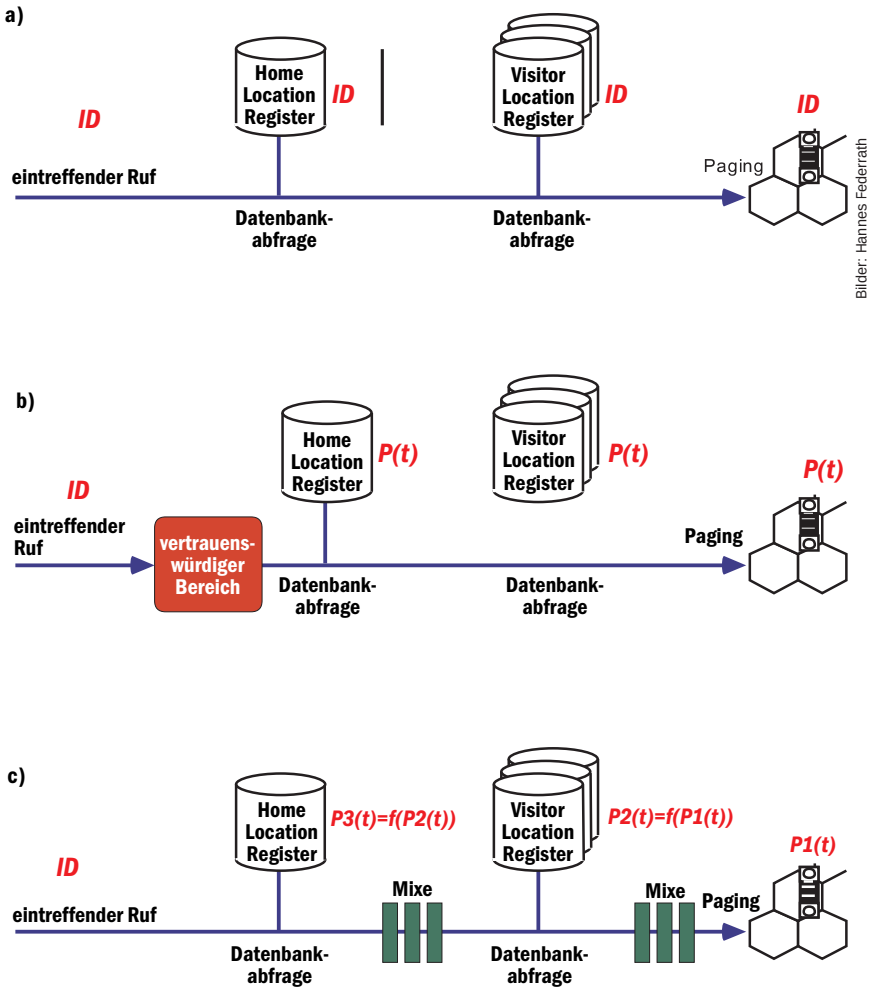
Mobilkommunikation ohne Spuren

Betreiber mobiler Kommunikationsnetze verheimlichen gern, daß jeder Nutzer ihrer Netze Spuren hinterläßt. Leider hat die Sicherheit von GSM (Global System for Mobile Communication) in dieser Hinsicht nicht mit der hohen Verbreitung der Mobilkommunikation Schritt gehalten.

Von Hannes Federrath



Bilder: Hannes Federrath

Verbindungsaufbau a) bei GSM, b) mit temporären Pseudonymen c) bei den Mobilkommunikationsmixen

Sobald der Besitzer sein Handy einschaltet, meldet es sich beim Netzbetreiber an. Hierzu werden Daten zur Identität des Nutzers, die Seriennummer des Handys und Daten zum aktuellen Standort an die Basisstation übermittelt. Unabhängig davon, ob der Nutzer wirklich telefoniert, tauscht das Handy mit der Basisstation Daten über den Standort aus. Das ist nötig, um eingehende Rufe zum Handy weiterzuleiten, wenn es eine Funkzelle wechselt. Der Netzbetreiber protokolliert und speichert jeden Verbindungsversuch, unabhängig davon, ob die Verbindung zustande kam oder nicht.

