Langfassung eines in Funkschau 71/12 (1998) 60-63 erschienenen Artikels

Mobilkommunikation ohne Spuren

Hannes Federrath

TU Dresden, Fakultät Informatik, 01062 Dresden
E-Mail: federrath@inf.tu-dresden.de
Telefon: (0351) 463-8470, Fax: -8255

Einführung

Mobilkommunikation hat in den letzten Jahren einige Furore gemacht: Fast flächendeckende Versorgung in Deutschland bzw. Europa, immer preisgünstigere Angebote und weltweite Nutzbarkeit sprechen für sich. Mobile Sprachkommunikation ist ein Massenprodukt geworden. Der bekannteste und verbreitetste Mobilkommunikationsstandard ist das GSM (Global System for Mobile Communication), ursprünglich eine europäische Entwicklung, die auch weltweite Verbreitung gefunden hat. Leider hat das Sicherheitsniveau mit der Verbreitung der Mobilkommunikation nicht mitgehalten.

Von den Telefongesellschaften werden an Sicherheitsfunktionen vor allem die Abhörsicherheit und die Sicherheit gegen illegale, unberechtigte Nutzung hervorgehoben. Dabei wird häufig (wenn nicht fast immer) verschwiegen, daß sich die Abhörsicherheit nur auf die Funkübertragung beschränkt und bei Streitfällen zwischen Nutzer und Telefongesellschaft eher die Kulanz der Telefongesellschaft über die Zufriedenheit der Nutzer entscheidet, wenn etwas schief gegangen ist. Die existierenden Mobilkommunikationsnetze sind keinesfalls sicherer als die festen Telefonnetze. Sie sind lediglich sicher gegen einige neue Mißbrauchsmöglichkeiten, die durch die Mobilität entstehen.

Welche Spuren hinterläßt der Mobilfunkkunde?

Worauf in den Werbeblättern der Anbieter nicht oder nur sehr unzureichend hingewiesen wird, sind die Spuren, die ein Nutzer hinterläßt.

1. Sobald das Handy eingeschaltet wird, meldet es sich beim Netzbetreiber an. Hierzu werden Daten zur Identität des Nutzers, die Seriennummer des Handys und Daten zum aktuellen Standort übermittelt.
2. Völlig unabhängig davon, ob der Nutzer telefoniert oder nicht, werden von Zeit zu Zeit die Daten über den Standort erneuert. Beim Verlassen des aktuellen Aufenthaltsgebietes ist dies nötig, um eingehende Rufe zum Handy noch zustellen zu können.
3. Jeder Verbindungsversuch zu einem Handy wird protokolliert und beim Netzbetreiber gespeichert, unabhängig davon, ob die Verbindung zustande kam oder nicht.
4. Die vorhandenen Sicherheitsfunktionen (Verschlüsselung, Authentisierung, Berechtigungsprüfung) können durch gezielte Angriffe ausgehebelt werden (siehe Kasten 1 zum IMSI-Catcher).

Einige der angesprochenen Daten werden für die Funktion des Netzes benötigt, hierzu zählt beispielsweise der aktuelle Standort, andere dienen der gezielten Beseitigung von Fehlfunktionen, 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. Dies gilt auch für die zwischen unterschiedlichen Betreibern zu speichernden und zu verarbeitenden Daten.

Kasten 1. Sicherheit des GSM gezielt aushebeln: IMSI-Catcher

Der Name des IMSI-Catchers bezieht sich auf die Abkürzung für die netzinterne Rufnummer International Mobile Subscriber Identity, kurz IMSI. Durch die gezielte Ausnutzung von „Schwächen" in den Sicherungsprotokollen des GSM ist es möglich, die netzinternen Rufnummern aller Nutzer einer Funkzelle zu ermitteln. Doch damit nicht genug: Der IMSI-Catcher soll sogar in der Lage sein, dem Handy des Nutzers zu signalisieren, daß es keine Verschlüsselung mehr auf der Funkstrecke, d.h. zwischen Handy und Basisstationen (Funkmasten) verwenden soll.

