Chapter 7.7
Privacy Threats in Emerging Ubicomp Applications:
Analysis and Safeguarding

Elena Vildjiounaite
VTT Technical Research Centre of Finland, Finland

Tapani Rantakokko
Finwe LTD, Finland

Petteri Alahuhta
VTT Technical Research Centre of Finland, Finland

Pasi Ahonen
VTT Technical Research Centre of Finland, Finland

David Wright
Trilateral Research and Consulting, UK

Michael Friedewald
Fraunhofer Institute Systems and Innovation Research, Germany

ABSTRACT

Realisation of the Ubicomp vision in the real world creates significant threats to personal privacy due to constant information collection by numerous tiny sensors, active information exchange over short and long distances, long-term storage of large quantities of data, and reasoning based on collected and stored data. An analysis of more than 100 Ubicomp scenarios, however, shows that applications are often proposed without considering privacy issues, whereas existing privacy-enhancing technologies mainly have been developed for networked applications and, thus, are not always applicable to emerging applications for smart spaces and personal devices, especially because the users and their data are not spatially separated in such applications. A partial solution

to the problem of users' privacy protection could be to allow users to control how their personal data can be used. The authors' experience with mobile phone data collection, nevertheless, suggests that when users give their consent for the data collection, they don't fully understand the possible privacy implications. Thus, application developers should pay attention to privacy protection; otherwise, such problems could result in users not accepting Ubicomp applications. This chapter suggests guidelines for estimating threats to privacy, depending on real world application settings and the choice of technology; and guidelines for the choice and development of technological safeguards against privacy threats.

INTRODUCTION

After having read a large number of scenarios of emerging Ubicomp applications (found in project deliverables and research publications which describe prototypes of smart spaces, smart personal devices, objects and their functionalities) and visionary future Ubicomp scenarios (found mainly in roadmaps), we concluded that most scenarios present a sunny, problem-free vision of our future. With the exception of the surveillance problem in some cases, most scenarios do not consider the privacy issues that the new technologies are likely to raise. For example, they do not discuss possible privacy problems due to conflicts between people's interests or personal curiosity.

The discovery that Ubicomp technologies raise privacy problems is not new; and research into privacy protection is actively going on, but after a state-of-the art review of work on privacy protection, we have come to the conclusion that most of this work deals with privacy protection in such network applications as m-commerce, Web browsing, virtual meetings, location-based services, and so forth, where users can be physically separated from their personal data. Even in these applications, no scalable solutions fully applicable in real life exist, and this lack of protection allows large-scale eavesdropping, as we know from the news (Web site of the American Civil Liberties Union and the ACLU Foundation, 2006).

The work on privacy protection in smart spaces and in connection with personal devices is even less mature than that concerned with network applications, while visionary Ubicomp scenarios suggest many situations in which confidential data and secrets occasionally can be discovered. When reading Ubicomp scenarios, however, we rarely found any discussions about the possible implications of a new technology for privacy, and even fewer descriptions of privacy protection measures. M. Langheinrich has collected a list of excuses why privacy protection is rarely embedded in new applications (Langheinrich, 2006), but such a practice can lead to the danger that problems appear after an application has already been developed and installed, and then either the users are left to suffer from privacy violation problems, or application developers are faced with the negative reactions of the users and the need to update the application. One recent example is a bus ticketing application in Helsinki which was storing data about travellers' routes. The application received bad publicity (criticism in the newspaper *Helsingin Sanomat* (Koponen, 2002)), and updating an already installed application would obviously be a costly operation. In cases where users' criticism is directed against an already installed application, which runs on non-reprogrammable microcontrollers (a common situation in the case of a commercial application), an application update can be very costly. Thus, embedding privacy protection in Ubicomp applications at the development stage would be beneficial for application developers.

The main emphasis in this chapter will be on possible problems rather than the benefits of new technologies and applications, because readers of Ubicomp papers usually encounter descriptions of benefits rather than descriptions of problems. The success of Ubicomp development also requires the