Einige der ausgetauschten Daten sind für die Funktion des Netzes notwendig. Hierzu zählt beispielsweise der aktuelle Standort, andere dienen der gezielten Beseitigung von Fehlfunktionen, wie etwa die Übermittlung der Seriennummer des Handys. Um die Zusammenarbeit unterschiedlicher Hersteller, Netzbetreiber und Dienstanbieter zu gewährleisten, werden viele Mechanismen und Protokolle über (nationale, europäische, internationale) Standards vereinbart. Einer dieser Standards ist GSM. Zum Standard gehören auch die zwischen unterschiedlichen Betreibern zu speichernden und zu verarbeitenden Daten. Um zu klären, welche Daten eines Kunden ein Netzbetreiber wie lange speichert, genügt jedoch der Blick in die Standards nicht.

Sobald die Verarbeitung von Daten allein die Sache eines Betreibers ist, kann er seine Entscheidungen weitgehend selbst treffen. Ansonsten gelten die gesetzlichen Regelungen. Welche Daten ein GSM-Abrechnungsdatensatz enthalten muß, regelt hingegen wiederum der Standard. Hierzu werden entsprechende Daten an Abrechnungszentralen übermittelt und nach Nutzern sortiert. Die Verbindungsdaten enthalten auch die Standortkennungen einer Verbindung, erlauben also Nutzer nachträglich zu lokalisieren.

Da die periodischen Mitteilungen über den aktuellen Aufenthaltsort ein hohes Verkehrsaufkommen im Netz verursachen können, ist zumindest technisch die Erstellung sogenannter Location Update Records vorgesehen. Diese enthalten neben der Rufnummer des Nutzers sowohl dessen alten und neuen Standort als auch die entsprechenden Zeitmarkierungen. Ein solcher Datensatz eignet sich ideal, um Nutzer zu überwachen.

Hat ein Nutzer einen Einzelentgeltnachweis gebucht, werden einige Daten der Ab-

rechnungszentralen an den Dienstanbieter und an den Nutzer weitergegeben. Ob die Standortkennungen an den Dienstanbieter weitergegeben werden, hängt im wesentlichen vom gebuchten Dienstprofil des Nutzers ab. Gewöhnlich werden sie jedoch nicht weitergegeben. An den Nutzer werden die Standortkennungen hingegen in keinem Fall weitergeleitet.

Ein Netz mit vorbezahlten Wertkarten zu benutzen, unterstützt der GSM-Standard nicht direkt, obgleich entsprechende Angebote der Netzbetreiber verfügbar sind. Diese arbeiten jedoch mit entsprechenden Schattenkonten auf Guthabenbasis, was die meist eingeschränkte internationale Nutzbarkeit, auf neudeutsch auch Roaming genannt, erklärt. Im GSM ist keine Online-Bonitätsprüfung vorgesehen!

Leider sind im GSM keinerlei Funktionen implementiert, die dem Nutzer garantieren, daß der Netzbetreiber nur das in Rechnung gestellt, was der Kunde auch tatsächlich genutzt hat. Im Streitfall ist er auf die Kulanz des Netzbetreibers angewiesen.

Bewegungsprofile und deren Verhinderung

Im allgemeinen kann man davon ausgehen, daß die Verbreitung der Mobilkommunikation zusätzlich zu den Fragen „wer hat wann was gesagt oder getan“ noch das „Wo?“ beantwortet. Obwohl die Lokalisierung von Nutzern etwa nach einem Unfall sogar lebensrettend sein kann, sollte es schon aus datenschutzrechtlichen Gründen nicht möglich sein im Normalbetrieb, detaillierte Bewegungsprofile zu erstellen. Nach geltendem Recht dürfen Bewegungsprofile nicht genutzt werden, wenngleich deren technische Erstellung möglich ist. Im engeren Sinn ist hier die Frage nach dem Vertrauen zu stellen: Der Nutzer soll selbst entscheiden können, wem er seine Daten anvertrauen will und wem nicht. Dieses Ziel wird durch datenschutzfreundliche Technologien erreicht.

Will sich ein Nutzer auch dagegen wehren, daß ein Netzbetreiber ein Bewegungsprofil aufzeichnet, versagen hingegen alle existierenden Mobilkommunikationsnetze. Da die Aufenthaltsorte der Nutzer gespeichert werden, kann der Netzbetreiber jederzeit darauf zugreifen und Bewegungsprofile ablesen.

