Bundesamt für Sicherheit in der Informationstechnik

GSM-Mobilfunk

Gefährdungen und Sicherheitsmaßnahmen

Diese BSI-Broschüre gibt einen Einblick in die Funktionsweise von Mobilfunksystemen nach dem GSM-Standard. Sie beschreibt mögliche Gefährdungen der Abhörsicherheit bei der Nutzung von GSM-Mobilfunkdiensten und zeigt geeignete Schutzmaßnahmen auf.

Bundesamt für Sicherheit in der Informationstechnik

Referat III 1.1 Mobilfunksicherheit

Postfach 20 03 63

53133 Bonn

Tel.: +49 (0) 1888-9582-0

E-Mail: mobilfunksicherheit@bsi.bund.de

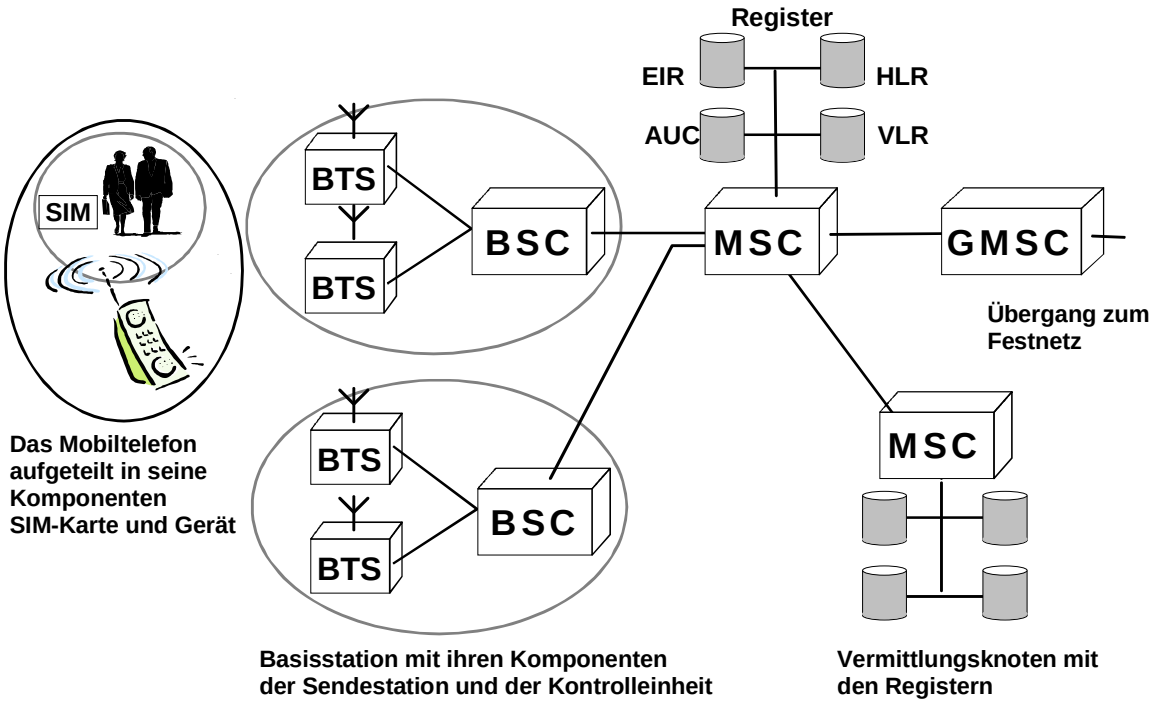
Internet: http://www.bsi.bund.de

Inhaltsverzeichnis

1 Grundlagen der GSM-Mobilfunktechnik

Das **GSM** (**G**lobal **S**ystem for **M**obile Communication) gehört zur Klasse der zellularen Mobilfunknetze mit Betriebsfrequenzen von rund 900 MHz und 1800 MHz. Das GSM-Netz ist entsprechend der unten angegebenen Darstellung hierarchisch gegliedert.

1.1 Technische Komponenten des Mobilfunks



1.1.1 Mobiltelefon

Ein GSM-Mobiltelefon besteht aus zwei Komponenten: dem Mobilfunkgerät selbst und dem **SIM** (**S**ubscriber **I**dentity **M**odule). Damit wird im GSM-Netz zwischen Nutzer und Gerät unterschieden.

Das Mobilfunkgerät ist gekennzeichnet durch seine international eindeutige Seriennummer (**IMEI** – **I**nternational **M**obile **E**quipment **I**dentity). Der Nutzer wird durch seine auf der SIM-Karte gespeicherte Kundennummer (**IMSI** – **I**nternational **M**obile **S**ubscriber **I**dentity) identifiziert. Sie wird dem Teilnehmer bei seiner Anmeldung vom Netzbetreiber zugeteilt und ist von den ihm zugewiesenen Telefonnummern (**MSISDN** – **M**obile **S**tation **ISDN N**umber) zu unterscheiden. Durch diese Trennung ist es möglich, dass ein Teilnehmer mit seiner SIM-Karte verschiedene Mobilfunkgeräte nutzen kann.

Auf der SIM-Karte wird auch die teilnehmerbezogene Rufnummer gespeichert. Ebenso sind die kryptographischen Algorithmen für die Authentisierung und Nutzdatenverschlüsselung implementiert. Darüber hinaus können Kurznachrichten, Gebühreninformationen und ein persönliches Telefonregister gespeichert werden.

1.1.2 Basisstation

Eine GSM-Basisstation (**BTS** – **B**ase **T**ransceiving **S**tation) ist der Standort des Sende- und Empfangsequipments einer oder mehrerer Zellen. Sie stellt die Schnittstelle zwischen dem Netzbetreiber und dem Mobiltelefon dar. Die Kontrollstation (**BSC** – **B**ase **S**tation **C**ontroller)

verwaltet die Sende- und Empfangsressourcen der angeschlossenen Basisstationen. Hier werden zum Beispiel die Kanäle für die Signalisierung und den Nutzverkehr bereit gestellt und der Datenverkehr zwischen BTS und MSC kontrolliert.