Die Funktionsweise des IMSI-Catchers ist denkbar einfach. Gegenüber dem Handy des Nutzers verhält es sich wie eine Basisstation, gegenüber der „echten" Basisstation des Netzbetreibers wie ein Handy.

Das Aushebeln der Sicherheitsfunktionen des GSM hätte man leicht verhindern können, indem anstelle einer einseitigen Authentikation Mechanismen zur gegenseitigen Authentikation (sowohl Nutzer vor Netz als auch Netz vor Nutzer) vorgesehen worden wären. Im GSM „beweist" nur der Nutzer vor dem Netzbetreiber, daß er „echt" bzw. berechtigt ist. Der technische Aufwand für die gegenseitige Authentikation wäre nur geringfügig höher gewesen.

Fragt man nun konkret, welche Daten ein Netzbetreiber wie lange über einen Kunden speichert, genügt der Blick in Standards allein nicht.

Abrechnung

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 wiederum der Standard (siehe Kasten 2). Hierzu werden entsprechende Daten an Abrechnungszentralen übermittelt und nach Nutzern sortiert. Die Verbindungsdaten enthalten auch die Standortkennungen einer Verbindung, erlauben also die nachträgliche Lokalisierung von Nutzern. Da auch die periodischen Mitteilungen über den aktuellen Aufenthaltsort einen hohen Anteil am Verkehrsaufkommen im Netz haben können, ist zumindest technisch die Erstellung sogenannter Location Update Records vorgesehen. Er enthält neben der Rufnummer des Nutzers dessen alten und neuen Standort zusammen mit den entsprechenden Zeitmarkierungen. Ein solcher Datensatz eignet sich ideal zur Überwachung der Nutzer.

Hat ein Nutzer einen Einzelentgeltnachweis gebucht, werden einige Daten der Abrechnungszentralen an den Dienstanbieter (soweit vorhanden) 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. Das weitergeben der Standortkennungen an den Nutzer ist nicht vorgesehen.

Kasten 2. Daten eines GSM-Abrechnungsdatensatzes (Auswahl)

- 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]

Die Netzbenutzung mit vorbezahlten Wertkarten wird vom GSM nicht direkt unterstützt, 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, da im GSM keine Online-Bonitätsprüfung vorgesehen ist.
Leider sind im GSM keinerlei Funktionen implementiert, die dem Nutzer garantieren, daß die Rechnungsstellung korrekt verlaufen ist, also nur das in Rechnung gestellt wurde, was tatsächlich genutzt wurde. In Streitfällen ist der Nutzer hier auf die Kulanz des Netzbetreibers angewiesen.

Bewegungsprofile und deren Verhinderung

Im Allgemeinen kann man davon ausgehen, daß die Beobachtbarkeit von Nutzern, d.h. *wer* hat *wann was* gesagt oder getan durch die Verbreitung der Mobilkommunikation noch das „*Wo*?“ hinzu bekommt. Obwohl die Lokalisierung von Nutzern im Einzelfall durchaus hilfreich oder sogar lebensrettend sein kann, z.B. nach einem Unfall, sollte im Normalbetrieb die Erstellung von Bewegungsprofilen schon aus datenschutzrechtlichen Gründen verhindert werden. Nach geltendem Recht dürfen Bewegungsprofile nicht erstellt 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 man sich als Nutzer auch gegen Verfolgung durch den Netzbetreiber schützen, versagen alle existierenden Mobilkommunikationsnetze. Da die Aufenthaltsorte der Nutzer

gespeichert werden, kann der Netzbetreiber jederzeit darauf zugreifen und Bewegungsprofile erstellen. Ein Netzbetreiber ist normalerweise nicht primär 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 für den Schutz vor Mißbrauch durch schwarze Schafe im eigenen Unternehmen und externe Angreifer an.

Tabelle 1. Konzepte zur Verhinderung von Bewegungsprofilen (Auswahl)

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 Nutzer ist in der Gruppe anonym.

