soft beziehungsweise IDC nicht die einzigen, die solche Gefahren beobachten - eine einfache Recherche bei Google fördert umfangreiche Berichte in Diskussionsforen über virenverseuchte Crack-Tools zu Tage.

Während sich jeder Nutzer von Schlüsselgeneratoren oder Crack-Tools der Gefahr bewusst sein sollte, dass er neben möglichen Urheberrechtsverletzungen auch massiv die Sicherheit seines Systems gefährdet, liegt für den professionellen Einsatz die Gefahr eher beim Kauf auf Online-Auktionsplattformen: Wie kann der Käufer zwischen einem „Schnäppchen" und einer Raubkopie unterscheiden? Die in der Studie genannten 50.000 Interventionen von Microsoft bei Ebay-Versteigerungen pro Jahr dürften nicht alle Raubkopien aus dem Verkehr ziehen. ■

Quellen:

IDC:The Risks of Obtaining and Using Pirated Software, Oktober 2006, <http://go.microsoft.com/fwlink/?linkid=73969>

Microsoft geht gegen Anbieter gefälschter Programme auf Online-Auktionen vor:

Pressemitteilung vom 31.10.2006, http://www.microsoft.com/germany/presseservice/detail.mspx?id=531775

Stichworte: Microsoft, Raubkopie, Software-Risiken

Ubiquitous Computing: Herausforderungen für Datenschutz und Datensicherheit

Stellen Sie sich vor, Sie leben in einer Welt, in der sich winzige Computer oder Sensoren an Sie anpassen, in der sich die Dinge nach Ihren Wünschen ändern - einfach, weil Sie es so wollen. Ein europäisches Forschungsprojekt hat die Probleme dieser „schönen neuen Welt" untersucht.

Von MICHAEL FRIEDEWALD und RALF LINDNER, Karlsruhe*

Der Begriff „Ubiquitous Computing" (UbiComp) wurde in den späten 1980er Jahren im kalifornischen Palo Alto Research Center der Firma Xerox von einem Forscherteam um Mark Weiser geprägt und bezeichnet die Vision einer alles durchdringenden Computertechnologie, welche durch die stetige Miniaturisierung von Computerchips und -speichern sowie Fortschritten der Sensortechnik und der drahtlosen Kommunikation ermöglicht wird. Zusammen mit stetig fallenden Preisen führen diese Fortschritte dazu, dass derartige elektronische Komponenten in immer mehr alltägliche Dinge eingebaut werden können, so dass diese letztlich über die Sensoren „fühlen", mit Hilfe des Chips „denken" und „sich erinnern" sowie dank der drahtlosen Kommunikationsmodule miteinander „reden" können. Das alles klingt nach Science Fiction, kann aber bald Realität sein.

Die Vision einer durch und durch vernetzten Zukunft voll smarter Alltagsgegenstände verspricht eine Reihe von faszinierenden Anwendungsmöglichkeiten: Gebrauchsgegenstände können kaum mehr verloren gehen, da sie jederzeit selbst wissen, wo sie sich befinden und diese Information bei Bedarf an das Mobiltelefon ihres Besitzers funken. Autos könnten automatisch ihren Verschleiß überwachen und rechtzeitig Wartungsarbeiten empfehlen. Im Umweltschutz könnten solche kommunizierenden Kleinstcomputer wertvolle Arbeit leisten, zum Beispiel als winzige Sensoren, die Fischschwärme verfolgen oder tektonische Bewegungen registrieren. Dazu kommt die unübersehbare Anzahl von personalisierten und ortsbezogenen Informationsdiensten. RFID-Technologie wird bereits heute von Einzelhandelsunternehmen wie Walmart oder Metro zur Überwachung der Logistikkette eingesetzt. Mit diesen Anwendungen werden - nicht immer ungewollt und quasi als Nebenprodukt der Verwendung solcher bequemer oder qualitätssteigernder Dienste - leicht individuelle Aktivitätsprotokolle angelegt, welche beinahe lückenlos Auskunft über das Leben einer Person geben können.

Langfristig ergeben sich, bedingt durch die Anwendungsbreite des UbiComp, viele spannende gesellschaftliche und politische Herausforderungen. So wächst innerhalb der Forschungs- und Entwicklungsszene langsam auch das Bewusstsein, dass das UbiComp weit reichende Implikationen für Privatsphäre, Identität, Sicherheit und Vertrauen haben wird. Das von der Europäischen Union geförderte Projekt „Safeguards in a World of Ambient Intelligence " (Schutzmaßnahmen in einer Welt intelligenter Umgebungen; Ambient Intelligence und Pervasive Computing sind weitere, synonyme Begriffe für Ubiquitous Computing) hat sich in den vergangenen zwei Jahren eingehend mit diesem Thema befasst.