1.1.3 Vermittlungsknoten

Die Basisstation wird über den Vermittlungsknoten (**MSC** – **M**obile **S**witching **C**enter) gesteuert. Dieser Vermittlungsknoten übernimmt alle technischen Funktionen eines Festnetz-Vermittlungsknotens, wie zum Beispiel Wegsuche, Signalwegschaltung und Dienstmerkmalsbearbeitung. Falls Verbindungswünsche zu einem Teilnehmer im Festnetz bestehen, werden sie vom Vermittlungsknoten über einen Koppelpfad ins Festnetz weitergeleitet.

Damit der Netzbetreiber in der Lage ist, auch alle gewünschten Dienste zu erbringen, muss er verschiedene Daten speichern. Er muss beispielsweise wissen, welche Teilnehmer sein Netz nutzen und welche Dienste sie in Anspruch nehmen wollen. Diese Daten, wie Teilnehmer, Kundennummer und beanspruchte Dienste, werden im Heimatregister (**HLR** – **H**ome **L**ocation **R**egister) abgelegt. Soll eine Verbindung, zum Beispiel von einem Festnetzanschluss zu einem Mobiltelefon, hergestellt werden, muss der Netzbetreiber wissen, wo sich der Teilnehmer befindet und ob er sein Mobiltelefon eingeschaltet hat. Diese Informationen werden im Besucher- (**VLR** – **V**isitor **L**ocation **R**egister) und im Heimatregister abgelegt.

Um zu prüfen, ob ein Teilnehmer überhaupt berechtigt ist, das Mobilfunknetz zu nutzen (also einen Kartenvertrag besitzt), gibt es beim Netzbetreiber eine Authentisierungszentrale (**AUC** – **Au**thentication **C**enter). Hier sind Algorithmen und teilnehmerbezogene Schlüssel gespeichert, die unter anderem bei einer Authentisierung benötigt werden.

Außerdem kann der Netzbetreiber ein Geräteregister, das **EIR** (**E**quipment **I**dentity **R**egister), führen. Hier sind alle im Netz zugelassenen Mobilfunkgeräte registriert und in drei Gruppen aufgeteilt, den so genannten weißen, grauen und schwarzen Listen. In der weißen Liste sind alle unbedenklichen Geräte registriert, die graue Liste enthält alle Geräte, die möglicherweise fehlerhaft sind und in der schwarzen Liste stehen all jene, die defekt oder als gestohlen gemeldet sind. Allerdings führen nicht alle Netzbetreiber ein Geräteregister.

1.1.4 Festnetz

Als Festnetz wird das öffentliche Telefonnetz mit seinen Verbindungswegen bezeichnet. Da bei jeder Mobilfunkverbindung auch Festnetze benutzt werden, sind die Gefährdungen bei der Nutzung von Festnetzen auch bei der Nutzung von Mobilfunknetzen vorhanden.

1.2 Verbindungsaufbau

Sobald der Besitzer sein Mobiltelefon einschaltet, meldet es sich über die nächstgelegene Basisstation beim Netzbetreiber an. Bei diesem werden Daten zur Identität des Nutzers, die Seriennummer des Mobiltelefons und die Kennung der Basisstation, über die die Anmeldung erfolgt ist, protokolliert und gespeichert. Dies erfolgt auch dann, wenn kein Gespräch geführt wird. Weiterhin wird jeder Verbindungsversuch, unabhängig vom Zustandekommen der Verbindung, gespeichert.

1.3 Sicherheitsmechanismen

Der Zugang zur SIM-Karte kann durch eine vier- bis achtstellige **PIN** (**P**ersonal **I**dentification **N**umber) gegen unberechtigten Zugriff geschützt werden. Mit Eingabe dieser PIN identifiziert sich der Teilnehmer nach dem Einschalten des Mobiltelefons gegenüber der Karte. Gelangt ein Unbefugter in den Besitz einer SIM-Karte, sollte es ihm ohne Kenntnis der PIN nicht möglich sein, diese Karte zu aktivieren. Um eine missbräuchliche Nutzung der SIM-Karte zu verhindern, sollte die PIN daher sicher aufbewahrt werden.

Mit der SIM-Karte und den darauf befindlichen kryptographischen Algorithmen identifiziert sich der Teilnehmer beim Einbuchen gegenüber dem Netzbetreiber. Die Authentisierung erfolgt mit Hilfe eines Authentisierungsschlüssels, der nur dem Netzbetreiber im AUC und dem Teilnehmer auf der SIM-Karte bekannt ist.

Die Daten werden in der Regel nur auf der Funkstrecke zwischen dem Mobiltelefon und der Basisstation verschlüsselt übertragen. Auf allen anderen Übertragungswegen sowohl im GSM-Netz als auch im Festnetzbereich wird nicht verschlüsselt. Aus betrieblichen Gründen besteht sogar auch auf der Funkstrecke die Möglichkeit, dass das Schlüsselverfahren nicht eingeleitet wird und dann unverschlüsselt übertragen wird. Abhängig von gesetzlichen Regelungen kann in einigen Ländern die Übertragungsverschlüsselung auch ganz abgeschaltet oder einzelne Sicherheitsparameter können schwächer sein.

1.4 Datenarten

Die bei der Telekommunikation verarbeiteten Daten lassen sich in drei Gruppen unterscheiden (vgl. [**BfD**]):

- **Bestandsdaten** (oder auch Stammdaten) sind diejenigen Daten, die in einem Dienst oder Netz dauerhaft gespeichert und bereit gehalten werden. Hierzu gehören die Rufnummer und gegebenenfalls der Name und die Anschrift des Teilnehmers, Informationen über die Art des Endgerätes, möglicherweise für den Anschluss jeweils verfügbare Leistungsmerkmale und Berechtigungen sowie Daten über die Zuordnung zu Teilnehmergruppen.
- **Inhaltsdaten** sind die eigentlichen „Nutzdaten“, d. h. die übertragenen Informationen und Nachrichten.
- **Verbindungsdaten** geben Auskunft über die näheren Umstände von Kommunikationsvorgängen. Hierzu gehören Angaben über Kommunikationspartner (z. B. Rufnummern des rufenden und des angerufenen Anschlusses), Zeitpunkt und Dauer der Verbindung, in Anspruch genommene Systemleistungen, benutzte Anschlüsse, Leitungen und sonstige technische Einrichtungen, Dienste und - bei mobilen Diensten - die Standortkennungen der mobilen Endgeräte.

