Diplomarbeit

Erkennen und Abwehren von Angriffen im Mobilfunknetz auf Smartphones

Wilhelm Büchner Hochschule Darmstadt
Fachbereich Informatik

von: Marcus Prem

I. Abstract

Diese Diplomarbeit hat insgesamt 56 Angriffsvektoren beschreiben können, von denen 44 auf eine mögliche Erkennung untersucht wurden.

Die hohe Anzahl an systemimmanenten Sicherheitsschwachstellen und der geschlossene Baseband-Bereich des Smartphones würden nur punktuelle oder sehr aufwendige Methoden zulassen, die eine Erkennung ermöglichen könnten. Dennoch gibt es eine Vielzahl an Alternativen, mit denen es möglich ist die Schwachstellen der Mobilfunktechnik zu umgehen.

Des Weiteren sind verschiedene Strategien dargestellt worden, auf deren Basis eine spätere Realisierung in Form von Hard- und Software möglich ist.

Behörden und Unternehmen nutzen eine eigene Infrastruktur, um eine sichere Kommunikation zu gewährleisten. Dabei müssen beide Gesprächspartner über die gleichen Sicherheitsstandards verfügen.

Zur Realisierung von mobilfunkspezifischen Applikationen hat sich gezeigt, dass die Android-Plattform die besten Voraussetzungen bietet. Es werden aber auch „Development-Kit“ und „Programmable-Modem“ beschrieben, mit denen eine uneingeschränkte Softwareentwicklung eines externen Funk-Empfängers möglich ist.

Der Ausblick zeigt, dass sich VoIP beim Mobilfunk, im Internet und auch bei Festnetzanschlüssen durchsetzen wird und damit auch die Ende-zu-Ende-Verschlüsselung, die einen wirkungsvollen Schutz gegen eine Vielzahl von Angriffsvektoren bieten kann.

II. Inhaltsverzeichnis

I. Abstract 3

II. Inhaltsverzeichnis 4

III. Abkürzungsverzeichnis 8

V. Abbildungsverzeichnis 9

VI. Tabellenverzeichnis 12

1. Einleitung 13

1.1. Zielsetzung 13

1.2. Aufbau der Arbeit 14

1.3. Technische Grundlagen bei GSM/UMTS und LTE 15

2. Angriffsvektoren und Schwachpunkte im Mobilfunknetz und im Smartphone 19

2.1. Daten- und Sprachübertragung im Mobilfunknetz 19

2.1.1. IMSI Catcher als „Man in the Middle“ 19

2.1.2. Verbindungsverschlüsselung mit A5/1, A5/2 und A5/3 21

2.1.3. GSM/UMTS Handover und Erzwingen eines “Fallback to CS” 24

2.1.4. GPRS Core Network 28

2.2. SMS-, MMS-Nachrichten und Signalisierungen im Telefonnetz 30

2.2.1. SMS-Kurznachrichten 30

2.2.2. USSD, MMI und GSM Steuercodes 34

2.2.3. MMS Nachrichten 35

2.2.4. Signalisierungen im Mobilfunknetz 37

2.2.5. Signalisierungen aus fremden Netzen 40

2.2.6. Lawful Interception 42

2.3. Schnittstellen am Smartphone 47

2.3.1. Sende- und Empfangseinheiten für den Mobilfunk ... 48
2.3.2. SIM- und USIM-Smartcard ... 50
2.3.3. Sonstige Schnittstellen ... 52
2.4. Ortung und Positionsbestimmung ... 55
2.5 Zusammenfassung ... 59
3 Angriffserkennung ... 60
3.1. Daten- und Sprachübertragung ... 61
3.1.1. Erkennen einer „fake“ Basisstation bzw. eines MITM-Attacks ... 62
3.1.2. Verbindungsverschlüsselung ... 70
3.1.3. GSM/UMTS Hand Over und Fallbackt to GSM ... 71
3.1.4. GPRS Core Network ... 71
3.1.5. Zusammenfassung ... 71
3.2. SMS, MMS und Signalisierungen im Telefonnetz ... 73
3.2.1. SMS Kurznachrichten ... 73
3.2.2. USSD und GSM Steuercodes ... 75
3.2.3. MMS Nachrichten ... 75
3.2.4. Signalisierungen im Mobilfunknetz ... 76
3.2.5. Signalisierungen aus fremden Netzen ... 76
3.2.6. Lawful Interception ... 77
3.2.7. Zusammenfassung ... 78
3.3. Schnittstellen am Smartphone ... 79
3.3.1. Sende- und Empfangseinheiten für den Mobilfunk ... 79
3.3.2. SIM- und USIM-Smartcard ... 80
3.3.3. Sonstige Schnittstellen ... 81
3.4. Ortung und Positionsbestimmung ... 82

3.5. Zusammenfassung 83
4. Gegenmaßnahmen 84
4.1. Gegenmaßnahmen zu den Angriffsvektoren 85
4.1.1. Kategorie A: IMSI-Catcher und Fake BTS 85
4.1.2. Kategorie B: SMS/PDU Analyse 86
4.1.3. Kategorie C: Mobilfunknetzwerk 87
4.1.4. Kategorie D: Lawful Interception 87
4.1.5. Kategorie E, Schnittstellen am Smartphone 88
4.1.6. Kategorie F, Ortung und Positionsbestimmung 90
4.2. Sicherheitskonzepte von mobilen Betriebssystemen 91
4.2.1. Android 94
4.2.2. BlackBerry OS 98
4.2.3. Apple iOS 100
4.2.4. Windows Phone 7/8 OS 103
4.3. Infrastrukturelle Gesamtkonzepte 105
4.3.1. Konzepte für die geschäftliche und behördliche Nutzung 105
4.3.2. GSM/UMTS Gateway für kleine Firmen und den privaten Gebrauch 109
4.4. Zusammenfassung 110
5 Lösungsoptionen 111
5.1. Konkrete Entwicklung 111
5.1.1. f-BTS-Detector 114
5.1.2. PDU-Filter 115
5.1.3. Layer 2/3 Firewall und IDS 117
5.2. Entwicklungsaufwand und Nutzen 118
5.3. Handlungsvorschläge bei der Nutzung von Smartphones 122