3. Explizite vertrauenswürdige Speicherung
Speichern von Aufenthaltsorten in einer dem Nutzer vertrauenswürdigen Umgebung (z.B. einer am festen Telefon des Nutzers angeschlossenen Box oder einer Chipkarte in einer speziellen Telefonsteckdose) 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
Speichernder 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]

Die in Tabelle 1 vorgestellten Konzepte haben das Ziel, Daten über Aufenthaltsorte beim Netzbetreiber möglichst zu vermeiden, ohne den Nutzer in seiner Mobilität einzuschränken. Im folgenden sollen nicht alle Verfahren erklärt werden. Stattdessen werden die wichtigsten Konzepte und deren Anwendung in der Mobilkommunikation erläutert. Hierzu zählen insbesondere:

- Pseudonyme als Erkennungszeichen von Nutzern anstelle von Identitäten (Rufnummern),
- ausforschungssichere, vertrauenswürdige Geräte zur Speicherung von vertraulichen Daten,
- Methoden zum Schutz von Verkehrsdaten, z.B. Mixe,

- spezielle Adressierungsverfahren, sogenannte implizite Adressen.

Diese Konzepte werden in den folgenden Verfahren beispielhaft erläutert. Die einzelnen Verfahren aus Tabelle 1 lassen sich in [FeJP_96, Hets_93, KeFo_95, KFJP_96, Pfit_93] oder im Überblick in [Fede_98] nachlesen. Einen allgemeinen (d.h. nicht mobilkommunikationsspezifischen) Überblick über die Verfahren zu datenschutzfreundlichen Technologien gibt z.B. [FePf_97].

Verwaltung von Aufenthaltsorten

Pseudonyme dienen als Verkettungsmerkmal zwischen Personen und ihren Handlungen. Sie sind nach dem gewünschten Grad der Anonymität eines Nutzers anpaßbar (skalierbar). 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 den Pseudonymen. Am Beispiel der TP-Methode (Temporäre Pseudonyme) soll das erläutert werden.

Zunächst wird angenommen, daß ein Nutzer, der sich schützen will, eine vertrauenswürdige Umgebung (Tabelle 1, Punkt 3) im Festnetz besitzt. Nun könnte er dort direkt seinen Aufenthaltsort ablegen. Ist er jedoch weit entfernt von seinem Heimatort, z.B. auf einem anderen Kontinent, muß die aktuelle Standortkennung, im Extremfall jeder Zellwechsel, über weite Strecken des Festnetzes signalisiert werden. Dies verursacht natürlich hohe Kosten. Im GSM wurde deshalb die netzseitige Datenbank geteilt (siehe Bild 1a). Ein Teil der Datenbank befindet sich fest im Heimatbereich des Nutzers (Home Location Register), ein weiterer wird im jeweils gerade besuchten Bereich angelegt (Visitor Location Register). Da im GSM die Datenbank unter der Identität (ID, konkret der Rufnummer) des Nutzers geführt wird, sind Bewegungsprofile erstellbar.

Die Idee der TP-Methode (Bild 1b) 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 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 (d.h. im Abstand von Minuten bis Stunden) die Synchronisation der Pseudonyme überprüft.

Aus technischer Sicht macht vor allem die vertrauenswürdige Umgebung Probleme. Sie könnte die Verfügbarkeit beeinträchtigen, da der Nutzer nicht erreicht werden kann, wenn sein vertrauenswürdiger Bereich technisch gestört ist bzw. durch einen Angreifer gezielt gestört wird. Daher wäre es wünschenswert, den Schutz des Aufenthaltsorts auch ohne eine individuelle vertrauenswürdige Umgebung zu erreichen. Eine Lösung hierfür bieten die Mobilkommunikationsmixe (Bild 1c). Anstelle der nutzerindividuellen vertrauenswürdi-