1.5 Fortentwicklung der GSM-Mobilfunktechnik

1.5.1 HSCSD

HSCSD (**H**igh **S**peed **C**ircuit **S**witched **D**ata), eine Erweiterung des GSM Standards, ist ein kanalvermittelnder Datendienst. Zur Datenübertragung werden gleichzeitig mehrere GSM-Funkkanäle genutzt, um höhere Datenübertragungsraten (57 kbit/s) zu ermöglichen.

1.5.2 GPRS

GPRS (**G**eneral **P**acket **R**adio **S**ervice) ist ein paketorientierter Datendienst zur Datenübertragung im GSM-Netz, das hierfür um weitere Infrastrukturkomponenten erweitert ist. Es können mehrere Funkkanäle gebündelt werden, so dass theoretische Übertragungsgeschwindigkeiten von bis zu 171 KBit/s (praktisch ca. 50 kBit/s) erreicht werden. Im Gegensatz zu HSCSD basiert GPRS auf der Vermittlung einzelner Datenpakete und nicht auf der Schaltung fester Übertragungswege. Dazu wird das Internetprotokoll verwendet und jedes mobile Endgerät erhält eine individuelle IP-Adresse (**I**nternet **P**rotocol). Über GPRS können die Nutzer ständig im Netz eingebucht bleiben („allways online“). Die zur Verfügung stehenden Funkkanäle werden auf alle Teilnehmer verteilt. Es wird nicht nach Online-Zeit abgerechnet, sondern auf Basis der übertragenen Datenmenge. Dieser Datendienst ist daher besonders für dialogorientierte Anwendungen, WAP, **i-mode™** und E-Mail geeignet.

1.5.3 UMTS – Die dritte Mobilfunkgeneration

Das Mobilfunksystem der dritten Generation **UMTS** (**U**niversal **M**obile **T**elecommunications **S**ystem) ist das Nachfolge-Mobilfunksystem der GSM-Systeme. Mittels einer leistungsfähigeren Funktechnik (u. a. größere Bandbreite, **CDMA**-Übertragungsverfahren) können beliebige Inhalte (z. B. Multimedia-Anwendungen, Downloads aus dem Internet, Videokonferenzen) mit hoher Übertragungsrate übermittelt werden. Das macht zukünftig diverse neue Dienste möglich.

Die spezifizierten Datenübertragungsraten im UMTS System reichen von 144 kbit/s für den hochmobilen Nutzer (maximale Geschwindigkeit 500km/h) bis zu 2Mbit/s für den quasistationären Betrieb. UMTS Endgeräte werden zunächst multi-mode-fähig sein, das heißt sie können für Sprach- und Datenverbindungen auch das GSM-Netz nutzen.

1.6 Zusätzliche Dienste

1.6.1 Kurznachrichten-Dienste

Mit **SMS** (**S**hort **M**essage **S**ervice) können Textnachrichten an Mobilfunkteilnehmer in aller Welt versendet werden. Bis zu 160 Zeichen dürfen die Kurzmitteilungen umfassen. Der Nachrichtentext wird dabei per Tastatur eingegeben und an den gewünschten Empfänger geschickt. Alternativ kann eine SMS-Mitteilung auch als Internet-Mail abgeschickt werden.

Eine **EMS**-Nachricht (**E**nhanced **M**essaging **S**ervice) besteht aus mehreren aneinander gereihten SMS-Nachrichten. Daraus resultiert, dass auch Mitteilungen mit weit mehr als 160 Zeichen versandt werden können. Ebenso ist es möglich, auch animierte Grafiken, Töne (z. B. Klingeltöne) und formatierte Texte zu verschicken.

MMS (**M**ultimedia **M**essage **S**ervice) ist eine Weiterentwicklung von SMS und EMS. MMS ermöglicht mit Hilfe gesteigerter Mobilfunk-Bandbreiten die Übertragung von farbigen Bildern (Digital-Fotos) und kurzen Filmsequenzen auf entsprechend ausgestattete Mobiltelefone.

Wenn man eine SMS-, EMS- oder MMS-Nachricht verschickt, wird diese auf einem Server des entsprechenden Netzanbieters, dem SMS-, EMS- beziehungsweise MMS-Center, hinterlegt. Der Netzanbieter versendet automatisch eine Benachrichtigung an den Empfänger. Zusätzlich werden von einigen Providern Message-Waiting-Indikatoren auf das Mobiltelefon des Empfängers gesendet (z. B. ein auf dem Display sichtbar werdendes E-Mail-Symbol). Ruft der Empfänger die Nachricht ab, so wird diese vom Server auf das Mobiltelefon übertragen. Anschließend sendet der Netzanbieter eine Anweisung, die das Symbol im Display des Mobiltelefons löscht.

1.6.2 WAP, i-mode™

Das **WAP** (**W**ireless **A**pplication **P**rotocol) und **i-mode™** sind Standards zur Datenübertragung von Internet-Inhalten und Servicediensten (z. B. Banking, Brokerage, Information, Shopping) auf mit jeweils speziellem Browser ausgestattete Mobiltelefone, Handhelds oder PDAs.

