Privacy in Ubiquitous Computing

Ivan Gudymenko, Katrin Borcea-Pfitzmann
Dresden University of Technology
Dept. of Computer Science
ivan.gudymenko@gmail.com, *katrin.borcea@tu-dresden.de*

1 Introduction

The advent of Ubiquitous Computing (UbiComp) has brought a set of new challenges along with numerous advantages. The notion of UbiComp was envisioned in 1991 by Marc Weiser in his seminal paper [1] and has become a hot topic ever since. Despite a lot of research conducted in the area, there are still a lot of issues to elaborate on.

In this position paper, we describe our concerns about designing UbiComp systems in a privacy compliant and secure fashion. We focus ourselves on privacy management in a dynamic UbiComp environment.

The paper is structured as follows. In Section 2 several UbiComp-specific problems are outlined. We provide for solutions and our general view on ensuring privacy and security in a UbiComp system in Section 3. The importance of implementing ubiquitous systems in a privacy-aware and secure way is outlined in Section 4.

2 Problem statement

UbiComp has a number of peculiarities that distinguish it from conventional computing (like the ones, listed in [2]). Along with the obvious benefits, a number of problems arise that might threaten individual's security and privacy. We name them *Transparent Accessibility* as well as *Self-governess and Loss of Control* problems.

The *Transparent Accessibility* problem is a side effect of the transparency property of UbiComp – hiding the unnecessary (in the context of current operation) information from the entities in order to facilitate their cooperation. The reason why a serious security challenge is introduced is that in case of an access procedure being executed in a transparent fashion, the user either is not able to see *what* is being accessed or by *which means* it has been accessed. Moreover, it might not be clear *which entity* performs an access procedure. This leads to a dramatic loss of control of security and as a consequence endangers privacy of an individual.

Privacy is a broad notion and in order to discuss privacy-related issues it is important to realize what is understood under the "privacy" term. In our group, we define privacy in the following way [3]:

Definition 1. *Privacy of an entity is the result of negotiating and enforcing when, how, to what extent, and in which context which data of this entity is disclosed to whom.*

The *Self-governess and Loss of Control* problem is a consequence of so-called "background computing" – the self-management of a UbiComp system aims at providing comfort and easiness of use, i.e. not distracting a user with technical details of system management and allowing him to focus on his own specific tasks. We believe that this can lead to unrecognized hacking of the whole system. The situation is aggravated by the fact that it is difficult to provide for physical protection of a system due to its pervasive nature (i.e. large spatial distribution and ubiquitous networking).

3 Discussion and Suggestions

In order to make a UbiComp system safer and more privacy-aware, we suggest that the following should be taken into account.

We claim that instead of implementing transparency as an inherent built-in property of UbiComp, it should be an *optional* feature: only if a user allows, the corresponding access procedure may be executed

in a transparent way. In other cases, the system is to provide all necessary details to the user (or to the user agent that has been authorized to manage the individual's privacy and security settings).

We argue that the problem of Self-governess and Loss of Control should be carefully considered while introducing the transition of computing power to the background of a UbiComp system. The desired automation property should be implemented in such a way that the stage of ensuring the required privacy and security levels is restricted to the system design time in order to make sure that proper privacy and security precautions are going to be *inherently* built into the functionality of a UbiComp system.

We believe that ensuring security in any UbiComp system should begin already at system design time and it should continue throughout all the other steps of a UbiComp system development. In order to make security and privacy management more flexible, special extension/variation points (so-called hooks) for unforeseeable extensions/variations (extension/variation hooks) might be provided at system design time. Figure 1 depicts the idea.

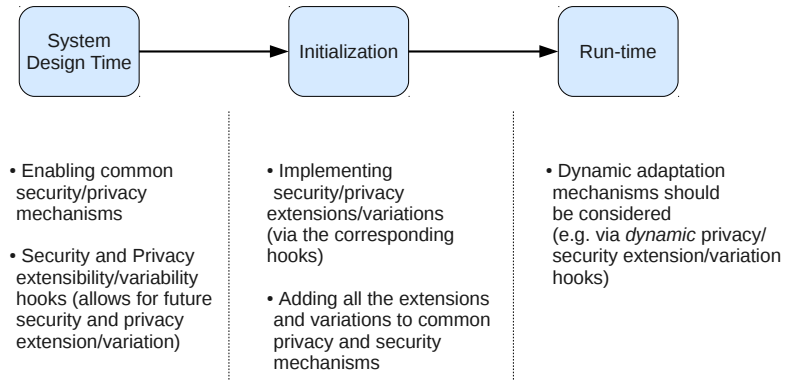

Figure 1: Implementing security and privacy in UbiComp.

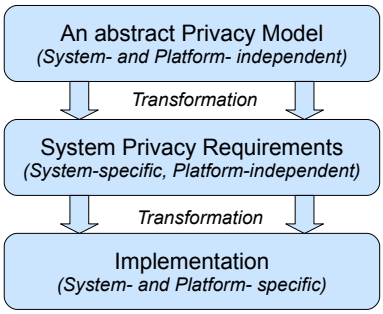

Figure 2: Transformation of a privacy model into implementable requirements.