Ein Netzbetreiber ist nicht in erster Linie daran interessiert, Daten über seine Nutzer zu sammeln, um diese anschließend mißbräuchlich zu verwenden. Im Gegenteil: Je weniger Daten er zur Diensterbringung benötigt, umso weniger Kosten fallen für deren Verarbeitung und vor allem auch für den Schutz vor dem Mißbrauch durch schwarze Schafe im eigenen Unternehmen und besonders durch externe Angreifer an.

Die in der Tabelle auf dieser Seite vorgestellten Konzepte haben das Ziel, Daten über Aufenthaltsorte beim Netzbetreiber möglichst zu vermeiden, ohne den Nutzer in seiner Mobilität einzuschränken. Im folgenden werden wir die wichtigsten Konzepte und deren Anwendung in der Mobilkommunikation erläutern. Hierzu zählen insbesondere:

- Pseudonyme als Erkennungszeichen von Nutzern anstelle von Identitäten (Rufnummern),
- ausforschungssichere, vertrauenswürdige Geräte zur Speicherung vertraulicher Daten,
- Methoden zum Schutz von Verkehrsdaten, zum Beispiel Mixe,
- spezielle Adressierungsverfahren, sogenannte implizite Adressen.

Diese Konzepte werden in den folgenden Verfahren beispielhaft erläutert. Die einzelnen Verfahren lassen sich im Überblick in [Fede_98] nachlesen. Einen allgemeinen, nicht nur auf Mobilkommunikation bezogenen Überblick finden Sie beispielsweise in [FePf_97].

Pseudonyme dienen als Verkettungsmerkmal zwischen Personen und ihren Handlungen. Der Nutzer von Pseudonymen kann sie dem gewünschten Grad der Anonymität anpassen (skalieren). Pseudonyme zum Schutz des Aufenthaltsortes sehen für alle Außenstehenden, auch für den Netzbetreiber, wie Zufallszahlen aus. Nur der Nutzer, der seinen Aufenthaltsort schützen will, kennt die Zuordnung zwischen seiner Identität und seinen Pseudonymen. Wir erläutern das am Beispiel temporärer Pseudonyme (TP) und gehen davon aus, daß der Nutzer eine vertrauenswürdige Umgebung im Festnetz besitzt. Diese Umgebung kann der Handy-Besitzer, etwa mit einer Chipkarte an einer speziellen ortsfesten Telefondose verwirklichen. Nun könnte er dort direkt seinen Aufenthaltsort speichern. Ist er jedoch weit entfernt von seinem Heimatort muß die aktuelle Standortkennung, im Extremfall jeder Wechsel einer Zelle, über weite Strecken des Festnetzes signalisiert werden. GSM-Netzbetreiber lösen das Problem, indem sie die netzseitige Datenbank teilen: Ein Teil der Datenbank befindet sich fest im Heimatbereich des Nutzers (Home Location Register), ein anderer Teil ist im gerade besuchten Bereich angelegt (Visitor Location Register). Da im GSM die Datenbank etwa unter der Rufnummer des Nutzers geführt wird, ist es möglich, Aufenthaltsorte zu protokollieren.

Die Idee der TP-Methode besteht nun darin, die wechselnden Aufenthaltsorte in den Datenbanken des Netzbetreibers nicht mehr unter der bekannten Rufnummer des Nutzers zu führen, sondern unter sich ständig wechselnden Pseudonymen P(t). Jeder Ortswechsel wird unter einem neuen Pseudonym registriert, und die alten Einträge verfallen nach einer gewissen Zeit automatisch. Da die Pseudonyme für niemanden, nicht einmal für den Netzbetreiber, miteinander verkettbar sind, lassen sich auch keine Bewegungsprofile erzeugen.