VI. Anhang 126

VII. Glossar 140

VIII. Literaturverzeichnis 141

III. Abkürzungsverzeichnis

BSS	Base Station Subsystem
BTS	Base Transceiver Station
BSC	Base Station Controller
BCCH	Broadcast Control Channel
IMEI	International Mobile Subscriber Identity
MSISDN	Mobile Subscriber ISDN Number
IMSI	International Mobile Subscriber Identity
PLMN	Public Land Mobile Network
PSTN	Public Switched Telephone Network
RSSI	Received Signal Strength Indicator
GSM	Global System for Mobile Communications
GPRS	General Packet Radio Service
EDGE	Enhanced Data Rates for GSM Evolution
LTE	Long Term Evolution
HSPA	High Speed Packet Access
UMTS	Universal Mobile Telecommunications System
SMS	Short Message Service
SIM	Subscriber Identity Module
MSRN	Mobile Station Roaming Number
ME	Mobiles Endgerät
MS	Mobile Station (Mobiles Endgerät) in der Literatur als “Mobiles Endgerät mit SIM-Karte” bezeichnet.
MVNE	Mobile Virtual Network Enabler

V. Abbildungsverzeichnis

IMSI, Quelle: ETSI-Standard 16

LAI, Quelle: ETSI-Standard 16

IMEI, Quelle: ETSI-Standard 16

BSIC, Quelle: ETSI-Standard 16

MSISDN, Quelle: ETSI-Standard 16

MSRN, Quelle: ETSI-Standard 16

A3/A8 Authentifizierung (COMP-128) 17

Mutual Authentication 18

IMSI Catcher als MITM-Angriff 19

KASUMI Block-Cipher 22

GSM-Map Europa Stand 08-201, Quelle: http://gsmmap.org 23

3GPP-Release99, Quelle: "Overview of UMTS", Guoyou He 25

3GPP-Release5, Quelle: "Overview of UMTS", Guoyou He 25

All IP Vision Release6, Quelle: "Overview of UMTS", Guoyou He 26

Mobilfunk Kern-Netz für den paketvermittelten Teil 28

SMS-Übertragung im Netzwerk, Quelle: UMTSlink.at 30

2G und 3G Mobilfunknetz (Release99) 37

Signalisierungen HSPA Rel. 6 und LTE Rel.8, Quelle: UMTSlink.at 39

LTE-Protokoll-Stack Quelle: Computer Communication “The International Journal for the Computer and Telecommunications Industry” 39

HI-Referenzmodell 43

MVNE-Platform mit LI, Quelle: Firma Telogic 46

Blockdiagramm Samsung S2 Quelle: Samsung GT-i9100 Service Manual 47

Arbeitsweise des BP 48

Smartcard Schnittstelle und Blockschaltbild 50

GSM Protokoll Schichten 1-3 60

UMTS Protokoll Schichten 1-3 61

IMSI Catcher Detection, Quelle: Catcher Catcher Projekt Wiki 63

Differenz zwischen falscher und echter BTS; Quelle: Die Werte sind mit G-MoN (Android APP) Ermittelt worden. 65

Verhältnis IMSI und TMSI 68

Frequency Jamming 69

Blockieren des Cipher-Modus 70

Zustandsdiagramm fB-Detection Software 72

Zusammenfassung AV-Erkennung 83

SMS Nachrichteneingang 86

Die Betriebssystemschichten von Android, Quelle: OHA[118] 94

Android RIL Quelle: Quelle: OHA[118] 97

BlackBerry OS Layer 98

iOS Layer 100

Windows Phone OS 7 Framework, Quelle: www.microsoft.com 103

Windows 8 Platform and Tools, Quelle: www.buildwindows.com 104

GSM/UMTS Gateway 109

Neo 1973 mit OpenMoko, Quelle: www.hightech-edge.com 111

G-Mate Dual SIM Adapter, Quelle: www.skyroam.com 112

iSDR RF-Front End, Quelle: digitalconfections.com 113

Turbo-SIM der Firma Bladox, Quelle: Eigene Herstellung 115

NFC und WLAN (Turbo BRA, Turbo Mini), Quelle: Bladox.com 116

Osmocom SIM Tracer und HTC Wildfire, Quelle: Eigene Produktion.....116

Wireshark Ausgabe 117

Aufwand/Nutzen PDU Filter, L2/3 Firewall.....119

Aufwand/Nutzen PDU Filter, L2/3 Firewall.....120

Fragmentierung der Betriebssysteme.....121

Abbildungen im Anhang:

A01 Cell-Broadcast.....125

A02 UMTS Connection Request.....125

A03 ASCI Zeichen 7-Bit.....126

A04-1 VUPEN 0-Day Exploit.....128

A04-2 VUPEN Access.....128

A05 1-4 Spy Files.....128

A06 Gesamtübersicht LI.....129

VI. Tabellenverzeichnis

Verbreitung der aktuellen Betriebssystem-Versionen (Stand 11-2012)……..79
fB-Detector, Berechnung Aufwand/Effizienz ……117
PDU-Filter und L2/3-Firewall, Berechnung Aufwand/Effizienz ……119