In order to provide for effective and flexible security and privacy management, we suggest that a so-called *Multilateral Security* concept is used (for more details see [4, 5, 6]). According to the Multilateral Security approach, each party is required to only minimally trust in the honesty of others, thus considering them as potential attackers. In a heterogeneous UbiComp environment, security and privacy conflicts are the norm and should be solved through a negotiation process. The concept implies what degree of security can be achieved against whom with respect to what kind of data or functionality, and what privacy setting is desired to be enforced against whom in which context.

To provide for automation and flexibility, a secure tasks and rights delegation should be supported by a UbiComp system. Under this term it is meant that a user explicitly agrees that a set of his tasks can be solved by another entity according to the user's preferences, i.e. the user *delegates* the rights to perform certain actions on his behalf to another entity.

One of the ways of improving security and privacy in UbiComp was mentioned in [7]: "doing personalized filtering and interpretation by the mobile devices enables to change the main direction of information flow from (semi-) fixed environment to individual instead of from individual to (semi-) fixed environment". This change of information flow "enables a quantum leap in privacy by avoiding the possibility to gather huge amounts of personal data" [7].

Thus, in order to design a UbiComp system in a privacy-aware and secure fashion, the following steps should be considered:

1. Weaving security and privacy mechanisms into the system's functionality already at system design time (see Figure 1). One of the major challenge here is to provide a consistent specification of security and (especially) privacy requirements, i.e. a decent security and privacy model is needed which will allow for a consistent transformation into implementable requirements (see Figure 2).

2. Implementing transparency as an *optional* feature, i.e. *enabling* the exposure of all necessary technical details on each request of a user (or his corresponding privacy and security agent).

3. Enhancing privacy of an individual by changing the main direction of information flow to "infrastructure → user" and applying filtering in order to avoid overload or annoyance of the user. In this case the infrastructure might also broadcast security and privacy advices (e.g. possible options, etc.).

4. Using the Multilateral Security approach to provide for flexible privacy and security management in the deployed UbiComp system through negotiation processes.

4 Why to invest in Privacy and Security

One of the questions that might arise is whether it is really necessary to take much care of security and privacy in UbiComp. Clearly, trying to implement any UbiComp system in a secure and privacy-aware way increases the cost of it. However, we argue that it is absolutely necessary to do so for the number of reasons:

- Security and Privacy concerns are one of the main burdens on the way to accepting ubiquitous systems. Ordinary users are usually not very privacy- and security- aware and would give away some private data in order to obtain certain bonuses [8]. The situation, however, tends to be changing. That means, that companies deploying a secure and privacy-aware UbiComp systems are more likely to have commercial success than the others who have not invested in privacy and security.
- When the infrastructure has been created, it is relatively easy to deploy the system (i.e. to accompany individuals with sensors) since "individual investments pay off immediately" [7] (consider an example of bringing innovation to the car sector ("more personal") and to the railway one ("more public")). Thus, a system with a good privacy and security management mechanisms is more likely to be accepted by the majority and can be deployed relatively easy and be commercially successful, even though additional investments in privacy and security of the system were made.

5 Conclusions

In this position paper, privacy and security issues of UbiComp were considered. Several area-specific problems were outlined and respective suggestions of eliminating/mitigating them were given. We also stated why it is important to construct UbiComp systems in a privacy-aware and secure fashion.

References

[1] Mark Weiser. The Computer for the 21st Century. *Scientific American*, February 1991.

[2] Poslad S. *Ubiquitous Computing: Smart Devices, Environments and Interactions.* Wiley Publishing, 2009.

[3] Manuela Berg and Katrin Borcea-Pfitzmann. Implementability of the Identity Management Part in Pfitzmann/Hansen's Terminology for a Complex Digital World. In Simone Fischer-Hübner, Marit Hansen, Penny Duquenoy, and Ronald Leenes, editors, *Proceedings of PrimeLife / IFIP Summerschool on Privacy and Identity Management for Life*, IFIP Advances in Information and Communication Technology. Springer, 2011.

[4] Andreas Pfitzmann. *Multilateral Security in Communications*, chapter Technologies for Multilateral Security, pages 85–91. Addison-Wesley-Longman, 1999.

[5] Kai Rannenberg, Andreas Pfitzmann, Günter Müller. *Multilateral Security in Communications*, chapter IT Security and Multilateral Security, pages 21–29. Addison-Wesley-Longman, 1999.

[6] Günter Müller, Kai Rannenberg, editor. *Multilateral Security in Communications.* Addison-Wesley-Longman, 1999.

[7] Andreas Pfitzmann. "Accompanying Ambient Intelligence (AAmI) – why you should take your sensors with you ". A sketch, April 2010.

[8] Katrin Borcea-Pfitzmann, Andreas Pfitzmann and Manuela Berg. Privacy 3.0 := Data Minimization + User-Control of Data Disclosure + Contextual Integrity. August 2010.