Das WAP beschreibt in Anlehnung an bestehende Internet-Technologien eine Architektur sowie eine Protokollfamilie zur Übermittlung von Informationen an mobile Endgeräte. Es definiert unter anderem Eckwerte für so genannte Micro-Browser, mit denen Webinhalte auf Mobiltelefon-Displays dargestellt werden können. Da Bilder und umfangreiche Grafiken im WAP nicht darstellbar sind, müssen entsprechende Inhalte im **WML**-Format (**W**ireless **M**arkup **L**anguage) aufbereitet werden. Hierbei handelt es sich um eine Beschreibungssprache, die zur geräteunabhängigen Darstellung der Informationen dient. Dynamische Informationen können, ähnlich wie mit Javascript im WWW, per **WMLScript** dargestellt werden.

Die WAP-Architektur ist, analog zur Architektur von bestehenden Datennetzen, Client-Server-basiert und beruht auf einem schichtenförmigen Modell, wie man es auch von anderen Netzwerkprotokollfamilien (z. B. TCP/IP) oder dem OSI-Referenzmodell kennt.

i-mode™ ist ein aus Japan kommender Datendienst und ermöglicht ähnlich wie WAP den mobilen InternetZugang. In Deutschland basiert er auf dem paketorientierten GPRS. Der Nutzer blockiert dadurch nicht ständig einen Funkkanal (bzw. Zeitschlitz) sondern die Daten werden in Pakete aufgeteilt und übertragen wenn Kapazitäten frei sind. Das schont Ressourcen und die Abrechnung erfolgt nach Datenmenge und nicht nach Verbindungsdauer.

Um i-mode™-Seiten nutzen zu können wird ein spezielles Endgerät benötigt, welches einen Browser integriert hat, der iHTML interpretieren kann. iHTML ist eine kompakte HTML-Variante, welche dem Standard-HTML sehr ähnlich ist. Es unterstützt HTML-formatierte Texte, Farbgrafiken sowie polyphone MIDI-Töne.

2 Gefährdungspotenzial bei der Nutzung von GSM-Mobilfunkeinrichtungen

Bei der Mobilkommunikation können die übertragenen Signale auf der „Funkstrecke“ nicht physikalisch gegen unbefugtes Mithören und Aufzeichnen abgeschirmt werden, weshalb ein Angriff ohne das bei leitungsgebundener Kommunikation bekannte Zugriffsproblem durchgeführt werden kann.

Ein zweites Problem resultiert daraus, dass die mobilen Kommunikationspartner aus technischen Gründen in regelmäßigen Zeitabständen (sowie stets bei Wechsel der Location Area) Informationen über ihren Standort mitteilen müssen, um immer erreichbar zu sein. Wenn sie selbst eine Verbindung aufbauen, senden sie ebenfalls Standortinformationen aus. Diese können durch den Netzbetreiber oder Dienstbetreiber - aber auch von Dritten - zur Bildung von Bewegungsprofilen missbraucht werden.

Da bei jeder GSM-Mobilfunk-Verbindung auch Festnetze benutzt werden, kann die Sicherheit im Mobilfunknetz nicht größer als dort sein.

2.1 Technisches Abhören der Telefonate

Verschafft sich ein Angreifer Zugang zu den technischen Einrichtungen des Netzbetreibers (Leitungen, Vermittlungseinrichtungen, Basisstationen), ist er in der Lage, alle Telefongespräche, die über diese Einrichtungen geführt werden, abzuhören. Dies gilt sowohl für Verbindungen im Mobilfunknetz als auch im Festnetz. Auch Richtfunkstrecken, auf denen die

Übertragung in der Regel unverschlüsselt erfolgt, sind mit einigem technischen Aufwand abhörbar.

Werden die Verbindungen über leitungsgebundene Wege von der Basisstation zu dem MSC geführt, ist ein physikalischer Angriff auf den Leitungswegen erforderlich. Wird eine Basisstation über eine unverschlüsselte Richtfunkverbindung an den Vermittlungsknoten angebunden, wie es in der Regel geschieht, besteht die Möglichkeit, diese Funksignale mit Antennen und Spezialempfängern unbemerkt aufzufangen und abzuhören. Die Gefährdung kann sich gegebenenfalls dadurch erhöhen, dass auf diesen Richtfunkstrecken alle Telefonate der angebundenen Basisstation übertragen werden.

Die Funkübertragung zwischen dem Mobiltelefon und der Basisstation wird in Deutschland in allen Mobilfunknetzen verschlüsselt. Es gibt aber spezielle technische Systeme, welche die Schwäche der einseitigen Authentisierung im GSM-Netz (nur Mobiltelefon gegenüber Basisstation) ausnutzen: Sie täuschen den Mobiltelefonen eine Basisstation vor, schalten die Verschlüsselung ab und geben den Klarbetrieb vor. Dem Netz gegenüber verhalten sich diese Geräte wie normale GSM-Endgeräte.

Andere denkbare Möglichkeiten zur Abschaltung dieser Verschlüsselung sind technische Manipulationen am Mobiltelefon oder an technischen Einrichtungen des Netzbetreibers.

Einige Mobiltelefone signalisieren eine fehlende Verschlüsselung durch ein Symbol auf dem Display.

Ferner gibt es in der kryptographischen Fachliteratur bereits Beschreibungen von möglichen Attacken auf den GSM-A5-Verschlüsselungsalgorithmus ([**A5**_**1**]).

2.2 Abhören von Raumgesprächen

2.2.1 Abhören mittels handelsüblicher Mobiltelefone

Mobiltelefone können dazu benutzt werden, unbemerkt Raumgespräche aufzuzeichnen oder abzuhören. Im einfachsten Fall dient hierzu ein Mobiltelefon, welches, zum Beispiel bei einer Besprechung, unauffällig im Raum platziert ist und von dem eine Verbindung zu einem interessierten Mithörer aufgebaut wird. Da die Akkukapazität begrenzt ist und auch das Mikrofon nicht auf Raumüberwachung ausgelegt ist, hat ein solcher Abhörversuch aber nur eine begrenzte Wirkung.