Bei einem eintreffenden Ruf muß die Verbindung zum aktuellen Aufenthaltsort des Nutzers durchgestellt werden. Hierzu fragt der Netzbetreiber die vertrauenswürdige Umgebung des Nutzers nach dessen aktuellem Pseudonym und vermittelt den Ruf ins Aufenthaltsgebiet, da er jetzt die passenden Datenbankeinträge zuordnen kann. Bei der TP-Methode muß nicht jeder Zellwechsel an die vertrauenswürdige Umgebung gemeldet werden. Es wird lediglich noch von Zeit zu Zeit, im Abstand von Minuten bis Stunden, die Synchronisation der Pseudonyme überprüft.

INFO

Wichtige Daten einer GSM-Abrechnung

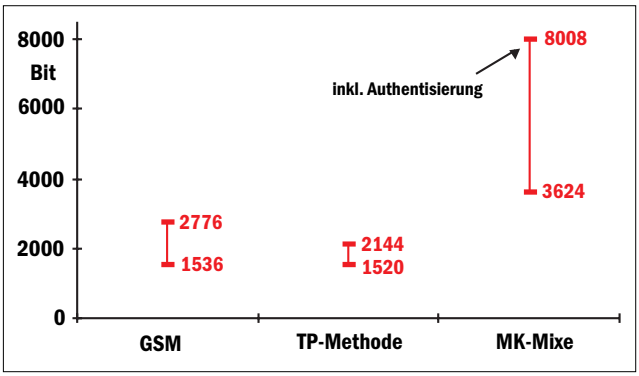
- **Rufnummer des rufenden Teilnehmers**
- **Rufnummer des gerufenen Teilnehmers,**
- **Standortkennung bestehend aus**
  - **Kennung der Vermittlungsstelle**
  - **Aufenthaltsgebiets- und Zellkennung**
  - **Funkkanalkennung**
- **Trunk-Group (die Verbindungsleitung, auf der die Vermittlungsstelle die Verbindung weiterschaltet)**
- **Seriennummer und Typ des benutzten mobilen Endgerätes**
- **Beginn, Ende, Dauer des Gesprächs**
- **Grund für die Beendigung des Gesprächs gibt an, ob normales Ende, Funkstörung, Erkennung eines gestohlenen Gerätes oder Ausfall einer Netzkomponente.**
- **Datenvolumen bei Datendiensten.**

Quelle: [MaMo_91]

Aus technischer Sicht macht vor allem die vertrauenswürdige Umgebung Probleme. Sie könnte die Verfügbarkeit beeinträchtigen. Ein Nutzer kann beispielsweise nicht erreicht werden, wenn sein vertrauenswürdiger Bereich technisch gestört ist oder auch ein Angreifer die Umgebung gezielt stört. Daher wäre es wünschenswert, den Schutz des Aufenthaltsorts auch ohne eine individuelle vertrauenswürdige Umgebung zu erreichen. Eine Lösung hierfür bieten die sogenannten Mobilkommunikations-Mixe. Anstelle der individuellen vertrauenswürdigen Umgebung werden spezielle Rechner, eben diese Mixe, in den Vermittlungsweg geschaltet. David Chaum führte Mixe erstmals 1981 ein. Ein Mix verbirgt den Zusammenhang zwischen eingehender und ausgehender Nachricht. Hierzu muß der Mix eingehende Nachrichten speichern, bis Nachrichten von genügend vielen Absendern vorhanden sind. Er verändert das Aussehen der Nachrichten, kodiert sie also um und ändert die Reihenfolge der ausgehenden Nachrichten. Die Kernfunktion der Mixe, das Umkodieren, basiert auf Public-Key-Kryptographie, beispielsweise auf dem bekannten RSA-Verfahren.

Um Angriffe durch Nachrichtenwiederholung zu verhindern, muß der Mix zu Beginn noch prüfen, ob eine eingehende Nachricht bereits gemixt wurde. Damit keine Verkettung zwischen eingehenden und ausgehenden Nachrichten an Hand der Länge der Datenpakete möglich ist, sollten alle eingehenden ebenso wie die ausgehenden Nachrichten die gleiche Länge haben.

Mixe müssen unabhängig vom Netzbetreiber implementiert, installiert und betrieben werden. In der Regel schaltet man mehrere Mixe hintereinander. So muß ein Angreifer entweder alle Mixe beherrschen, indem er jeden einzelnen knackt oder „überbrückt“, oder er muß alle Nachrichten selbst einspeisen, um eine bestimmte Kommunikationsbeziehung zu enttarnen.