gen Umgebung werden jetzt spezielle Rechner, sog. Mixe, in den Vermittlungsweg geschaltet. Mixe wurden erstmals 1981 von David Chaum vorgestellt.
Ein Mix [Chau_81] verbirgt die Verkettung zwischen eingehenden und ausgehenden Nachrichten. Hierzu muß ein Mix eingehende Nachrichten speichern, bis genügend viele Nachrichten von genügend vielen Absendern vorhanden sind, ihr Aussehen verändern, d.h. sie umkodieren und die Reihenfolge der ausgehenden Nachrichten verändern, d.h. sie umsortieren. Die Kernfunktion der Mixe, das Umkodieren, basiert auf Public-Key-Kryptographie, z.B. auf dem bekannten RSA-Verfahren.

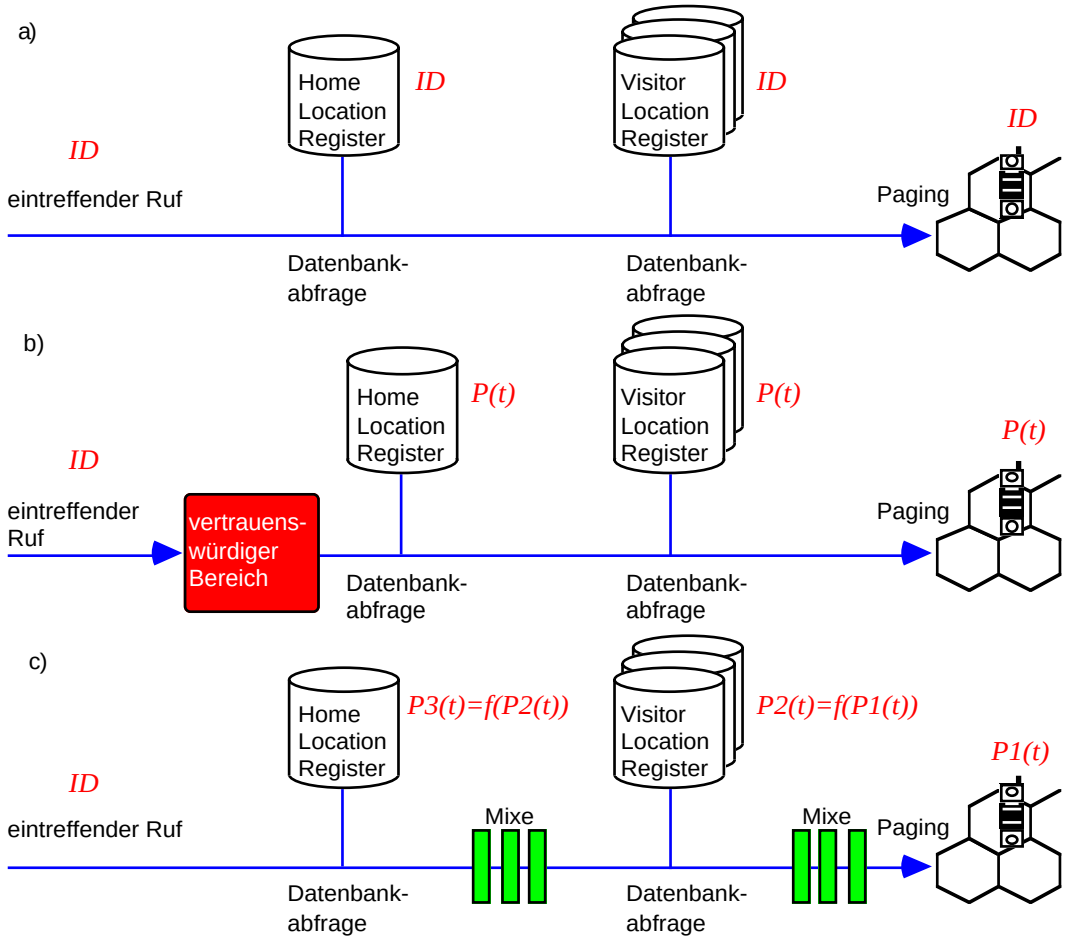

Bild 1. Verbindungsaufbau
a) bei GSM
b) bei der TP-Methode
c) bei den Mobilkommunikationsmixen