Durch geschickte Wahl von Leistungsmerkmalen und Kombination mit einer Freisprecheinrichtung kann erreicht werden, dass ein Mobiltelefon durch einen Anruf von außen in den Gesprächszustand versetzt wird, ohne dass es dies durch einen Rufton signalisiert.

2.2.2 Abhören mittels manipulierter Mobiltelefone

Zum Abhören von Raumgesprächen können auch speziell manipulierte Mobiltelefone und Phone-Cards zum Einsatz kommen, deren Betrieb in Deutschland verboten ist. Das manipulierte Endgerät dient dabei als Abhöranlage, die über das Telefonnetz von jedem Ort der Welt aktiviert werden kann, ohne dass dies am Mobiltelefon erkennbar ist.

Mögliche Hardwaremanipulationen sind zum Beispiel eingebaute Lauschsender - auch in Akkus - und Einbau zusätzlicher Steuerhardware.

Eine andere Möglichkeit, Mobiltelefone für Abhörzwecke nutzbar zu machen, besteht in der Manipulation der geräteinternen Steuersoftware (Firmware). So ist beispielsweise ein Gerätetyp bekannt, bei dem auf diese Weise das Display des Mobiltelefons abgeschaltet wird, obwohl zu dem Gerät eine Gesprächsverbindung besteht.

Durch die Erweiterung der Menüfunktionen der Mobiltelefone mittels „SIM-Toolkit“ und einer neuen Generation von SIM-Toolkit-fähigen SIM-Karten werden Mobiltelefone noch flexibler. Ein derart ausgestattetes Mobiltelefon lässt sich per Mobilfunk vom Netzbetreiber mit neuen Funktionen programmieren. So kann der Kartenanbieter zum Beispiel die Menüstruktur individuell an die Bedürfnisse eines Kunden anpassen. Daraus resultiert eine erhöhte Manipulationsgefährdung.

Damit der Angreifer eine Manipulation durchführen kann, ist es erforderlich, dass sich das zu manipulierende Gerät für eine gewisse Zeit in seinem Besitz befindet.

2.3 Missbräuchliche Datenweitergabe über GSM-Endgeräte

2.3.1 Unberechtigte Datenweitergabe (Innentäterproblematik)

Mit Hilfe von mobilen GSM-Endgeräten zum Beispiel in Form einer PC-Einsteckkarte (Card-Phone) ist es möglich, Daten von dem PC über das Mobilfunknetz und gegebenenfalls per Internet weltweit zu einem anderen PC zu übertragen.

Auf diese Weise kann ein Innentäter unter Umgehung der internen Telefonanlage und am Werksschutz vorbei große Mengen vertraulicher Daten - bei Nutzung von HSCSD oder GPRS mit entsprechend höheren Datenraten - unbemerkt nach außen senden.

Sogar eine nachträgliche Überprüfung solcher Vorkommnisse ist nicht immer möglich, da die Verbindungsdaten beim Netzbetreiber schon gelöscht sein können.

2.3.2 Ungewollte Datenweitergabe (Außentäterproblematik)

Auch Card-Phones können wie normale Mobiltelefone Gegenstand der Manipulation sein. Darüber hinaus besteht hier die zusätzliche Gefahr der leichten Manipulierbarkeit der PC-Software über Viren oder „trojanische Pferde“, die unbemerkt in den Rechner gelangt sein können. Diese Gefahr ist besonders kritisch, da bei einem solchen Angriff nicht nur die gerade verarbeiteten Informationen, sondern auch der gesamte Datenbestand des PC unbemerkt abfließen oder zerstört werden kann.

2.4 Erstellen von Bewegungsprofilen

Bei jedem Einbuchen eines Mobiltelefons werden aus technischen Gründen Informationen über die genutzte Basisstation, die Identität des Nutzers und die Seriennummer des Mobilgerätes an den Netzbetreiber übermittelt. Damit wäre ein Netzbetreiber in der Lage, festzustellen, wann, wo und von wem ein bestimmtes Mobiltelefon eingeschaltet beziehungsweise benutzt wurde. Die Anfertigung von Kommunikationsprofilen und personenbezogenen Bewegungsprofilen ist aber durch Bestimmungen des Datenschutzes untersagt ([**BfD**]).

Durch das Auswerten der Übertragungsprotokolle ist der Netzbetreiber auch in der Lage, die Entfernung des Teilnehmers zur Basisstation zu bestimmen und so zu orten, wo sich ein GSM-Nutzer gerade aufhält. Diese Ortung kann zum Vorteil der Kunden für die Realisierung einer „Homezone“ oder für Zusatzdienste (Location Based Services) genutzt werden.

Mittels spezieller Angriffstechnik ist es möglich, von allen Mobiltelefonen innerhalb des Erfassungsbereiches sowohl die SIM-Karten als auch die Geräteidentität zu ermitteln, ohne dass der Zugang zu den beim Netzbetreiber gespeicherten Verbindungsdaten erforderlich wäre. Damit können ebenfalls Bewegungsprofile von bestimmten Personen oder Mobilfunkgeräten erstellt werden.

2.5 Rufnummernermittlung

Wenn einem Angreifer bestimmte Informationen (IMSI,IMEI,MSISDN) über den Teilnehmer oder ein Mobiltelefon bekannt sind, ist er mit einem hohen technischen Aufwand in der Lage, einzelne Telefonate zu identifizieren.

Auf den Richtfunkstrecken im Mobilfunknetz können die Gespräche anhand der IMEI aus dem Datenstrom gezielt herausgefiltert werden. Die Gespräche können auch im öffentlichen Telefonfestnetz identifiziert werden, wofür die Kenntnis der Teilnehmerrufnummer notwendig ist. IMSI und IMEI können mit entsprechendem Angriffsgerät direkt auf der Funkstrecke zwischen Mobiltelefon und Basisstation ermittelt werden.

Die Ermittlung der Rufnummer MSISDN könnte durch einen Innentäter erfolgen, der beim Netzbetreiber aus der Bestandsdatenbank den Zusammenhang zwischen IMSI, IMEI und MSISDN herstellt oder der zum Beispiel in einer Firma die dienstlichen oder privaten Telefonnummern aus Telefonlisten entnimmt.