Tabellen im Anhang:

T01 A5-Algorithmen ……107
T02 GEA Algorithmen ……107
T03 PDU Typen ……108
T04 Beispiel einer SMS Nachricht ……108
T05 Codierungsgruppen des DCS ……108
T06 Daten der SIM-Karte ……112
T07 Tabelle der Angriffsvektoren …… 130
T08 Funktionen der fB-Detection Software …… 135

1. Einleitung

Das Ausspionieren von Personen über das Mobiltelefon und das Abhören der Gespräche ist mittlerweile relativ einfach und kostengünstig realisierbar. Neben den dazu autorisierten Behörden können auch Privatfirmen auf standardisierte Produkte zurückgreifen, die von der Industrie angeboten werden. Privatpersonen können mit wenigen Hardwaremodulen und Open Source Software, den Betrieb einer eigenen Basisstation realisieren. Besonders in Ländern ohne funktionierende Rechtsprechung ist das ein ernstzunehmendes Problem für jeden Mobilfunknutzer. Zusätzlich entstehen Gefährdungen bei der Nutzung zur Anlagensteuerung und Fernwartung, was oft als „Machine to Machine“ (M2M) bezeichnet wird.

Die Gerätehersteller und Service-Provider vernachlässigen meist den Schutz der Privatsphäre ihrer Kunden. Vorhandene Schutzmechanismen werden oft nur teilweise oder gar nicht eingesetzt, da sie Kosten verursachen und die Leistungsfähigkeit des Netzwerks beeinträchtigen können.

1.1. Zielsetzung

Das primäre Ziel ist, die konzeptionellen Schwachstellen und Angriffsmethoden auf Smartphones zu untersuchen, um eine eventuelle Erkennung und Abwehr zu ermöglichen. Die Lösungen sollten möglichst praxisnah beschrieben werden, um als Bauplan für die spätere Softwareentwicklung zu dienen. Zugleich sollen die Sicherheitskonzepte der unterschiedlichen Betriebssysteme für Smartphones verglichen werden.

Der klassische Befall durch Schadprogramme, die eher zufällig durch den Besuch auf einer Internetseite den Weg auf das Smartphone findet, soll nicht Gegenstand der Arbeit sein.

Zur Protokollierung der einzelnen Schwachstellen wird eine entsprechende Markierung [AV-xxx] im Text gesetzt und in die Tabelle „Angriffsvektoren“ eingetragen. Danach werden die ermittelten Vektoren kategorisiert und zu Gruppen zusammengefasst, wenn es Parallelen im Lösungsansatz gibt.

1.2. Aufbau der Arbeit

Nach einer kurzen technischen Einführung werden im zweiten Kapitel mögliche Angriffspunkte und Schwachstellen identifiziert. Die Luftschnittstelle, die an erster Stelle behandelt wird, ist für potentielle Angreifer am Interessantesten, weil Telefonate belauscht und übertragene Daten mitgelesen werden können, ohne auf das Smartphone direkt einwirken zu müssen. Hierbei wird zwischen der U_m-Schnittstelle für GSM und der U_u-Schnittstelle für UMTS unterschieden.

Die Signalisierung und Datenübertragung im Providernetzwerk wird an zweiter Stelle bearbeitet. Hierzu gehören das Zugangsnetz, also die Basisstationen und deren Controller-Einheiten, sowie das sogenannte Kern-Netz. SMS Dienste nutzen den Signalisierungskanal, um Informationen zu Übertragen und werden deshalb auch in diesem Abschnitt behandelt, sowie die gesetzlich vorgeschriebene Implementierung der sogenannten „Lawful Interception“ Standards.

Im dritten Teil steht das Smartphone im Mittelpunkt der Betrachtung. Es werden zunächst die Schnittstellen des Smartphones untersucht. Über Bluetooth, WLAN oder NFC können interessante Informationen für den Angreifer einsehbar sein.

Im dritten Kapitel werden Lösungen zur Erkennung der Angriffe erarbeitet, um im vierten Kapitel Strategien zur Abwehr und gegebenfalls Gegenmaßnahmen zu entwickeln. In diesem Abschnitt wird auf die unterschiedliche Hard- und Software eingegangen, um im fünften Kapitel eine Bewertung der verschiedenen Smartphone-Systeme durchführen zu können. Neben der theoretischen Lösung soll auch eine mögliche praktische Umsetzung beschrieben werden.

1.3. Technische Grundlagen bei GSM/UMTS und LTE

Das mobile Endgerät (ME) versucht ständig an einer Basisstation (BTS) in Reichweite angemeldet zu sein, damit Anrufe oder SMS-Nachrichten jederzeit empfangen bzw. versendet werden können. Dieser Betriebszustand, bei dem keine aktive Verbindung besteht, wird als „Idle-Mode“ bezeichnet. Das ME empfängt und verarbeitet jedoch ständig Daten aus folgenden Funkkanälen der Luftschnittstelle U_m der BTS:

- BCCH: Broadcast Control Channel zur Identifikation des Netzes (BSIC) und Übermittlung aller nötigen Parameter, um die Kommunikation mit der Basisstation aufzunehmen.
- CBCH: Cell Broadcast Channel überträgt aktuelle Nachrichten, z.B. Wetterdaten oder die lokale Verkehrssituation.
- PCH: Paging Channel kündigt eingehende Anrufe oder SMS an (Downlink).
- RACH: Random Access Channel wird genutzt um sich bei der BTS anzumelden (Shared Uplink).
- AGCH: (Access Grant Channel) dieser Kanal ist dem ME als Downlink zugewiesen. Auf diesem Frequenzband können Signale empfangen werden.