Um Angriffe durch Nachrichtenwiederholung zu verhindern, muß zu Beginn noch geprüft werden, ob eine eingehende Nachricht bereits gemixt wurde. Damit keine Verkettung zwischen eingehenden und ausgehenden Nachrichten über deren Länge möglich ist, sollten alle eingehenden Nachrichten die gleiche Länge haben, ebenso die ausgehenden.
Mixe müssen unabhängig vom Netzbetreiber implementiert, installiert und betrieben werden. In der Regel schaltet man mehrere Mixe hintereinander. So muß ein Angreifer ent-

weder alle Mixe beherrschen (knacken oder „überbrücken“) oder er muß alle Nachrichten selbst eingespeist haben, um eine bestimmte Kommunikationsbeziehung zu enttarnen.

Implizite Adressierung zum Schutz des Empfängers

Alle angedeuteten Methoden zum Schutz des Aufenthaltsorts nützen nichts, wenn beim Paging, d.h. bei Rufen des Nutzers in den Funkzellen des Aufenthaltsgebietes wieder die Identität (Rufnummer oder anderes Personenkennzeichen) übermittelt wird. 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 sog. implizite Adresse verwendet werden. Implizite Adressen ermöglichen es dem Nutzer und nur ihm, die für ihn bestimmten Nachrichten (z.B. Verbindungswünsche) zu erkennen. Implizite Adressen werden ebenfalls über kryptographische Verfahren gebildet.

Was „kostet“ die zusätzliche Sicherheit?

Um es gleich vorweg zu nehmen: keines der vorgestellten Verfahren zum Schutz vor Verfolgung kann man bisher kaufen. Trotzdem stellt sich die Frage nach Aufwand und Nutzen, da die Entwicklung im Mobilfunkbereich weitergehen wird. Eine Entwicklung in die nächste Generation ist beispielsweise das Universal Mobile Telecommunication System (UMTS).

Die Funkstrecke als größter Engpaß der Netze besitzt eine besondere Bedeutung für den Vergleich der Verfahren. Im Bild 2 sind die typischen Nachrichtenlängen für GSM, die TP-Methode und die Mobilkommunikationsmixe (MK-Mixe) für den Verbindungsaufbau angegeben.

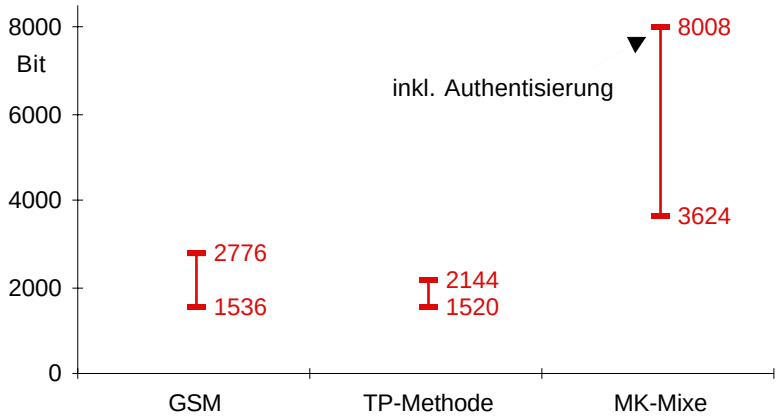

Bild 2. Nachrichtenlängen bzw. -intervalle beim Verbindungsaufbau

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 beispielsweise an seinen festen Telefonanschluß installiert wird. Hinzu kommen dann bei jedem Verbindungsaufbau die Telefon-

kosten zu dieser Box. Bei den Mobilkommunikationsmixen erkauft man sich die Einsparung der Box durch einen höheren Übertragungsaufwand von und zum Handy. Dieser hat seine Ursachen in den angewendeten Verschlüsselungsverfahren. Die starke Expansion 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 die Zukunft? — UMTS