2.6 Gefährdungen bei der Nutzung zusätzlicher Dienste

2.6.1 Kurznachrichten-Dienste

Für das Abhören von Kurznachrichten gelten ebenfalls die in Kapitel 2.1 gemachten Aussagen. Ergänzend dazu sei erwähnt, dass die Speicherung und Verarbeitung der Kurznachrichten in den Message-Centers unverschlüsselt erfolgt.

In der Vergangenheit sind Fälle bekannt geworden, in denen Hacker Software-Fehler in bestimmten Mobiltelefonen ausgenutzt haben, um diese durch per SMS-Übertragung erzeugten Buffer Overflow abstürzen zu lassen („Einfrieren“ des Mobiltelefons im aktuellen Betriebszustand).

Es sind ferner Fälle bekannt geworden, in denen Mobiltelefone nach Eingang einer Hacker-SMS nicht mehr löschbare Symbole auf dem Display anzeigten.

Solche Versuche, ein Mobiltelefon via SMS zu stören, sind in der Regel ungefährlich; die auftretenden Funktionsstörungen können meist einfach und schnell korrigiert werden.

Neben den bereits erläuterten Gefährdungen durch SMS-Nachrichten gibt es darüber hinaus noch die Belästigung durch ungebetene SMS-Botschaften - unter anderem verbunden mit der Aufforderung, eine bestimmte Nummer (z. B. eine gebührenpflichtige 0190-Nummer) zurückzurufen.

2.6.2 M-Commerce und M-Payment

Bei M-Commerce-Anwendungen via i-mode™ oder WAP gesellen sich zu den unter 2.3 beschriebenen Gefährdungen alle Gefahren, die bereits an anderer Stelle im Zusammenhang mit E-Commerce beziehungsweise Internet-Nutzung beschrieben worden sind ([**BSIecomm**]).

Bei der Nutzung von Diensten zum Bezahlen per Mobiltelefon (M-Payment) kommen zu den bisher genannten Gefährdungen sämtliche Sicherheitsaspekte im Zusammenhang mit Homebanking hinzu (vgl. [**BSIhomeb**]).

2.6.3 Virenproblematik

Durch die wachsenden Möglichkeiten softwarebasierter Anwendungen auf mobilen Endgeräten steigt auch die Gefahr durch Viren und trojanische Pferde.

2.7 Hoaxmeldungen

Ein Hoax (engl. Streich, falscher Alarm) ist eine Nachricht, die eine Warnung vor neuen IT-Problemen enthält, aber nicht auf realen technischen Fakten basiert. Die einzigen Schäden, die ein Hoax herbeiführt, sind die Verunsicherung und Irritation der Empfänger und gegebenenfalls die Kosten an Zeit und Geld für den Weiterversand des Hoax.

Im Bereich des Mobilfunks gab es eine ganze Reihe solcher Hoax-Nachrichten, bei denen davor gewarnt wurde, dass an Mobiltelefonen die Eingabe bestimmter Tastenkombinationen oder die Wahl bestimmter Rufnummern dazu führen könnten, Gespräche abzuhören oder auf Kosten anderer zu telefonieren. Durch die Nennung renommierter Firmen bestimmter Mobiltelefon-Marken und einiger technischer Fachbegriffe wird der Anschein von Seriosität erweckt. [**BSIgshb**]

3 Schutzmaßnahmen

Grundsätzlich gilt, dass Art und Umfang der Schutzmaßnahmen abhängig sind von der Gefährdungslage. Welche Maßnahmen im Einzelfall umgesetzt werden, liegt in der Verantwortung des Einzelnen.

Da aber oft auch leichtfertig mit der Abhörgefahr im Telekommunikationsbereich umgegangen wird, sollten Sicherheitsverantwortliche prüfen, inwieweit die bisherigen Maßnahmen zur Aufklärung ihrer Mitarbeiter über Gefährdungen im Telekommunikationssektor ausreichen. Mitunter ist es angebracht, die Mitarbeiter regelmäßig über die Abhörgefahren zu informieren und damit auch zu sensibilisieren.

3.1 Schutz vor Abhören von Telefonaten

Ein wirksamer Schutz gegen das Abhören von Telefonaten ist die interoperable, netzübergreifende Ende-zu-Ende-Verschlüsselung. Solange eine solche Verschlüsselung nicht realisiert ist, kann jede Verbindung, ob im Festnetz oder im Mobilfunknetz, potenziell abgehört werden.

Folgende Maßnahmen werden zur Verringerung der Gefährdung empfohlen:

- Grundsätzlich sollten ohne besondere Schutzmaßnahmen keine Telefongespräche mit sensiblem Inhalt geführt werden.
- Es sollten Geräte verwendet werden, die eine fehlende Verschlüsselung auf dem Display anzeigen.
- Im Bedarfsfall ist geschlossenen Benutzergruppen die Verwendung von speziellen kryptierenden Mobiltelefonen anzuraten. Für behördliche Benutzerkreise sei an dieser Stelle auf Kryptomobiltelefone mit VS-Zulassung hingewiesen.
- Einzelverbindungsnachweise sollten auf unbekannte Rufnummern hin überprüft werden.
- Ferner sollte geprüft werden, ob alle Gesprächsgebühren dem Teilnehmer in Rechnung gestellt wurden; fehlende Gebühren für bestimmte Verbindungen können auf Abhören hindeuten.