Für die von UbiComp ausgehenden Gefahrenpotenziale für die Privatsphäre zeichnen zwei zen-

trale technische Innovationen verantwortlich: zum einen die massiv erhöhten Kapazitäten zur technischen Erfassung und Speicherung alltäglicher Aktivitäten und Interaktionen von Privatpersonen in vielfältigen Ausprägungen sowie über große Distanzen und Zeiträume hinweg, zum anderen die gesteigerten Fähigkeiten zur schnellen Durchsuchung und Verknüpfung von großen Datenbanken, womit zusätzliche Möglichkeiten zur Erstellung von personenbezogenen Datenprofilen und anderen Formen des Data Mining einhergehen.

Die bisher durch den Gesetzgeber erhobene Forderung nach prinzipieller Zweckgebundenheit aller gewonnenen Daten erscheint in einer Zukunft voll „schlauer" und miteinander kommunizierender Alltagsgegenstände nicht mehr praktikabel, da sie das Gedächtnis solcher Gegenstände so gut wie verbietet. Ein Verbot der Speicherung von Information für zukünftige, aber a priori unbekannte Zwecke widerspricht allerdings dem Kerngedanken vieler personalisierter UbiComp-Anwendungen.

Ganz allgemein kann man folgende Problembereiche identifizieren, mit denen die Nutzer beziehungsweise Betroffenen von UbiComp sehr wahrscheinlich konfrontiert sein werden:

1. Ein allgegenwärtiges Netzwerk von Anwendungen und Kommunikationen zieht einen massiven Anstieg bei der Erhebung und Übermittlung personenbezogener Daten nach sich, eine zeitliche und räumliche Begrenzung ist kaum mehr möglich.

2. Die Einführung von biometrischen Verfahren, Kameras und Wahrnehmungssensoren für bestimmte Anwendungen verändert die Qualität der im Umlauf befindlichen personenbezogenen Daten.

3. Neue Verfahren der Verarbeitung und Verknüpfung von Daten erlauben eine umfassende Katalogisierung der Person.

4. Die Interkonnektivität zwischen vielen smarten Gegenständen schafft ein kaum mehr zu überblickendes Datennetz, im dem Datenströme mit herkömmlichen Mitteln nicht mehr zu kontrollieren und zu verwalten sind.

Die Studie identifiziert eine Reihe von Themen, die sich als problematisch erweisen könnten: Datenschutz und Datensicherheit, Identität sowie Überwachung.

Schutz der Privatsphäre: Wenn Datenschutz das individuelle Recht ist, die Verbreitung von Informationen über die eigene Person zu kontrollieren, wie schützt sich dann der Einzelne in einer Welt, in der überall und automatisch personenbezogene Daten erhoben werden? In einer Welt des UbiComp können wir davon ausgehen, dass wir ununterbrochen überwacht werden, weil die dauernde Erfassung und Echtzeit-Verarbeitung von Daten über unsere Präsenz und unser Verhalten eine Grundvoraussetzung der UbiComp-Welt sind.

Sicherheit: Neben dem Schutz persönlicher Daten zur Gewährleistung der Privatsphäre ist beim UbiComp natürlich auch die Datensicherheit von Bedeutung, worunter klassischerweise Vertraulichkeit, Zugriffsschutz und Authentizität fallen, aber im allgemeineren Sinne auch Eigenschaften wie Vertrauenswürdigkeit, Verfügbarkeit, Verlässlichkeit und Funktionssicherheit verstanden werden dürfen. Sicherheit ist in diesem Sinne oft auch eine Voraussetzung zur Realisierung von Datenschutzzielen. In einer Welt intelligenter Dinge dürfte ein Hauptproblem der Sicherheit in der Heterogenität und der großen Zahl der beteiligten Komponenten liegen, die in einer offenen Umgebung sicher und verlässlich zusammenspielen sollen, wobei erschwerend hinzukommt, dass die Komponenten typischerweise mobil sind und untereinander spontane Kooperations- und Kommunikationsbeziehungen eingehen können.

Vertraulichkeit: Es ist offensichtlich, dass durch die notwendigerweise drahtlose Kommunikation mobiler Gegenstände eine im Prinzip einfache Mithörmöglichkeit durch benachbarte Empfänger gegeben ist - in der Regel erscheint also eine Verschlüsselung der Kommunikation unabdingbar. Dem stehen in manchen Fällen jedoch mangelnde Ressourcen entgegen: Kleinsten Sensoren etwa steht oft nur sehr wenig Energie zur Verfügung, eine Verschlüsselung der zu übermittelnden Sensordaten kann den Energiebedarf vervielfachen, was wiederum einige Anwendungen erschwert.

Neben technischen Aspekten spielen bei den Themen Datenschutz- und -sicherheit auch soziale, rechtliche und politische Gesichtspunkte eine Rolle. Während man früher den allwissenden Staat beargwöhnte, inzwischen aber mehr und mehr informationshungrige Marketingabteilungen großer Firmen im Blickfeld hat, wird mit Miniaturkamera und in die Kleidung integriertem Computer jeder Einzelne zum ständigen Datensammler – oder, schlimmer noch, sogar smarte Gegenstände, für die sich niemand mehr richtig verantwortlich fühlt. An die Stelle des „großen Bruders" treten so zahllose „kleine Geschwister" in Form von neugierigen Nachbarn und eifersüchtigen Bekannten, deren Hemmschwelle für ein gelegentliches Bespitzeln mit dem technischen Aufwand für solch eine Überwachung sinken dürfte.

