in: Helmut Bäumler, Astrid Breinlinger und Hans-Hermann Schrader (Hrsg.): Datenschutz von A-Z; Erg. Lfg. 4, Luchterhand, Neuwied 2001.

Mobile Computing

Hannes Federrath
federrath@inf.tu-dresden.de

Zum Begriff

Mobile Computing ist ein unscharfer Oberbegriff für verschiedene Formen von Mobilkommunikation. Unter Mobile Computing im engeren Sinn versteht man die Datenverarbeitung auf einem tragbaren Computer. Hierzu kommen leichte, portable Geräte zum Einsatz. Mobile Rechner können Laptops, Personal Digital Assistants (PDAs), Mobiltelefone (→ *Mobilfunknetze*) mit PDA-Funktion sowie kleine, in Gegenstände eingebettete Computer (embedded devices) sein.

Im Zusammenhang mit Mobile Computing findet man u.a. die Begriffe Ubiquitous Computing, Nomadic Computing, Pervasive Computing, Wireless Networks (auch Wireless LANs), Wireless Application Protocol (WAP), Bluetooth, Mobile IP, mobile Agenten, die jeweils Konzepte bzw. Technologien des Mobile Computing sind.

Interessant wird Mobile Computing, wenn die Geräte trotz ihrer Ortsunabhängigkeit vernetzt werden, z.B. an das → *Internet* angeschlossen werden können oder sich spontan untereinander vernetzen (z.B. in einem Konferenzraum) mittels so genannter Ad-hoc-Netzwerke.

Technische Anforderungen

Mobile Computer müssen, da sie viel leichter als stationäre Computer in fremde Hände gelangen können, besonders gut gegen unbefugten Zugang und damit Zugriff auf die darauf gespeicherten Daten geschützt werden. Inzwischen sind derartige Produkte (mit → *Chipkarten*-Zugangssystem oder → *Biometrie*) verfügbar. Es ist zu beachten, dass die auf dem Massenspeicher (→ *Festplatte*) gespeicherten Daten möglichst verschlüsselt abgelegt sind und erst nach einer erfolgreichen Zugangskontrolle entschlüsselt zugreifbar sind.

Durch die Mobilität der Teilnehmer entstehen an die Technik im Vergleich zur ortsgebundenen Festnetzkommunikation neue Herausforderungen: Die Bandbreite auf der Luftschnittstelle ist knapp und zudem störanfälliger als die Leitungen des Festnetzes. Zeitweilige Diskonnektivitätsphasen führen möglicherweise zum Abbruch der Kommunikation und müssen z.B. durch Caching-Techniken (vorsorgliches Speichern später benötigter Daten) ausgeglichen werden.

Datenschutzrechtliche Risiken

Die Luftschnittstelle bietet leichte Angriffsmöglichkeiten. Daten können, wenn sie nicht besonders geschützt sind, leicht gestört, verändert und mitgelesen werden. Aus Datenschutzsicht sollte insbesondere das leicht mögliche Abhören durch den Einsatz von Verschlüsselungstechnologien (→ Kryptographie) verhindert werden. Verschlüsselungsverfahren werden zunehmend eingesetzt, sind aber meist noch nicht standardmäßig vorhanden. Außerdem ist für den mobilen Benutzer

häufig nicht erkennbar, ob vorhandene Verschlüsselungsverfahren auch tatsächlich aktiviert sind (so beispielsweise bei GSM-Mobiltelefonen, Schnurlostelefonen nach dem DECT-Standard sowie Wireless LANs).

Die Mobilität führt zur Erhebungsmöglichkeit personenbezogener Ortsinformation (Peilbarkeit) oder sogar zur Erstellbarkeit von Bewegungsprofilen. Spezielle Verfahren zum Schutz vor Lokalisierung sind theoretisch zwar entwickelt, aber praktisch noch nicht im Einsatz.

Die starke Vernetzung mobiler Geräte bringt ebenfalls Datenschutzprobleme mit sich: Die potentielle Möglichkeit beim Ubiquitous Computing, dass jedes kleine, mobile Gerät mit jedem anderen kommunizieren kann, führt aufgrund der meist statischen Adressierungsinformation (jedes Gerät besitzt eine Adresse, z.B. eine → IP-Nummer, über einen längeren Zeitraum) zu Überwachbarkeit der Aktivitäten des Benutzers.

Perspektiven

Die Mobilität der Benutzer ermöglicht auch die Realisierung neuer Informationsdienste, bei denen das Informationsangebot in Abhängigkeit vom aktuellen Standort wechselt. Solche ortsabhängigen Dienste (z.B. Finden der nächstgelegenen Tankstelle oder Abruf des lokalen Wetterberichts) sind durchaus zweckmäßig, sollten aber unter Datenschutzgesichtspunkten möglichst datensparsam implementiert sein, was momentan eher nicht der Fall ist, da der mobile Benutzer meist ständig lokalisier- und verfolgbar ist.

Die Miniaturisierung ermöglicht es zukünftig, sehr kleine Computer in unscheinbaren Geräten (Kaffeetassen, Regenschirmen, Büchern, Schreibgeräten etc.) unterzubringen, die sich spontan mit anderen Computern vernetzen und Daten auszutauschen. Somit ist nahezu keine Umgebung mehr vom Mobile Computing und der Vernetzung ausgeschlossen. Die Allgegenwart von Informationsverarbeitung wird deshalb auch als Pervasive bzw. Ubiquitous Computing bezeichnet. Beim Pervasive bzw. Ubiquitous Computing ist nicht mehr leicht nachvollziehbar, wer welche Daten wann und wo verarbeitet hat. Teilweise ist wegen der Kleinheit der Computer nicht einmal mehr erkennbar, dass Daten verarbeitet werden.

Links und Literatur zu Mobile Computing

Allgemeine Informationen zu Mobile Computing

- *Jochen H. Schiller:* Mobilkommunikation -- Techniken für das allgegenwärtige Internet. Addison-Wesley, 2000
- Linksammlung des Computer Information Center „Mobile and Wireless Computing“: http://www.compinfo-center.com/tpmobl-t.htm

Sicherheitsapekte und Schutz vor Bewegungsprofilen

- *Hannes Federrath:* Sicherheit mobiler Kommunikation. DuD Fachbeiträge, Vieweg, Wiesbaden 1999
- Links zu Sicherheit im Mobile Computing und Mobilkommunikation: http://www.inf.tu-dresden.de/~hf2/mobil

Ubiquitous Computing und Pervasive Computing

- http://eclass.cc.gatech.edu/classes/cs8113c_99_spring/readings/overview.html
- http://nano.xerox.com/hypertext/weiser/UbiHome.html
- http://homepage1.nifty.com/konomi/shinichi/ubicomp.html