Ist das ME noch gar nicht am Funknetz angemeldet, scannt es nach verfügbaren Stationen, indem es sich zunächst mit einem Sender synchronisiert und dann den BCCH ausliest. Auf diesem Broadcast Channel werden Systeminformationen[1] der BTS gesendet. An die Station mit der höchsten Sendeleistung wird dann ein „Access Burst“ gesendet, der aus einer „Channel Request Message“ auf dem RACH besteht.

Danach wird dem ME eine Frequenz (ARF Channel) und ein „Time-Slot“ zugewiesen, damit es sich über den SDCCH bei dem Netzwerk anmelden kann. Hierzu sendet das Mobilteil ein „Location Update Request“, in dem die IMSI und LAI im Klartext an das Mobilfunknetz gesendet werden.

[1] BTS-Broadcast siehe Anhang Abbildung A01 „Cell-Broadcast“

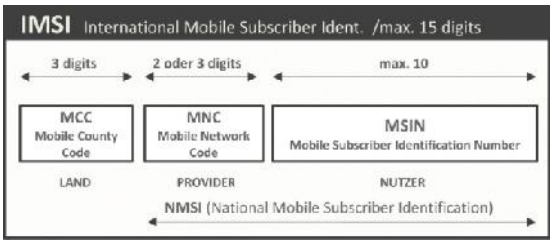


Abbildung 1: IMSI, Quelle: ETSI-Standard[2]

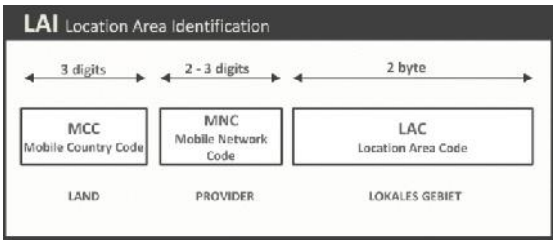


Abbildung 2: LAI, Quelle: ETSI-Standard[3]

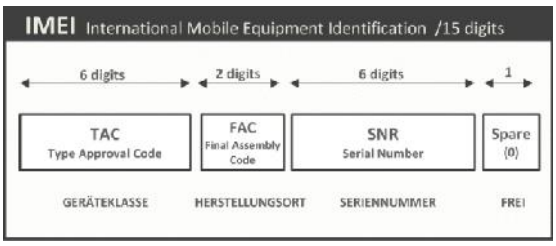


Abbildung 3: IMEI, Quelle: ETSI-Standard[4]

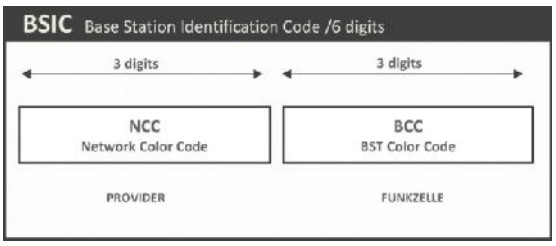


Abbildung 4: BSIC, Quelle: ETSI-Standard[5]

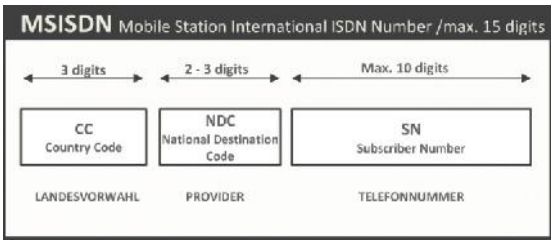


Abbildung 5: MSISDN, Quelle: ETSI-Standard[6]

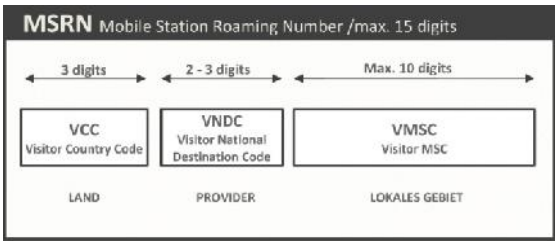


Abbildung 6: MSRN, Quelle: ETSI-Standard[7]

Die IMSI befindet sich auf der SIM Karte sowie in der Datenbank des Providers (HLR „Home Location Register“). Diese weltweit einmalige Nummer wird zur Identifikation des Nutzers benötigt. Wenn die IMSI bei einem Provider registriert ist, darf sich das Smartphone bei der Station anmelden.

Die national/regional eindeutige LAI (Location Area Identity) beinhaltet Informationen über den geografischen Bereich, in der die SIM-Karte zuletzt eingebucht war. Gemeinsam mit der MSISDN (Telefonnummer), TMSI (Temporary MSI) und der Mobile Station Roaming Number (MSRN) wird der Nummerierungsplan gebildet. Eine weitere, eindeutig zuweisbare Nummer ist die IMEI, die im Mobilteil gespeichert ist.

