Sichere Netze

– mit dem Nutzer im Zentrum

Im letzten Jahrzehnt des zwanzigsten und im ersten Jahrzehnt des einundzwanzigsten Jahrhunderts hat die weite Verbreitung zweier neuartiger Kommunikationstechnologien die Kommunikation von Menschen drastisch verändert. Der Mobilfunk unterstützt hierbei die persönliche Mobilität von Menschen, und das ubiquitär verfügbare Internet ermöglicht eine Vielzahl von neuartigen Anwendungen, die weit über die klassische Telefonie hinausgehen. Der Schutz der Privatsphäre ist dabei eine wichtige aber bisher nur unzureichend gelöste Herausforderung.

Secure Networks – focusing on the user

In the last decade of the 20th century and in the first decade of the 21st century, the wide distribution of two novel communication technologies changed dramatically the way we communicate. Mobile communications support the user´s personal mobility and the new ubiquity of the internet allows a multitude of novel applications, reaching far beyond conventional telephony. Privacy protection in this context is an important but so far inadequately solved challenge.

Matthias Hollick, Thorsten Strufe, Alejandro Buchmann • Mit der Verfügbarkeit kostengünstiger drahtloser Sensoren/Aktoren ist in einem nächsten Schritt zu erwarten, dass Gegenstände des Alltags vernetzt und in der digitalen Welt erreichbar werden. Es findet also eine Vernetzung nicht nur der Menschen und deren „digitaler Repräsentanten“ sondern auch der sie umgebenden „digitalen Helfer“ statt. Eine Vielzahl nützlicher Anwendungen und Szenarien ist denkbar: „Smart Spaces“, „Smart Homes“ und „Smart Cities“. Diese Anwendungen bezeichnet man als smart, weil sie mit der Umwelt interagieren können und sich hierdurch eine Vielzahl von neuen Möglichkeiten eröffnet: Das Sparen von Energie, weil Sensoren eine optimierte Steuerung von Heizung und Licht ermöglichen; die Steigerung der Effizienz in Logistik und Verkehr, weil Sensoren Auskunft geben über Verkehrsflüsse und Staus und eine optimierte Verkehrslenkung erlauben. Darüber hinaus sind die Nutzer selbst und ihre sozialen Gemeinschaften Teil dieser „smarten“ Umgebungen: Sie bilden ihre sozialen Beziehungen aus der realen Welt in Online-Sozialen Netzen ab und ermöglichen damit eine Verknüpfung dieser sozialen Beziehungen mit den erfassten Umweltdaten. Sie erzeugen und konsumieren Informationen – einerseits in klassischen Server-basierten Netzen aber auch direkt untereinander in sogenannten Peer-to-Peer Netzen. Sie ergänzen vorhandene Sensoren der Infrastruktur durch ihre mit vielfältigen Sensoren ausgestatteten Mobiltelefone (z. B. Mikrofon, Kamera, Beschleunigungssensoren, GPS) die ihre direkte Umwelt erfassen.

Aus technologischer Sicht bilden Kommunikationsnetze den Nukleus der oben genannten Systeme. Sie zeichnen sich dadurch aus, dass die Anzahl der vernetzen Geräte extrem hoch ist, da auf jeden Einwohner einer „Smart City“ mannigfaltige vernetzte Geräte entfallen. Diese Netze besitzen heterogene Komponenten: Von dedizierten und kabelgebundenen stationären Sensoren bis hin zu hochmobilen Endsystemen, die drahtlos kommunizieren. Eine Vielzahl technologischer Herausforderungen für diese Netze der Zukunft gilt als bisher ungelöst, wie zum Beispiel die Netze hinsichtlich Nutzeranzahl, Ereignismenge, Mobilität, etc. skalierbar zu gestalten. Betrachtet man diese Netze mit dem Menschen im Fokus, so ist der Schutz der Privatsphäre eine wichtige aber bisher nur unzureichend gelöste Herausforderung.