Die Durchdringung praktisch aller Lebensbereiche mit UbiComp-Anwendungen birgt außerdem

die Gefahren des Drucks zur sozialen Anpassung und der digitalen Spaltung der Gesellschaft. So könnten viele Menschen gezwungen sein, die neue Technologie anzuwenden, um wichtige Dienste überhaupt nutzen und am gesellschaftlichen Leben teilnehmen zu können.

Angesichts der Vielschichtigkeit potenzieller Gefahren, die mit UbiComp verbunden sein können, fordert die Studie ein möglichst breit angelegtes Risikomanagement und präventive Schutzmaßnahmen in mehreren Dimensionen:

- UbiComp befindet sich noch überwiegend in der Forschungs- und Entwicklungsphase. Insofern werden in den aktuellen Prozessen der Technikgestaltung bedeutsame Weichenstellungen vorgenommen. Daher gilt es, frühzeitig auf datensparsame und datenschutzfreundliche Anwendungen hinzuwirken. Die öffentliche Förderung von F&E-Projekten könnte weitaus stärker als bisher an eine verpflichtende Auseinandersetzung etwa mit Fragen der informationellen Selbstbestimmung, des Schutzes der Privatsphäre und des sicheren Identitätsmanagements geknüpft werden.

- Transparenz sollte die Standardeinstellung bei UbiComp-Diensten sein. Nutzer hätten dann einen Anspruch darauf, detailliert in Erfahrung bringen zu können, welche Daten von wem für welche Zwecke erhoben, gespeichert und gegebenenfalls weiterverarbeitet werden. Aufgrund der Vielzahl der Datenerfassungen ist hier eine allgemein verständliche Aufklärung der Betroffenen geboten.

- An zahlreichen Stellen gilt es, den rechtlichen Rahmen an die Herausforderungen von UbiComp anzupassen. So ist derzeit nicht abschließend geklärt, welchen rechtlichen Status Willenserklärungen haben, die im Namen des Nutzers zum Zwecke des automatisierten Identitätsmanagements von technischen Assistenten (zum Beispiel Smartphones) abgegeben werden. Ferner wirft die zu erwartende Intensivierung der Weiterverarbeitung personenbezogener Daten in verschiedenen Ländern die Frage nach der Durchsetzung eines einheitlichen Schutzniveaus auf.

- Datenschutzrechtliche Bedenken der Verbraucher können neben der eigentlich selbstverständlichen Einhaltung von rechtlichen Vorschriften auch durch verschiedene Formen der Selbstverpflichtung - etwa die Umsetzung einschlägiger Industrienormen wie ISO 15408 und ISO 17799 – oder unabhängige Zertifizierungen begegnet werden.

Bekanntlich ist aber der kompetente und aufgeklärte Verbraucher der wirksamste Schutz vor bedenklichen Eingriffen in das Recht auf informationelle Selbstbestimmung.

Dies gilt umso mehr unter den Bedingungen von UbiComp. Öffentliche Bewusstseinsbildung, Sensibilisierung und die Entwicklung von Medienkompetenz bleiben somit eine der zentralen Forderungen an Bildungseinrichtungen wie öffentliche Institutionen. ■

Internet: http://swami.jrc.es

* Michael Friedewald und Ralf Lindner sind wissenschaftliche Mitarbeiter am Fraunhofer-Institut für System- und Innovationsforschung (www.isi.fraunhofer.de).

Stichworte: Ubiquitäres Computing

Anonymisierungssoftware von IBM

IBM hat am 26. Januar 2007 die Fertigstellung einer Software verkündet, mit der Nutzer ihre personenbezogenen Daten im Internet verstecken oder anonymisieren können. Der „Identity Mixer“ oder „Idemix“ , der im Züricher Labor von IBM entwickelt wurde, soll es Kunden ermöglichen, im Internet Waren oder Dienstleistungen zu erwerben, ohne dabei ihre Identität preisgeben zu müssen. Die Idemix-Software soll dem Eclipse Higgins-Projekt zur Verfügung gestellt werden. Dieses Projekt bemüht sich um die Entwicklung von Open Source-Software, mit der Nutzer selbständig kontrollieren können sollen, wer im Internet Zugriff auf ihre persönlichen Daten nehmen darf. Idemix verwendet dabei Pseudonyme, die es dem Nutzer beispielsweise ermöglichen sollen, Onlineeinkäufe ohne Angabe der Kreditkartennummer zu tätigen oder den Altersnachweis ohne Angabe des Geburtsdatums zu erbringen. Zertifizierte Institutionen wie Banken können dem Nutzer einen Berechtigungsnachweis für den Ausweis gegenüber anderen Onlineinstitutionen ausstellen. ■ SK

Internet: www.zurich.ibm.com

Stichworte: IBM, Identity Mixer, Idemix, Pseudonym, Open Source