[2, 3, 4, 5, 6, 7] ETSI „Digital cellular telecommunications system (Phase 2+); Numbering, addressing and identification, TS GSM 03.03, V5.0.0, 1996

Anmeldeprozedur an einem 2G-Mobilfunknetz:

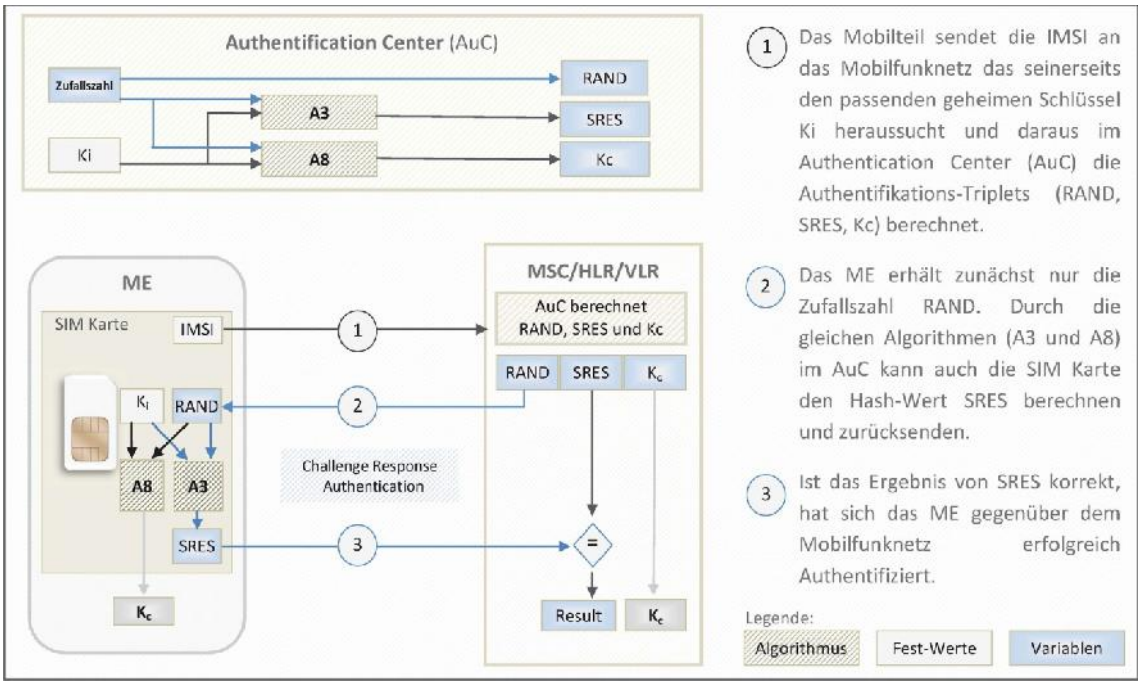


Abbildung 7: A3/A8 Authentifizierung (COMP-128)

Der geheime Schlüssel K_i und der berechnete „Session Key“ K_c, werden niemals über das Netz gesendet. K_c wird später zur Übertragungsverschlüsslung benutzt.

Nach dieser „IMSI-Attach“-Prozedur wird zum Schutz der Privatsphäre anstatt der IMSI die TMSI berechnet und zur weiteren Identifikation benutzt.

Die TMSI ist nur in dem Aufenthaltsbereich LAI gültig und wird bei einem Wechsel in eine andere Funkzelle oder in regelmäßigen Zeitabständen (Periodic Location Update) erneuert, wodurch das Anlegen eines Bewegungsprofils erschwert werden soll. Das Smartphone ist jetzt mit einer Basisstation verbunden.

Ob es aber auch für das Endgerät eine vertrauenswürdige Verbindung ist, kann nicht sichergestellt werden.

Das Konzept hinter UMTS, beziehungsweise dem Zugangsnetz UTRAN, baut auf dem GSM-Standard auf und bietet zusätzliche Eigenschaften und Funktionen[8]. Die Kanalanforderung des in diesem Netz als User Equipment (UE) bezeichneten Endgerätes unterscheidet sich jedoch von seinem Vorgänger. Zuerst wird mit einer Präambel um Erlaubnis gefragt, um dann ein „RRC Connection Request“ auf dem „Physical Random Access Channel“ (PRACH) zu senden (siehe Anhang Abbildung 2).

Zur Identifikation wird aber immer noch die IMSI im Klartext gesendet.

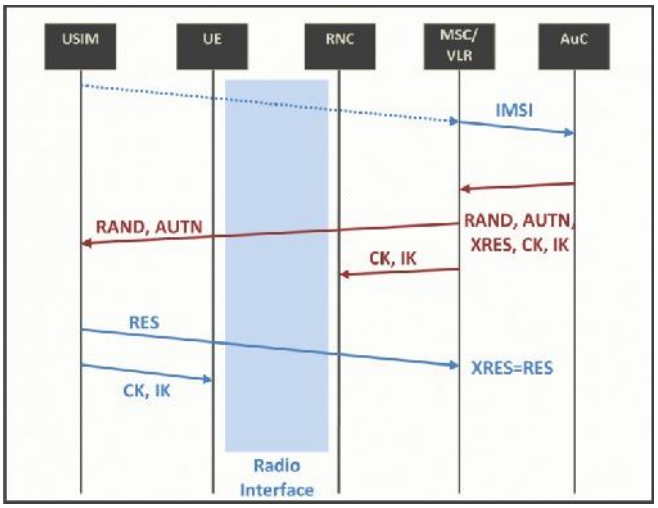


Abbildung 8: Mutual Authentication

Quelle: Klaus v. d. Heyde „Sicherheit im Mobilkommunikationsnetz der 3. Generation (UMTS)“ 2002, S.8

Das UTRAN muss sich mittels „Cipher Key“ (CK) und „Integrity Key“ (IK) auch gegenüber dem Endgerät authentifizieren. Ein MITM wird außerdem durch „Key Refreshness“ und dem Integritätsschutz der Signalisierungsdaten verhindert.

Wobei sich nicht alle Signalisierungsdaten vor Tracking und Tracing schützen lassen. Die Sicherung der Nachrichtenintegrität zwischen UE und RNC erfolgt auf der Protokollebene (Radio Resource Control). Ob der Provider alle Sicherheitsoptionen im vollen Umfang nutzt, ist ihm überlassen.