Wieso ist dies der Fall? In „smarten“ Umgebungen wird eine Vielzahl von Daten erhoben, die über einzelne Nutzer Aufschluss geben können. Die Nutzer selbst sind über am Körper getragene Sensoren (zum Beispiel Mobiltelefone) integraler Bestandteil des Monitorings ihrer Umgebung. Soziale Beziehungen zwischen Nutzern sind über Online-Soziale Netze nachvollziehbar. Eine Verknüpfung dieser unterschiedlichen Datenquellen, deren Aggregation oder Anreicherung führt dazu, dass potenziell Bewegungsmuster erstellt werden können und der Schutz der Privatsphäre der Nutzer bedroht ist.

Hier setzen die Arbeiten der Gruppen von Alejandro Buchmann, Matthias Hollick und Thorsten Strufe an, indem sie auf unterschiedlichen Ebenen Beiträge leisten, die den Schutz der Privatsphäre von Nutzern auch für die skizzierten zukünftigen Netze ermöglichen.

Scopes – Ein neues Kommunikationsparadigma für Sensornetze

Das in der Gruppe von Alejandro Buchmann entwickelte Kommunikationsrahmenwerk Scopes wurde speziell auf drahtlose Sensornetze angepasst und ermöglicht, dass die Sichtbarkeit der erfassten Daten eingeschränkt werden kann. Scopes basiert

Matthias Hollick

auf dem Grundprinzip des Publish/Subscribe; hierbei werden von der Datenquelle Ereignisnachrichten erzeugt und kommuniziert, auf Abnehmerseite wird das Interesse an Ereignissen spezifiziert, ein Mediator vermittelt zwischen Quelle und Abnehmer der Ereignisse. Scopes realisiert als ein solcher Mediator dynamische Gruppen innerhalb des Sensornetzes. Diese können auf Basis von Anwendungsklassen („Alle Temperatursensoren"), geographischen Positionen („Sensoren im Hauptbahnhof"), Systemeigenschaften/-zuständen („Sensoren mit Fehlergenauigkeit kleiner 1%, Sensoren mit Restlaufzeit von mindestens 1 Woche"), Schutzleveln („Öffentliche Sensoren"), etc. sowie Kombinationen entsprechender Kriterien („Sensoren zur Messung der Luftqualität in der Rheinstrasse; Restlaufzeit von mindestens 1 Monat ") erstellt und dynamisch verwaltet werden.

Thorsten Strufe

Die Einschränkung der Sichtbarkeit von Daten erfordert in Kombination mit Scopes den Einsatz entsprechender angepasster Kryptoverfahren, da klassische identitätsbasierte Verfahren nicht flexibel genug sind. Für den vorgestellten Anwendungsfall bietet sich die attributbasierte Kryptographie an, bei der der Zugriff auf die erhobenen Daten anhand von Attributen der Daten selbst und nach entsprechenden Regeln erfolgt. Gleichzeitig müssen diese Verfahren der attributbasierten Kryptographie für leichtgewichtige Sensorplattformen angepasst werden.

Schutz der Privatsphäre für Sensornetze auf Basis von Mobiltelefonen

Neben dedizierten Sensornetzen wird aktuell die Nutzung von Mobiltelefonen als Sensoren vorangetrieben (sogenannte „partizipative" Sensornetze). Der Vorteil einer extrem hohen Durchdringung unserer Umwelt mit diesen Sensoren - wo Nutzer sind, sind auch Sensoren – ist gleichzeitig kritisch hinsichtlich des Schutzes der Privatsphäre zu bewerten – eine direkte Zuordnung von Sensor zu Nutzer ist möglich.

