C.1 Privatheitsschutz in mensch-nahen sensorgestützten Umgebungen

Beteiligte: Matthias Hollick, Philipp Richter, Alexander Roßnagel

Motivation

1. Mensch-nahe Sensorik erfasst hochsensitive Information der Trägerin und ihrer unmittelbaren Umgebung in unerreichter Auflösung
   → Privatheitsschutz unzureichend unterstützt
2. Mensch-nahe Aktorik (Herzschrittmacher, Hörhilfe, Insulinpumpe, Exoskelett etc.) zunehmend vernetzt → Missbrauch hat dramatisches Schadpotential; Vertrauensbewertung unzureichend

'Smartphone'

'Smart Watch'

Insulinpumpe

'Fitness Tracker'

'Smart Glasses'

Exoskelett

Idee: rechtskonforme, mensch-nahe, verteilte Ansätze für Privatheitsschutz und Vertrauensbewertung

Stand der Forschung

Stand der Wissenschaft – ausgewählt

- **'Participatory Sensing':** J. Burke, D. Estrin, et al. "ParticipatorySensing". In: Proc. ACM SenSys, WSW Workshop, 2006
- **Zentrale technologische Ansätze:** E. De Cristofaro, C. Soriente, "PEPSI—Privacy-Enhanced Participatory Sensing Infrastructure". In: Proc. ACM WiSec, 2011
- **Erste dezentrale technologische Ansätze:** J. Shi, R. Zhang, et al. "PriSense: Privacy-preserving Data Aggregation in People-centric Urban Sensing Systems". In: Proc. IEEE INFOCOM, 2010
- **Rechtliche Problembereiche:** Schwenke, T. "Google Glass - Eine Herausforderung für das Recht" In: Kommunikation & Recht (K&R), 2013

Eigene Vorarbeiten – ausgewählt

- **Privatheit für *'Participatory Sensing'* :** D. Christin, M. Hollick, et al. "A Survey on Privacy in Mobile Participatory Sensing Applications". In: Journal of Systems & Software (JSS), 2011
- **Dezentrale Schutzmechanismen:** D. Christin, M. Hollick, et al. "IncogniSense: An Anonymity-preserving Reputation Framework for Participatory Sensing Applications". In: Pervasive and Mobile Computing (PMC), 2013
- **Rechtliche Vorschläge für Wearables:** A. Roßnagel, S. Jandt, et al. "Datenschutz bei Wearable Computing - Eine juristische Analyse am Beispiel von Schutzanzügen". In: Schriftenreihe Datenschutz und Datensicherheit, 2012

Hauptziele und wissenschaftliche Vorgehensweise

Nutzer

Technische und juristische Lösungen

Technologie, Infrastruktur und Rechtsrahmen

(1) Angepasste Infrastrukturmodelle:
Auf Basis von Machbarkeitsstudie, für …
i. Part. Sensornetze, smarte Räume
ii. Vitaldaten-, Audio-, Videosensorik
iii. Implantate, medizinische Aktorik

(2) Dezentrale Datenverarbeitungsansätze:
- Inhärent die Privatheit schützende Verarbeitung der Daten
- Sichere verteilte Speicherung der Daten nahe am Nutzer

(3) Rechtsrahmen für die Datenerfassung:
- Analyse der aktuellen Rechtslage
- Definition und Erweiterung des Rechtsrahmens
- Ableitung technischer Anforderungen

wissenschaftliche Vorgehensweise:

- Bereich Machbarkeitsanalyse
  - Bestimmung funktionaler und nichtfunktionaler Anforderungen
  - Entwurf angepasster Infrastrukturmodelle auf Basis der Vorarbeiten zu '*Participatory Sensing*'
  - Einbeziehung Postdoktorand insbesondere für '*Wearables*' und medizinische Implantate
- Bereich Rechtsrahmen
  - Bestimmung von Risiken in spezifischen Situationen der Betroffenen (z.B. Arbeitsverhältnis, gesundheitliche Abhängigkeit)
  - Bestimmung ungeeigneter Rechtsregeln
  - Vorschläge für technikadäquate Rechtsregeln
  - Vorschläge rechtsverträgliche Technikgestaltung
- Bereich Datenverabeitungsansätze
  - Protokollentwurf unter Berücksichtigung von Benutzbarkeitsaspekten (Nachvollziehbarkeit der Datennutzung)
  - Leistungsbewertung durch Simulation und Testbed-Experimente
  - Analyse der Benutzbarkeit durch Nutzerstudien, hierzu Einbeziehung der Usability Experten

Vernetzung

Innerhalb des GRK

Nutzung der leichtgewichtigen Mechanismen	**A.1** Nutzer-Ermächtigung und Dienst-Nutzung
Verständlichmachen des Wertes von Nutzerdaten	**A.2** Nutzersensibilisierung Privatheit & Vertrauen
Analyse von Nutzer-Beziehungen für Mechanismendesign	**B.1** Vertauensbewertung in Sozialen Netzen
Gemeinsame techn. & juristische Betrachtung	**C.2** Privatheit mensch-ferne Sensorik
Nutzung des AlterEgo Ansatzes als Vertrauensanker	**D.1 – D.4** AlterEgo

Innerhalb C.1: Privatheitsschutz in mensch-nahen sensorgestützten Umgebungen

Promotionsthema:
Generische dezentrale Dienstprimitive zum Schutz der Privatheit in mensch-nahen Sensorumgebungen

Betreuer:
Professor Dr. **Matthias Hollick**

Tandem:
Informatik – Recht

Postdoktorand:
Dr. **Philipp Richter**
Rechtliche Herausforderungen der Verschmelzung von Mensch und Technik

Externer Doktorand:
Sicherheit und Privatheit in Netzen

Außerhalb des GRK

Projekt '*EC-Spride*', Sicherheit und Privatheit in Netzen

Nutzung sicherer Kryptobausteine aus TP P1, P2 und S4.

Internationale Kooperation mit der UNSW, AUS