Das Universal Mobile Telecommunication System soll die existierenden Mobilfunknetze und -standards (GSM, DECT, Pagerdienste) unter sich vereinen und auf eine gemeinsame Plattform stellen. Neue Dienste mit höherer Datenrate, besserer Sprachqualität und sogar Multimediafähigkeit sollen folgen. Es stellt sich natürlich die Frage, ob in UMTS noch Optionen zum Einbau der beschriebenen Verfahren existieren.
UMTS ist schon von seiner modularen Grundstruktur her geeignet, derartige Konzepte zu unterstützen. Als architekturelle Basis für UMTS gilt nach [Mitt_94] eine Dreiteilung in die Komponenten Access Network, Intelligent Network und Core (oder Fixed) Network.

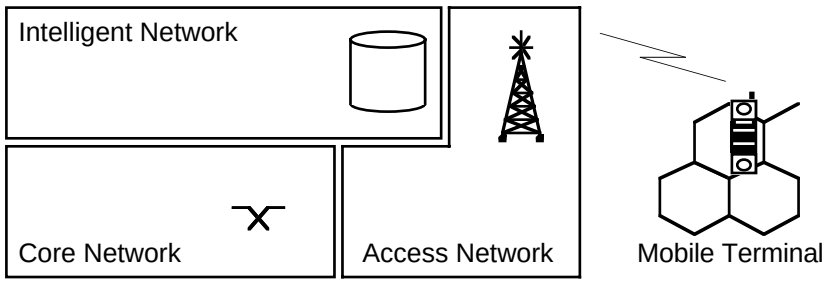

Bild 3. Das Architekturkonzept von UMTS

Durch das Konzept des Intelligenten Netzes soll die schnelle und flexible Implementierung von Diensten erreicht werden. Die Mobilitätsfunktionen (z.B. Aufenthaltsortsregistrierung) 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 Kommunikationsendgerätes (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 sog. fortgeschrittene Location Management Prozeduren zugunsten einer höhere Effizienz sogar noch verschärft. Solange an UMTS jedoch noch standardisiert wird, existieren Möglichkeiten zur konsequenten Definition von entsprechenden Schutzfunktionen.

Der nachträgliche Einbau von Sicherheit kostet sonst nur unnötige Kompromisse und mehr Geld.

Literatur

Chau_81 David Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM 24/2 (1981) 84-88.

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

FeJP_96 Hannes Federrath, Anja Jerichow, Andreas Pfitzmann: Mixes in mobile communication systems: Location management with privacy. in: R. Anderson (Hrsg.): Information Hiding, LNCS 1174, Springer-Verlag, Berlin 1996, 121-135.

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

Hets_93 Thomas Hetschold: Aufbewahrbarkeit von Erreichbarkeits- und Schlüsselinformation im Gewahrsam des Endbenutzers unter Erhaltung der GSM-Funktionalität eines Funknetzes. GMD-Studien no. 222, Oktober 1993.

KeFo_95 Dogan Kesdogan, Xavier Fouletier: Secure Location Information Management in Cellular Radio Systems. IEEE Wireless Communication System Symposium 95, Proceedings, Long Island (1995), 35-46.

KFJP_96 Dogan Kesdogan, Hannes Federrath, Anja Jerichow, Andreas Pfitzmann: Location managment strategies increasing privacy in mobile communication. in: Sokratis K. Katsikas, Dimitris Gritzalis (Hrsg.): Informations Systems Security, IFIP SEC '96 Conference Committees, Chapman & Hall, London, 1996, 39-48.

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

Mitt_94 Hakan Mitts: Universal Mobile Telecommunication Systems - Mobile access to Broadband ISDN. in: W. Bauerfeld, O. Spaniol, F. Williams (Hrsg.): Broadland Islands ´94, Connecting with the End-User, 1994, 203-209.

Pfit_93 Andreas Pfitzmann: Technischer Datenschutz in öffentlichen Funknetzen. Datenschutz und Datensicherung DuD 17/8 (1993) 451-463.