In bisherigen Systemen ist der Nutzer zwar in den Prozess der Datenerfassung einbezogen, nicht jedoch in die Abwägungen zum Schutz der Privatsphäre. In der Gruppe von Matthias Hollick werden daher Lösungen entwickelt, die den Nutzer aktiv in den Prozess der Privatsphäre-bewussten Datenerhebung und -weitergabe einbeziehen. Hierzu wird abweichend von den klassischen Systemen, die eine zentrale Datenbank für erfasste Sensordaten nutzen, ein verteilter Ansatz auf Basis des Peer-to-Peer Paradigmas verfolgt. Dieser baut darauf auf, die erhobenen Daten mit vertrauenswürdigen Nutzern oder vertrauenswürdigen Nutzergruppen zu teilen (diese Beziehungen können bspw. in Online-Sozialen Netzen abgebildet werden). Innerhalb dieser Gruppen sich vertrauender

Fachgebiet Sichere Mobile Netze
Prof. Dr.-Ing. Matthias Hollick
Tel. 06151/16-70922
E-Mail: matthias.hollick@seemoo.tu-darmstadt.de
www.seemoo.tu-darmstadt.de

Fachgebiet Peer-to-Peer Netzwerke
Prof. Dr.-Ing. Thorsten Strufe
Tel. 06151/16-6774
E-Mail: strufe@cs.tu-darmstadt.de
www.p2p.tu-darmstadt.de

Fachgebiet Datenbanken und Verteilte Systeme
Prof. Alejandro Buchmann, PhD
Tel. 06151/16-6228
E-Mail: buchmann@dvs1.informatik.tu-darmstadt.de
www.dvs.tu-darmstadt.de