Nachrichtenlängen und -intervalle der vorgestellten Verfahren beim Verbindungsaufbau

Kosten der Anonymität

Alle angedeuteten Methoden zum Schutz des Aufenthaltsorts nützen nichts, wenn beim Paging, also beim Rufen des Nutzers in den Funkzellen des Aufenthaltsgebietes wieder die Identität übermittelt wird. Die Identität ergibt sich beispielsweise aus der Rufnummer. Im GSM wird ein begrenzt gültiges Kennzeichen, die Temporary Mobile Subscriber Identity (TMSI), übermittelt. Sie soll die Lokalisierung durch das Abfangen der Funksignale verhindern. Will sich der Nutzer auch gegen die Lokalisierung durch den Netzbetreiber schützen, muß anstelle der TMSI eine sogenannte implizite Adresse verwendet werden. Implizite Adressen ermöglichen es dem Nutzer und nur ihm, die für ihn bestimmten Nachrichten, etwa Verbindungswünsche, zu erkennen. Implizite Adressen werden ebenfalls über kryptographische Verfahren gebildet.

Um es gleich vorweg zu nehmen: keines der vorgestellten Verfahren können Sie bisher kaufen oder einsetzen. Trotzdem stellt sich die Frage nach Aufwand und Nutzen, da sich der Mobilfunk weiter entwickeln wird. Die nächste Mobilfunk-Generation ist beispielsweise das Universal Mobile Telecommunication System (UMTS). Die Funkstrecke besitzt als Flaschenhals der Netze eine besondere Bedeutung für den Vergleich der Verfahren. Bei der TP-Methode macht sich der zusätzliche Aufwand für den Schutz praktisch nicht bemerkbar, verursacht jedoch im Vorfeld einen hohen Aufwand, da sich jeder Nutzer eine „vertrauenswürdige Box“ anschaffen muß, die er beispielsweise an seinen festen Telefonanschluß installiert. Hinzu kommen dann bei jedem Verbindungsaufbau die Kosten der Telefonverbindung zu dieser Box. Bei den Mobilkommunikationsmixen erkauft man sich die Einsparung der Box durch einen höheren Übertragungsaufwand von und zum Handy. Der höhere Aufwand hat seine Ursachen in den angewendeten Verschlüsselungsverfahren. Die starke Aufblähung der Nachrichten mag im ersten Moment schwerwiegend erscheinen, relativiert sich jedoch, wenn man bedenkt, daß in UMTS jene Public-Key-Kryptoverfahren standardmäßig eingesetzt werden sollen, die auch bei den Mobilkommunikationsmixen verwendet werden.

Was bringt UMTS?

Das Universal Mobile Telecommunication System soll die existierenden Mobilfunknetze und -standards (GSM, DECT, Pagerdienste) als übergeordneter Standard vereinen. Neue Dien-

HINTERGRUND

Konzepte um Bewegungsprofile zu vermeiden

- **1. Broadcast-Methode**
  Verzicht auf Speichern von Aufenthaltsorten und Verteilung (Paging) von Verbindungswünschen im gesamten Versorgungsbereich des Netzes.
- **2. Methode der Gruppenpseudonyme**
  Viele Nutzer werden in einer gemeinsamen Anonymitätsgruppe (unter einem gemeinsamen Gruppenpseudonym) zusammengefaßt. Der Aufenthaltsort eines einzelnen Nutzers ist in der Gruppe anonym.
- **3. Explizite vertrauenswürdige Speicherung**
  Speichern von Aufenthaltsorten in einer vertrauenswürdigen Umgebung (beispielsweise eine am festen Telefon des Nutzers angeschlossene Box) oder bei einem vertrauenswürdigen Dritten (Trust Center).
- **4. Temporäre Pseudonyme (TP-Methode)**
  Pseudonyme Speicherung von Aufenthaltsorten im Netz und Verkettung des Pseudonyms über eine vertrauenswürdige Umgebung. Dieses Verfahren basiert auf der expliziten vertrauenswürdigen Speicherung (siehe 3.), ist jedoch effizienter.
- **5. Methode der kooperierenden Chips**
  Speichern der Aufenthaltsorte in ausforschungssicherer Hardware, z.B. einer Chipkarte, die das Gegenstück zur Chipkarte im Handy ist.
- **6. Mobilkommunikationsmixe**
  Geschütztes Speichern von Aufenthaltsorten im Netz mit Hilfe von Kryptographie. Dieses Verfahren verhindert außerdem die Überwachung von Gesprächen.

