



Chapter XII

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

30 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/privacy-threats-emerging-ubicom-applications/4927

Related Content

Event-Based and Publish/Subscribe Communication

Erwin Aitenbichler (2008). *Handbook of Research on Ubiquitous Computing Technology for Real Time Enterprises* (pp. 152-171).

www.irma-international.org/chapter/event-based-publish-subscribe-communication/21767

A QoS aware Framework to support Minimum Energy Data Aggregation and Routing in Wireless Sensor Networks

Neeraj Kumar and R.B. Patel (2009). *International Journal of Advanced Pervasive and Ubiquitous Computing* (pp. 91-106).

www.irma-international.org/article/qos-aware-framework-support-minimum/41706

A Secure Mobile Wallet Framework with Formal Verification

Shaik Shakeel Ahamad, V. N. Sastry and Siba K. Udgata (2012). *International Journal of Advanced Pervasive and Ubiquitous Computing* (pp. 1-15).

www.irma-international.org/article/secure-mobile-wallet-framework-formal/71881

At Sensor Diagnosis for Smart Healthcare: Probability or Conditional Probability Based Approach vs. k-Nearest Neighbour

Chetna Laroia and Vijay Bhushan Aggarwal (2018). *International Journal of Advanced Pervasive and Ubiquitous Computing* (pp. 1-13).

www.irma-international.org/article/at-sensor-diagnosis-for-smart-healthcare/211939

Four Degrees of Freedom Robot Arm, Low-Cost Competition in the Design and Development

Liu Hongcong (2013). *International Journal of Advanced Pervasive and Ubiquitous Computing* (pp. 50-65).

www.irma-international.org/article/four-degrees-of-freedom-robot-arm-low-cost-competition-in-the-design-and-development/93002