3.2 Schutz vor Abhören von Raumgesprächen

3.2.1 Schutz vor Abhören von Raumgesprächen mittels handelsüblicher Mobiltelefone

- Das Abhören von Raumgesprächen mittels Mobiltelefonen kann nur dann sicher ausgeschlossen werden, wenn das Einbringen von Mobiltelefonen in den zu schützenden Raum verhindert wird.
- Auf dem Markt sind passive Warngeräte (GSM-Mobiltelefon-Detektoren) verfügbar, die Mobiltelefone, die sich im Sendebetrieb befinden oder neu in Sendebetrieb gehen, melden. Der Wirkungsbereich der Geräte kann so eingestellt werden, dass er auf den zu überwachenden Bereich beschränkt ist. Es wird empfohlen, solche Warngeräte zu installieren und diese bei Gesprächen mit sensitivem oder vertraulichem Inhalt zu aktivieren.
- Es gibt aktive Mobiltelefon-Detektoren, die alle in Reichweite befindlichen Mobiltelefone auffordern, in den Sendebetrieb zu gehen. Diese können wegen der fehlenden Betriebserlaubnis für Deutschland nicht empfohlen werden. Auch für Störsender, die in einem räumlich abgegrenzten Bereich den Funkbetrieb derart stören, dass dort kein Mobilfunkempfang möglich ist, gibt es in Deutschland keine Betriebsgenehmigung.

3.2.2 Schutz vor Abhören von Raumgesprächen mittels manipulierter Mobiltelefone

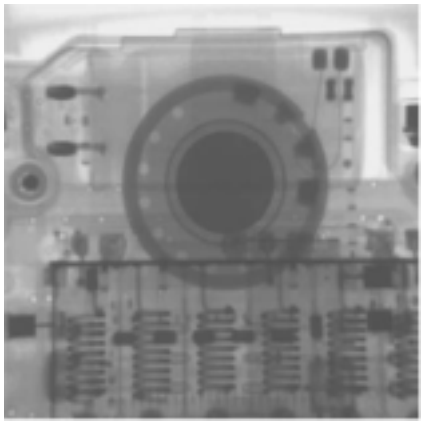
Die unter 3.2.1 genannten Schutzmaßnahmen gelten unverändert auch für den Fall manipulierter Mobiltelefone. Zusätzlich ist Folgendes zu beachten:

- Das Ausschalten des Mobiltelefons reicht als Schutz nicht aus, da bei manipulierten Mobiltelefonen ein unbemerkter Übergang in den Sendebetrieb nicht mit hinreichender Sicherheit ausgeschlossen werden kann (vgl. 2.2.2). Eine solche ungewollte Inbetriebnahme ließe sich allein durch das Entfernen des Akkus unterbinden.

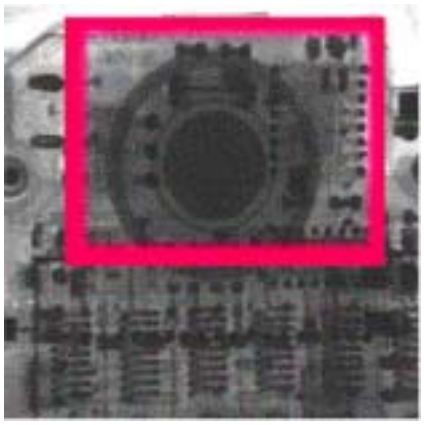
Das Risiko einer Manipulation kann vermindert werden, wenn folgende Punkte beachtet werden:

- Der Kauf von Mobiltelefonen sollte bei vertrauenswürdigen Stellen erfolgen, damit nicht schon beim Erwerb mit einer Manipulation gerechnet werden muss. Bei der Beschaffung größerer Stückzahlen sollte der Auftrag auf mehrere Anbieter aufgeteilt werden.
- Bei Manipulationsverdacht sollte das betroffene Mobiltelefon aus dem Verkehr gezogen werden.
- Hardware-Manipulationen können sicher mit Röntgenprüfverfahren erkannt werden, indem man bei einem Manipulationsverdacht Referenzröntgenbilder von nicht manipulierten Mobiltelefonen mit aktuellen Bildaufnahmen vergleicht.
- Hardware-Manipulationen, bei denen Abhör-Sonderfunktionen mittels zusätzlicher Schaltungseinbauten realisiert sind, sind auch per Sichtprüfung nach Zerlegen des Gerätes nachweisbar.

Derzeit existiert kein Prüfwerkzeug, mit dem die Firmware von Mobiltelefonen auf Manipulationen hin überprüft werden kann.



Referenzröntgenbild eines Mobiltelefons (Teilansicht)



Röntgenbild eines hardware-manipulierten Mobiltelefons (Teilansicht)

3.3 Schutz vor missbräuchlicher Datenweitergabe über GSM-Endgeräte

3.3.1 Schutz vor unberechtigter Datenweitergabe

Einen absoluten Schutz gegen Innentäter gibt es nicht. Daher ist es ratsam, die Mitnahme von Mobiltelefonen in sensitive Bereiche zu untersagen; die Umsetzung dieses Verbotes sollte überprüft werden.

3.3.2 Schutz vor ungewollter Datenweitergabe

Da Fälle von manipulierten Card-Phones nicht auszuschließen sind, sollten in PCs, auf denen sensitive Daten verarbeitet werden beziehungsweise die mit einem Rechner-Netzwerk verbunden sind**,** keine Mobilfunkkarten zugelassen werden. Zur Problematik der Manipulation mit Hilfe „trojanischer Pferde“ wird auf [**BSIvirFB**] verwiesen.

3.4 Schutz vor SIM-Kartenmissbrauch

Das Mobiltelefon und die SIM-Karte sollten stets sicher aufbewahrt werden. Die persönliche Geheimzahl PIN sollte aktiviert bleiben und darf keinesfalls zusammen mit der zum Mobiltelefon gehörigen SIM-Karte aufbewahrt werden.

Bei Verlust der SIM-Karte sollte sofort beim Netzbetreiber eine Kartensperre veranlasst werden, um einen eventuellen Missbrauch - und damit auch einen persönlichen Schaden - abzuwehren.

Es ist empfehlenswert, Einzelverbindungsnachweise regelmäßig auf unerklärliche Gebühren und Zielrufnummern zu prüfen.

