Diss. ETH Nr. 16100

Personal Privacy in Ubiquitous Computing

Tools and System Support

A dissertation submitted to the
SWISS FEDERAL INSTITUTE OF TECHNOLOGY ZURICH

for the degree of
Doctor of Sciences

presented by
Marc Langheinrich
Diplom-Informatiker, University of Bielefeld
born February 25, 1971
citizen of Germany

accepted on the recommendation of
Prof. Dr. Friedemann Mattern, examiner
Prof. Dr. Günter Müller, co-examiner

2005

Abstract

Visions of future computing environments involve integrating tiny microelectronic processors and sensors into everyday objects in order to make them "smart." Smart things can explore their environment, communicate with other smart things, and interact with humans, therefore helping users to cope with their tasks in new, intuitive ways. However, this digitization of our everyday lives will not only allow computers to better "understand" our actions and goals, but also allow others to inspect and search such electronic records, potentially creating a comprehensive surveillance network of unprecedented scale.

How should these developments affect our notion of privacy, our "right to be let alone," our freedom to determine for ourselves when, how, and to what extend information about us is communicated to others? Should we give up our solitude and anonymity in light of these new technological realities and create a "transparent society," in which nothing can be kept secret anymore, for better or for worse? Or do we need to surround ourselves with better security mechanisms that will make our communications and our presence untraceable to anyone but the most determined observer?

This thesis argues for a third alternative, a middle ground between the two extremes of abandoning privacy and attempting full-scale anonymity. It proposes an architecture to facilitate the upfront notices of data collections in future computer environments, means to automatically process such announcements and individually configure the available collection parameters, processes to store and subsequently process any such collected data automatically according to the given notices, and tools for individuals to control and inspect their state of privacy in an ever connected world.

In particular, this thesis provides for

- a method to announce privacy policies in smart environments via *privacy beacons* and personal *privacy assistants*,

- a method to reason and act upon such policies by automatically configuring the available services with the help of *privacy proxies*, and
- a method to store the collected information and enforce their respective collection and usage policies through *privacy-aware databases*.

Taken together, these mechanisms can provide the technical foundations for future privacy frameworks that provide a level of privacy protection suitable for smart environments: anytime, anywhere, effortless privacy.

Kurzfassung

In zukünftigen computerisierten Umgebungen werden winzige Mikroprozessoren und -sensoren in Alltagsgegenstände integriert sein, um diese „smart" zu machen. Smarte Dinge können ihre Umgebung wahrnehmen, mit anderen smarten Dingen kommunizieren und mit Menschen interagieren, um so ihre Benutzer beim Bewältigen ihrer Aufgaben auf neue, intuitive Art und Weise zu unterstützen. Diese Digitalisierung unseres Alltags wird allerdings nicht nur Computer dazu befähigen, unsere Handlungen und Ziele immer besser zu verstehen, sondern ebenso unseren Mitmenschen ermöglichen, diese elektronischen Datenspuren zu durchsuchen und damit potentiell ein flächendeckendes Überwachungsnetz von Orwell'schen Ausmaßen Realität werden zu lassen.

Wie sollen diese Entwicklungen unser Verständnis von Privatheit beeinflussen? Werden wir gezwungen, unsere heutige Form der Privatspähre angesichts des technisch Machbaren aufzugeben und eine transparente Gesellschaft zu erschaffen, in der es keine Heimlichkeiten mehr geben wird? Oder müssen wir uns umso stärker um verbesserte Sicherheitsmechanismen bemühen, die es uns erlauben, unsere Kommunikation für Fremde unhörbar und unsere Anwesenheit unsichtbar zu machen?

Diese Arbeit schlägt eine dritte Alternative vor, einen Mittelweg zwischen diesen beiden Extremen von totaler Transparenz und absoluter Geheimhaltung und Anonymität. Sie stellt eine Architektur vor, die den frühzeitigen Austausch von Datenschutzregeln in zukünftigen computerisierten Umgebungen gestattet, die automatische Verarbeitung solcher maschinenlesbarer Ankündigungen zur individuellen Konfiguration der verfügbaren Dienste durchührt, und die die datenschutzgerechte Verwendung der dabei ausgetauschten personenbezogenen Informationen ermöglicht. Gleichermaßen wird den Benutzern ein Werkzeug zur Verfügung gestellt, mit dem sie den aktuellen Zustand ihrer Privatheit – wer hat wann und wie lange welche Informationen über mich und zu welchem Zweck gesammelt – zu jedem Zeitpunkt feststellen und gege-

benenfalls korrigieren können.

Dazu liefert die vorliegende Arbeit die folgenden Beiträge:

- eine Methode, um maschinenlesbare Datenschutzregeln in zukünftigen computerisierten Umgebungen durch *Privacy Beacons* automatisch zugänglich zu machen,
- eine Methode, um in Abhängigkeit dieser Regeln und aufgrund persönlicher Präferenzen mit Hilfe von *Privacy Proxies* Entscheidungen zu treffen und eine Dienstumgebung individuell zu konfigurieren, sowie
- eine Methode, um die so erhobenen Daten im Rahmen der angegebenen Regeln in einer unterstützenden Datenbank (einer sogenannten *Privacy-Aware Database*) zu speichern und zu verarbeiten.

Zusammengenommen können diese Mechanismen eine Grundlage für zukünftige Datenschutzsysteme bilden, die einer Umgebung voller „smarter" Gegenstände angemessen sind: Datenschutz überall, jederzeit und ohne größeren Aufwand für den Einzelnen.