[8] Technische Spezifikation 3GPP TS 25.401

2. Angriffsvektoren und Schwachpunkte im Mobilfunknetz und im Smartphone

2.1. Daten- und Sprachübertragung im Mobilfunknetz

Anrufe werden immer noch leitungsvermittelt (CS) im Mobilfunknetz übertragen. Bis zu dem Controller des jeweiligen Zugangsnetzes (BSC oder RNC) werden die paketvermittelten (PS) Daten und die CS Daten über die gleichen Komponenten übertragen. Erst dann wird für CS- in das „Network & Switching Subsystem“ (NSS) oder für PS-Dienste in das „GPRS Core Network“ weiter vermittelt.

2.1.1. IMSI Catcher als „Man in the Middle“

[AV-A01] Der Authentisierungsalgorithmus A3 sowie der Algorithmus A8 zur Schlüsselerzeugung werden vom Mobilfunkprovider implementiert. Bei Fehlern können tiefgreifende Sicherheitsprobleme entstehen, durch die zum Beispiel ein Identitätsdiebstahl (SIM-Cloning) ermöglicht werden kann.

[AV-A02] Das Problem bei GSM (CSD,HSCSD, GPRS und EDGE ist die fehlende Authentifizierung der Basisstation (BTS) gegenüber dem Endgerät. Hierdurch kann mit einer „fingierten Basisstation“, beziehungsweise einem IMSI-Catcher[9,10] ein „Man In The Middle“-Angriff durchgeführt werden.

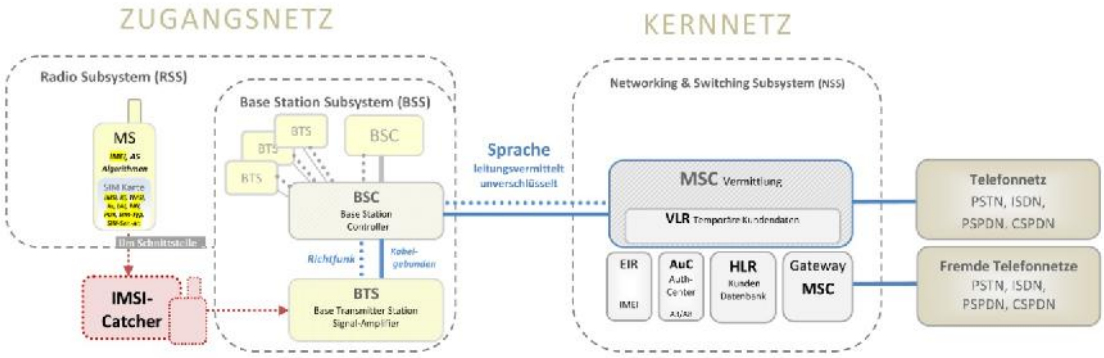


Abbildung 9: IMSI Catcher als MITM-Angriff

Hierzu muss das System in der Nähe der auszuspionierenden Person platziert werden. Durch Erhöhung der Sendeleistung werden die im Umkreis befindlichen

[9] Daehyun Strobel „IMSI Catcher“, Seminararbeit der Ruhr-Universität Bochum 2007
[10] Adam Kostrewa „Development of a man in the middle attack on the GSM Um-Interface“, Master Thesis, Technische Universität Berlin 2011

ME dazu gebracht, sich mit dieser Station des Angreifers zu verbinden. Ist die IMSI-Nummer der abzuhörenden Person noch nicht bekannt, muss sie erst aus der Vielzahl der im Umkreis geführten Telefonate identifiziert werden. Professionelle Geräte wie zum Beispiel der GA-901 von „Rohde & Schwarz“ können deshalb mehrere Kanäle gleichzeitig aufnehmen. Hierdurch werden dann auch unbeteiligte Personen abgehört. Es können bei dieser Methode nur abgehende Telefonate belauscht werden. Der ausgehende Ruf wird an eine „echte“ BTS weitergeleitet. Im Falle der Open-Source-Lösung[11] wird eine Breitbandverbindung genutzt, damit eine Verbindung zum angerufenen Teilnehmer aufgebaut werden kann.

Der sogenannte „MITM-Impersonation“ nutzt das „Dynamic SIM-Cloning“ Verfahren, um sich im Up- sowie auch im Down-Link Kanal zwischen den Kommunikationspartnern zu positionieren, was in Kapitel 2.3.2. „SIM- und USIM-Smartcard“ genauer beschrieben wird.

Dass dieser Angriff auch bei einem gemeinsamen Betrieb von GSM- und UMTS-Netz möglich ist und in bestimmten Fällen sogar ein UMTS MITM, zeigen die wissenschaftlichen Arbeiten von Ulrike Meyer[12] und Susanne Wetzel, auf die später näher eingegangen wird.

[AV-A03] Durch einen „IMSI-Request“ wird das Mobilteil zur Preisgabe dieser eindeutigen Nummer aufgefordert, was im normalen Betrieb nur selten vorkommt. Dadurch können Bewegungsprofile erstellt werden, obwohl dies durch die TMSI verhindert werden soll.

[AV-A04] „Jammer“ bewirken Störungen in den GSM-, UMTS- und LTE-Frequenzbändern.