Quelle: [Fede_98]

INFO

Literatur

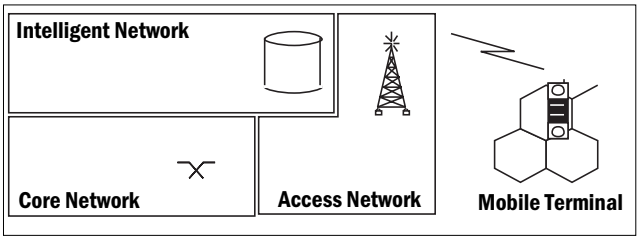
Fede_98
Hannes Federrath: Vertrauenswürdiges Mobilitätsmanagement in Telekommunikationsnetzen. Dissertation, TU Dresden, Fakultät Informatik, Februar 1998.

FePf_97
Hannes Federrath, Andreas Pfitzmann: Bausteine zur Realisierung mehrseitiger Sicherheit. Günter Müller, Andreas Pfitzmann (Herausgeber): Mehrseitige Sicherheit in der Kommunikationstechnik, Addison-Wesley-Longman 1997, 83-104.

MaMo_91
Mannesmann Mobilfunk: Anrufdatensätze. Ergänzung zur Dokumentation des ITG-Forums „Gestaltungsfelder beim Mobiltelefon“, 12. Mai 1992, Frankfurt am Main.

ste mit höherer Datenrate, besserer Sprachqualität und sogar Multimediafähigkeit sollen folgen. Es stellt sich die Frage, ob die beschriebenen Verfahren in UMTS umgesetzt werden können.

UMTS ist schon von seiner modularen Grundstruktur her geeignet, derartige Konzepte zu unterstützen. Für UMTS ist eine Dreiteilung in die Komponenten Access Network, Intelligent Network und Core (oder Fixed) Network vorgesehen. Das Konzept des Intelligenten Netzes soll die schnelle und flexible Implementierung von Diensten ermöglichen. Die Mobi-



Das Architekturkonzept des zukünftigen Telekommunikations-Standards UMTS

litätsfunktionen, etwa die Registrierung des Aufenthaltsorts, sollen auch dort realisiert werden. Das Core Network soll durch Breitband-ISDN (B-ISDN) realisiert werden. Die Schnittstelle zum mobilen Nutzer bildet ein spezielles Zugriffsnetz, das direkt an das B-ISDN ankoppelt. Damit ist UMTS nicht mehr das mobile Netz, sondern ein „Netz von Netzen“.

Um die Vielfältigkeit der angebotenen Dienste und Übertragungstechniken überhaupt effizient nutzen zu können, ist die Entwicklung eines multifunktionalen persönlichen Kommunikationsendgeräts (Personal Communicator), das alle mobilen Möglichkeiten in sich vereint, nötig. Außerdem wird es sicher in Zukunft an vielen öffentlichen Stellen multifunktionale Endgeräte und Kommunikationsdosen geben, über die die Dienste genutzt werden können.

Leider wurden bei der Standardisierung von UMTS keine starken Schutzmaßnahmen gegen Bewegungsprofile vorgesehen. Teilweise wird die Situation gegenüber dem GSM durch sogenannte fortgeschrittene Location Management Prozeduren zugunsten einer höheren Effizienz sogar noch verschärft. Solange an UMTS jedoch noch standardisiert wird, existieren Möglichkeiten zur konsequenten Definition von entsprechenden Schutzfunktionen. Der nachträgliche Einbau von Sicherheit muß sonst durch unnötige Kompromisse und mehr Geld bezahlt werden. *(TZ)*

Hannes Federrath arbeitet an der Fakultät für Informatik der TU Dresden, und hat dort gerade seine Dissertation abgeschlossen. E-Mail: federrath@inf.tu-dresden.de