3.5 Schutz vor Erstellen von Bewegungsprofilen

Wird die Erstellung von Bewegungsprofilen als Gefährdung angesehen, dann sollten - falls umsetzbar - die Mobiltelefone und auch die SIM-Karten häufiger unter den Mitarbeitern getauscht werden. So wird eine Zuordnung der Geräte und Karten zu einem bestimmten Nutzer zumindest erschwert.

Soll der Aufenthaltsort zu bestimmten Zeiten unentdeckt bleiben, hilft nur ein Ausschalten des Mobiltelefons. Um ganz sicher zu sein, sollte der Akku entfernt werden.

3.6 Schutz vor Rufnummernermittlung

Einen gewissen Schutz gegen die Zuordnung von Rufnummern zu bestimmten Personen gewährt wie bei 3.5 der Austausch von Mobiltelefonen und SIM-Karten. Damit ist keine dauerhafte Zuordnung zwischen Benutzer und Rufnummer beziehungsweise Gerät und Nutzer möglich. Die Zuordnung zum Beispiel zu einer Firma bleibt aber bestehen.

Andere Möglichkeiten zum Schutz gegen Rufnummernermittlung:

- keine Veröffentlichung der Rufnummern im öffentlichen Telefonbuch,
- keine Veröffentlichung der Rufnummern im internen Telefonbuch.

3.7 Schutzmaßnahmen für die Nutzung zusätzlicher Dienste

3.7.1 Kurznachrichten-Dienste

Da es keine Möglichkeit gibt, den Empfang von SMS zu unterbinden, kann an dieser Stelle nur die Empfehlung ausgesprochen werden, die eigene Rufnummer nur vertrauenswürdigen Personen mitzuteilen.

3.7.2 M-Commerce und M-Payment

Vgl. [**BSIecomm**].

3.7.3 Virenproblematik

Vgl. [**BSIvirFB**].

3.8 Hoaxmeldungen

Eine Sammlung von Hoax-Meldungen findet man im Internet unter:
http://www.bsi.bund.de/av/vb/hoaxes.htm.

4 Abkürzungsverzeichnis

AUC	**Au**thentication **C**enter
BSC	**B**ase **S**tation **C**ontroller
BSS	**B**ase **S**tation **S**ubsystem
BTS	**B**ase **T**ransceiver **S**tation
CDMA	**C**ode **D**ivision **M**ultiple **A**ccess
EIR	**E**quipment **I**dentity **R**egister
EMS	**E**nhanced **M**essaging Service
GPRS	**G**eneral **P**acket **R**adio **S**ervice
GSM	**G**lobal **S**ystem for **M**obile Communication
GMSC	**G**ateway **MSC**, Übergang zum Festnetz
HLR	**H**ome **L**ocation **R**egister
HSCSD	**H**igh **S**peed **C**ircuit **S**witched **D**ata
HTML	**H**yper-**T**ext **M**arkup **L**anguage
iHTML	HTML-Variante für i-mode™
IMEI	**I**nternational **M**obile **E**quipment **I**dentity
IMSI	**I**nternational **M**obile **S**ubscriber **I**dentity
IP	**I**nternet **P**rotocol
ISDN	**I**ntegrated **S**ervices **D**igital **N**etwork
MIDI	**M**usical **I**nstruments **D**igital **I**nterface
MMS	**M**ultimedia **M**essaging **S**ervice
MSC	**M**obile **S**witching **C**enter
MSISDN	**M**obile **S**tation **ISDN N**umber
OSI	**O**pen **S**ystems **I**nterconnection
PIN	**P**ersonal **I**dentify **N**umber
SIM	**S**ubscriber **I**dentity **M**odule
SMS	**S**hort **M**essage **S**ervice
TCP	**T**ransmission **C**ontrol **P**rotocol
UMTS	**U**niversal **M**obile **T**elecommunications **S**ystem
VLR	**V**isitor **L**ocation **R**egister
WAP	**W**ireless **A**pplication **P**rotocol
WML	**W**ireless **M**arkup **L**anguage

5 Literatur und Links

[EBEgsm] **Eberspächer J., Vögel H.-J., Bettstetter C.:**GSM Global System für Mobile Communication Vermittlung. Dienste und Protokolle in digitalen Mobilfunknetzen. Stuttgart: Teubner 2000 (3. Auflage)

[WALmobil] **Walke B.:** Mobilfunknetzte und Ihre Protokolle. Stuttgart: Teubner 1998

[BSIgshb] **Bundesamt für Sicherheit in der Informationstechnik**: IT-Grundschutz-handbuch. Köln: Bundesanzeiger 2002 (Auch als CD unter www.bsi.bund.de erhältlich.)

[BSIecomm] **Bundesamt für Sicherheit in der Informationstechnik:** Electronic Commerce (Faltblatt), Bonn 2001 (Faltblatt zum Download unter www.bsi.bund.de/literat/index.htm)

[**BSIhomeb**] **Bundesamt für Sicherheit in der Informationstechnik:** Homebanking. Bonn 2001 (Faltblatt zum Download unter www.bsi.bund.de/literat/index.htm)

[BSIvirFB] **Bundesamt für Sicherheit in der Informationstechnik:** Trojanische Pferde. Sowie Kurzinformationen zu Computer-Viren. Bonn 2001 (Beide Faltblätter zum Download unter www.bsi.bund.de/ literat/index.htm)

[A5_1] **Biryukov A., Shamir A., Wagner D.:** Real Time Cryptanalysis of A5/1 on a PC. In: Schneier B. (Hrsg.): Fast Software Encryption. Heidelberg: Springer 2000 (Siehe auch http://cryptome.org/a51-bsw.htm)

[3gpp] **3rd Generation Partnership Project:** www.3ggp.org

[BfD] **Bundesbeauftragter für den Datenschutz:** www.bfd.bund.de

[BSI] **Bundesamt für Sicherheit in der Informationstechnik:**www.bsi.bund.de

[ETSI] **European Telecommunications Standard Institute:** www.etsi.org

[heise] **Heise Newsticker:** www.heise.de