[AV-A05] UMTS-Femtozellen für den gewerblichen und privaten Bereich werden von verschiedenen Providern im Ausland vertrieben. Alle eingehenden Daten werden über die Breitbandverbindung des Kunden an das Kern-Netzwerk der Telefongesellschaft weitergeleitet. Nicht nur der Besitzer, sondern alle Kunden der Telefongesellschaft können diese Femtozelle benutzen. In England ist ein Fall bei

[11] Uli Ries „IMSI-Catcher für 1500 Euro im Eigenbau“, Zeitschrift C’t 01.08.2010
[12] Ulrike Meyer (University of Technology, Darmstadt), Susanne Wetzel (Stevens Institute of Technology, USA) “ON THE IMPACT OF GSM ENCRYPTION AND MITM ATTACKS ON THE SECURITY OF INTEROPERATING GSM/UMTS Networks” und “A Man-in-the-Middle Attack on UMTS”, 2004

Vodafone dokumentiert, mit dem es möglich war kostenlos Telefonate zu führen und auch alle Telefonate und SMS abzuhören, die über diese Zellen (mit der Bezeichnung „Shure Signal“) geführt wurden. Sogar das Abhören des kompletten Datenverkehrs des Providers war angeblich möglich[13].

2.1.2. Verbindungsverschlüsselung mit A5/1, A5/2 und A5/3

Auf der Luftschnittstelle (U_m) zwischen dem ME und der BTS wird der Verschlüsselungsalgorithmus A5 eingesetzt. Als A5/1 und A5/2 in den späten achtziger Jahren entwickelt wurde, entschied man sich zur „Security By Obscurity“ (Sicherheit durch Unklarheit), was bedeuten soll, dass die Sicherheit des Verfahrens auf die Geheimhaltung des Algorithmus angewiesen ist. Bis 1999 wurden beide Stromchiffre-Verfahren von Marc Briceno und anderen Wissenschaftlern durch Reverse Engineering untersucht und schließlich veröffentlicht.

[AV-A06] Ein Angriff auf A5/1 ist von A. Biryukov, A. Shamir, und D. Wagner[14] im Jahre 2000 durchgeführt worden. Die Komplexität von ursprünglich 2^{64} konnte auf 2^{38}, beziehungsweise 2^{48} vermindert werden. Mittlerweile werden zum Entschlüsseln des A5/1 „Rainbow Tables“[15,16] genutzt. Diese Technik verkürzt den rechnerischen Aufwand, um den richtigen Session Key zurückzurechnen, mit dem dann ein passives Mithören von Telefonaten in Echtzeit möglich ist. Ein modifiziertes Handy älterer Bauart reicht hierzu völlig aus.[17]

In Europa und den USA wird A5/1 eingesetzt. Der viel schwächere A5/2 wurde für Länder entwickelt, in denen eine starke Verschlüsslung verboten ist. Seit 2007 darf dieser Algorithmus laut Standardisierungs-Komitee nicht mehr eingesetzt werden.

---

[13] Roland Eikenberg „Britische Vodafone Kunden mit Femto-Zelle abhörbar“, Zeitschrift C’t 14.07.2011

[14] Alex Biryukov, Adi Shamir, und David Wagner “Real time cryptanalysis of A5/1 on a PC”, “Advances in Cryptology, proceedings of Fast Software Encryption”, Lecture Notes in Computer Science Vol.2139, Springer-Verlag 2001, Seite 1-18

[15] Karsten Nohl „1519_26C3.Karsten.Nohl.GSM.pdf“ (Präsentationsfolien), 26. Berlin CCC

[16] Karsten Nohl “Attacking Phone Privacy”, BlackHat USA-2010

[17] Karsten Nohl “1783_101228.27C3.GSM-Sniffing.Nohl_Munaut.pdf“ 27.CCC Berlin 2010

[AV-A07] A5/0 bedeutet unverschlüsselt, was laut Standard[18] auf dem Display des ME als Cipher-Indicator (zum Beispiel als offenes Schloss) angezeigt werden kann. Die Funktion muss vom Endgerät unterstützt werden und auch auf der SIM-Karte muss dass das „Administartive Cipher Bit“[19] gesetzt sein.

Bei UMTS wird ausschließlich A5/3 zur Verschlüsselung der Funkverbindung verwendet. Das auch als KASUMI bekannte Verfahren wurde im Jahr 2002 veröffentlicht. Mehr Sicherheit entsteht jedoch nur durch die erhöhte Komplexität des Blockchiffre-Verfahrens. Orr Dunkelman, Nathan Keller und Adi Shamir konnten durch einen sogenannten „Sandwich Attack“ die Komplexität von ursprünglich 2^{76} auf 2^{32} reduzieren[20].

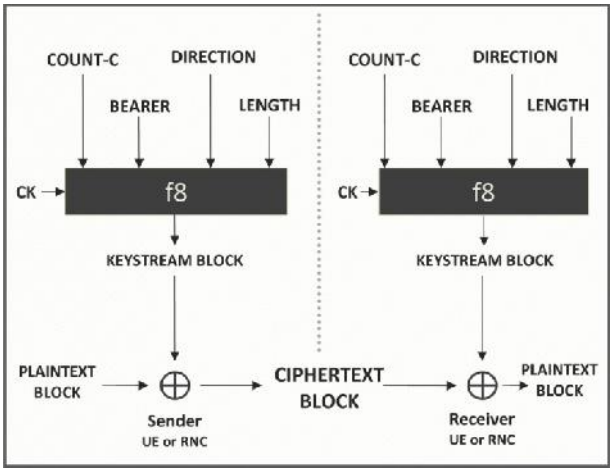


Abbildung 10: KASUMI Block-Cipher

[AV-A08] Integritätsschutz auf der Luftschnittstelle bei UMTS

Veränderungen an den Daten werden vom Empfänger nicht erkannt, wenn der Integritätsschutz deaktiviert ist. So können unter anderem Steuerungssignale eigespielt werden um die Verbindung des UE zu manipulieren. Die Daten zwischen UE und RNC können prinzipiell auch unverschlüsselt Übertragen werden.

