by smartphones, but also automatically recognition and automatic functions can be adjusted. Consequently, the user is able to control his data and information by selecting just several services.

On the one hand, like its mentioned in the literature review previously, attackers are able to get information about a mobile user that he might not want to be shared since they are very personal and not for public. But on the other hand, we have to take into consideration, that public authorities or other institutions may be able gain information about planned terrorist attacks or other criminal activities. Consequently, the fact that recording, monitoring and saving of data is ubiquitous today is not solely negative, but also could be used for positive applications. In addition, the data could be used to improve products and services as well as to adapt those to our individual needs. Nevertheless, the full automation of services and improvements in AI can lead to the loss of jobs. In the end, it is hard to answer the question whether the ubiquitous collection of data is good or bad since there are as always several advantages and disadvantages. People have to decide by their own whether they want to benefit of new technologies or not and in this context they must accept that data of them in collected as a result of using applications. People do not have the possibility to choose to pay money for a service instead of data. They have to decide if the benefit of a service is bigger than the abandon of data. Not using technological services is often connected with losses in costs and efficiency. Finally, the fact that the German law is very strict makes it maybe easier for people to trust services that use their data even if there are sometimes adjustments necessary.

6 Conclusions

The provided research paper analysed and illustrated challenges to security and privacy of mobile users in intelligent environments through a critical analysis of IS literature as well as by methods of interviews with experts. The aim of this research paper was to answer the research question, i.e. if mobile users have to worry a lot about data security and privacy in intelligent environments, due to growing importance of new information and communication technologies as well as significant advances in technological developments that are connected with ubiquitous data collection. These developments lead to the relevance of data security and privacy. As a direct result, some advances in security and privacy for mobile users in intelligent environments have been presented.

To begin with, a systematic literature review according to Webster and Watson (2002) has been conducted to structure and filter relevant articles as a basis for this research paper before several theoretical foundations have been described. In this connection, the main terms of the title, “security and privacy”, “mobile users”, and “intelligent environments” have been defined, analysed and described in more detail to provide insight into the topic and also to delimitate and clarify the main topics. Afterwards, interviews with experts have been conducted to gain additional insight and uncover research gaps by means of specialised knowledge and also to establish practical relevance and experiences. Finally, the interviews with experts represent an essential element with regard to answer the research question.

Significant challenges in security and privacy for mobile users in intelligent environments that have been identified during the literature review are in general hardware-centric, device-independent, software-centric and user-layer attacks and can be divided into passive and active threats. In Particular, monitoring, identity theft, malware and the user itself represent essential challenges with regard to security and privacy for mobile users. In addition to that, there are several security solutions such as encryption and authentication described in today’s specialist literature. Referring to this, after comparing all interviews with experts, it has been turned out that there are a lot of important advances in data security and privacy solutions, on account of which the experts think that mobile user do not have to fear the challenges in security and privacy today as much as 10 years ago. Some experts state that the user itself could decide whether services are used or not since there are access rights, which the user can agree or declare. Nevertheless, 3 of 4 experts declare that it will be more difficult in future to not use technologies and keep all data private and safety. Moreover, it could be inferred from the interviews with experts that no stronger regulations in German law are necessary to protect data since it is already very strict und long procedure to push something but connect with the condition that laws might have to be developed as fast as technological developments are to be always up to date.

In conclusion, the research question cannot be clearly answered with yes or no. Despite the fact that there are advanced security solutions, there can still be threats such as unauthorised access of third persons or monitoring. 100% safety is never existing but researchers today have advanced knowledge and develop steadily new solutions and things. Furthermore, people are still able today to decide which technologies they want to use and which data they want to share. With regard to the experts opinions, this may change in future and if not, people who do not want to benefit of these steadily new technologies in future might suffer a loss of efficiency if they do not use them.

7 Limitations and Further Research

The elaborated research paper is designed to turn out the current state of research as well as identify potential academic voids in intelligent environments with regard to challenges to privacy and security for mobile users. To clarify these issues relevant literature was initially structured by the methods of Webster and Watson before it was summarized and analysed. Despite the fact that it is a very recent and new topic, there is a huge amount of specialist literature available, as a result of which this research paper is temporally restricted to ten years, i.e. it is limited to a period of time from 2007 to 2017. Besides, the fact that the research field is highly dynamic and constantly changing makes necessary for this temporal limitation. Nevertheless, a few books and articles that were published prior to 2007 are used by way of an exception since they provide fundamental and therefore relevant findings. Referring to this, it is necessary to mention that there are some relevant articles for which costs are liable on account of which they could not be used. Another limitation is based on languages. Only English and German papers haven been taken into consideration even though there might be further relevant articles published in other languages offering useful insights. In addition, a larger number of experts in chapter 4 could lead to a higher validity and comparability of the collected data. Unfortunately, the willingness of experts to participate on interviews that are conducted for university research papers is low since there is no real benefit for the experts. Without any personal contacts it is hard to find experts that are willing to do such interviews.

An analysis in the framework of this research paper centres one's attention exclusively on mobile users. It can only be assumed that non-mobile user have to deal with quite similar challenges and chances. In addition, the legal regulations described in chapter 3.3.2 are highly reduced, as a detailed depiction of all German laws and policies would outrun the extent of this research paper as well as being too much focused on legal aspects. Additionally, it may be supposed that there are a few differences in law compared with non-European countries. In further research papers it might be interesting to take a closer look at the parallels and the stages of development of global regulations concerning privacy and security. Furthermore, “Intelligent Environment” is a broad term and involves among other things AI, Sensor Networks and robotics as well as finds application in various practical areas as already described in chapter 3.2.3. Each of these aspects illustrates a research area itself for future papers.

Finally, this research paper is based on a very complex topic consisting of a variety of fields. On account of this, some contextual limitations have been necessary as already mentioned in chapter 3.2 and 3.3. On the one hand, in chapter 3.2.1 the term intelligent environments is simplified, generalised and reduced to all physical surroundings that involve technical components and all kinds of AI. On the other hand, in this chapter various areas of application have been named but only smart homes have been described in more detail. The reason why has already been explained before. It might be interesting to take a closer look at other areas of application than the smart home or create an extra research paper just for one of several areas of applications. Concerning chapter 3.3, challenges to intelligent environments can be divided into ecological, economical, social, ethical or legal and technical challenges (see Donath & Jüptner, 2009, p. 26 ff.). This research paper is limited on ethical, legal and social issues. Even if security and privacy are topics of high interest, in particular in intelligent environments, further research could focus, for example, on these other challenges named, i.e. ecological, economic and technical challenges. Taking everything into consideration, this research paper presents challenges to security and privacy for mobile users in intelligent environments. Few safety measures, advances and solutions are just highlighted within the expert interviews and named in the literature review but not described in detail, on account of which a literary review of advances in security and privacy could be undertaken in the next step.