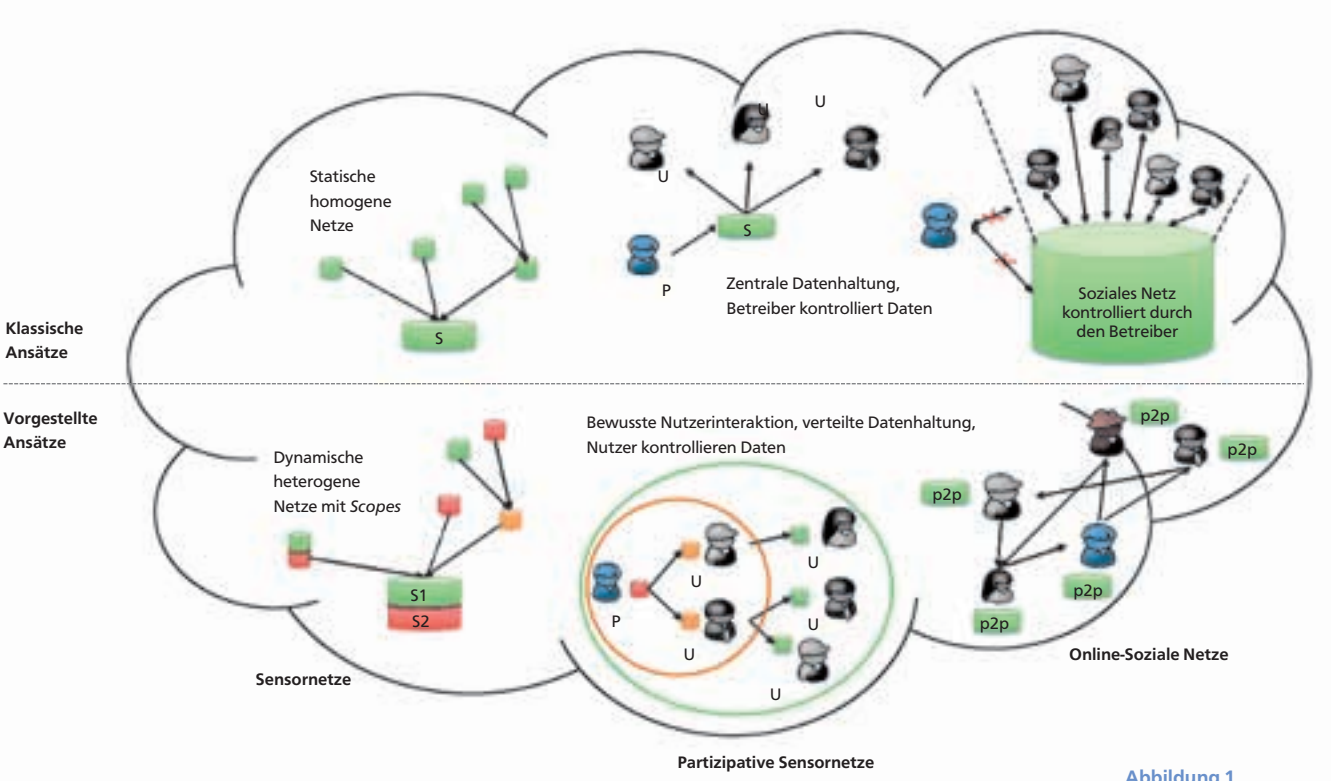

Abbildung 1
Klassische vs. nutzerzentrierte Sicherheit in Netzen

Nutzer erfolgt eine Verschleierung der Identität der Datenquelle, indem sich vertrauende Nutzer die Daten anonymisieren bzw. aggregieren: Mit zunehmender Entfernung von der Datenquelle verringert sich damit die Möglichkeit direkte Rückschlüsse auf die Quelle zu ziehen.

Dem Nutzer fällt bei dem hier verfolgten partizipativen Ansatz eine Schlüsselrolle zu: Die Festlegung der Attribute der erfassten Daten zur Zugriffsbeschränkung sowie die Etablierung von Vertrauensverhältnissen beziehen den Nutzer mit ein. Sensoren des Mobiltelefons werden genutzt, um in direkter Interaktion mit anderen Nutzern Vertrauensbeziehungen bewusst zu etablieren.

Schutz der Privatsphäre in Online-Sozialen Netzen (OSN)

Online-Soziale Netze wie Facebook, LinkedIn, XING, bilden soziale Beziehungen der realen Welt in die virtuelle Welt des Internet ab. Der Schutz der Privatsphäre wird bei diesen Systemen heute von den Betreibern des sozialen Netzes definiert und umgesetzt, häufig zu Lasten des Nutzers, der Privates nur unzureichend schützen kann.

Die Gruppe von Thorsten Strufe erforscht aus diesem Grund die Benutzung, und insbesondere neue Architekturen für Online-Soziale Netze. Dabei steht der bessere Schutz privater Daten der Benutzer im Vordergrund. Auch hier wird das Peer-to-Peer Prinzip verfolgt: Die Daten werden nicht zentral gespeichert und verwaltet sondern verteilt auf den Rechnern der beteiligten Benutzer. Diese können den Zugriff auf ihre Daten feingranular erlauben, oder auf Wunsch – bis hin zu ihrer eigenen vollkommenen Unsichtbarkeit für andere Benutzer – verstecken. Ein allwissender Zugriff zentraler Instanzen, wie er bisher den kommerziellen Betreibern möglich ist, wird dadurch verhindert.

Fazit

Die vorgenannten Lösungsansätze basieren auf verwandten und sich gegenseitig ergänzenden Grundprinzipien: Die Einschränkung der Sichtbarkeit von Daten; die verteilte Speicherung und Datenhaltung; die Nutzung attributbasierter Zugriffskontrolle und die Einbindung des Nutzers selbst in den Prozess der Attributzuweisung. Gemeinsam erlauben diese Ansätze einen verbesserten und transparenten Schutz der Privatsphäre von Nutzern.

Matthias Hollick ist seit 2009 Professor am Fachbereich Informatik der TU Darmstadt. Er leitet das Fachgebiet „Sichere Mobile Netze" und ist Principal Investigator des LOEWE-Zentrums CASED.

Thorsten Strufe ist seit 2009 Juniorprofessor am Fachbereich Informatik der TU Darmstadt. Er leitet das Fachgebiet „Peer-to-Peer Netzwerke" und ist Principal Investigator des LOEWE-Zentrums CASED.

Alejandro Buchmann ist seit 1991 Professor am Fachbereich Informatik der TU Darmstadt. Er leitet das Fachgebiet „Datenbanken und Verteilte Systeme" und ist Principal Investigator des LOEWE-Zentrums CASED.