[18] ETSI-Standard TS 100 906 V6.2.0 2000-04, siehe B.1.26
[19] ETSI Standard 300 977 GSM 11.11, Siehe 10.3.18
[20] Orr Dunkelman, Nathan Keller und Adi Shamir „A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony“, Cryptology ePrint Archive: Report 2010/013

Eine aktuelle Übersicht über den Sicherheitsgrad der im Einsatz befindlichen Mobilfunknetze soll das Projekt GSM-MAP ermöglichen. Auf der Webseite werden die mit Osmocom kompatiblen Mobiltelefonen[21] und Laptops ermittelten Daten auf einer Landkarte visualisiert.

Abbildung 11: GSM-Map Europa Stand 08-201, Quelle: http://gsmmap.org[22]

Oben: „Intercept“ (Abhören) bei deutschen Providern.

Links: Intercept (Abhören)

Mitte: Impersonation (Identitätswechsel)

Rechts: Tracking (Bewegungsprofil)

[21] Open-Source-Mobiltelefon für Entwickler wiki.openmoko.org das auch bei dem Projekt Osmocom.org verwendet wird.
[22] GSM Map, http://gsmmap.org, [Stand 08-2012]

2.1.3. GSM/UMTS Handover und Erzwingen eines “Fallback to CS”

Ein Handover bezeichnet den Wechsel eines Endgerätes in eine andere Funkzelle (bzw. Kanal und Zeitschlitz). Dies kann verschiedene Gründe haben. Wenn sich das Handy im „Dedicated Mode“ befindet und den Standort wechselt, sich die Übertragungskapazität verknappt oder Störungen im Frequenzband auftreten, kann vom jeweiligen BSC ein Handover eingeleitet werden. Im „Idle Mode“ dagegen entscheidet das ME bzw. UE selbst darüber, mit welcher Station es in Verbindung stehen möchte. Die Verbindungsparameter können also nur im aktiven Zustand wie zum Beispiel während eines Telefonats von dem Mobilfunknetz vorgegeben werden (MAHO Mobile Assisted Handover).

Hierzu gibt es folgende Verfahren:

- Bei einem „Intra-Cell Handover“ wird in der gleichen Zelle nur der Channel oder der Zeitschlitz gewechselt. (GSM/GPRS)
- Der „Inter-Cell Handover“ vermittelt in eine andere Funkzelle. Der BSC ändert sich nicht, weshalb dieser Handover auch als „Intra-BSC Handover“ bezeichnet wird.
- Der „Inter-BSC“ und „Inter-MSC Handover“ vermittelt das ME an eine andere Funkzelle, BSC beziehungsweise MSC.
- „PLMN Handover“ bezeichnet die Übergabe an einen anderen Provider.
- „Inter-System Handover“ bei unterschiedlichen Techniken (GSM/UMTS).
- Bei einem „Soft Handover“ ist das ME mit mehreren Zellen gleichzeitig verbunden, sodass die Verbindung nie abbrechen kann (oft nur für Sprachverbindungen vorgesehen). Das Endgerät ermittelt die Empfangsstärke „Relativ Signal Strength Indicator“ (RSSI) des Broadcast Channels und übermittelt die Informationen an den Controller. Dieser Handover findet zwischen zwei NodeB statt und wird vom RNC organisiert.
- Ein „Hard-Handover“ sieht vor, dass es immer nur eine Verbindung gleichzeitig geben kann. Das Endgerät kommuniziert permanent („ping-ponging“) mit dem zuständigen MSC darüber, mit welcher Station es gerade verbunden sein möchte. Diese Variante tritt bei einem Handover zwischen einem BTS und einer NodeB oder beim PLMN Handover auf.

Die einzelnen Entwicklungsstufen von GSM bis zu LTE werden von einer Gruppe von Standardisierungsgremien im „3GPP-Standard“ spezifiziert. Die aktuelle Ausbaustufe des Mobilfunknetzes ist an der 3GPP Release-Nummer zu erkennen, wobei bereits eingeführte Zugangsnetze wie GSM und EDGE auch in den folgenden Releases weiter betrieben werden[23]. Das Europäische Institut für Telekommunikationsnormen (ETSI) ist Mitglied des „3rd Generation Partnership Project“ 3GPP.

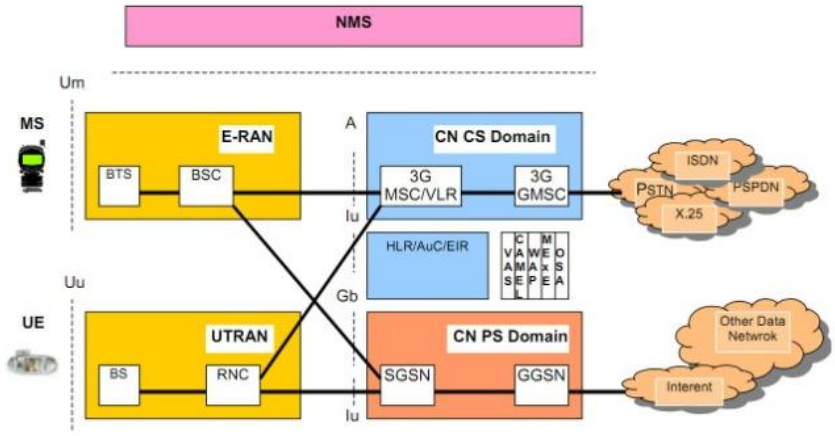


Abbildung 12: 3GPP-Release99, Quelle: "Overview of UMTS", Guoyou He

In der Release99 wird das hinzukommende UMTS-Zugangsnetz UTRAN parallel zum bestehenden Funknetz am MSC und der SGSN betrieben.

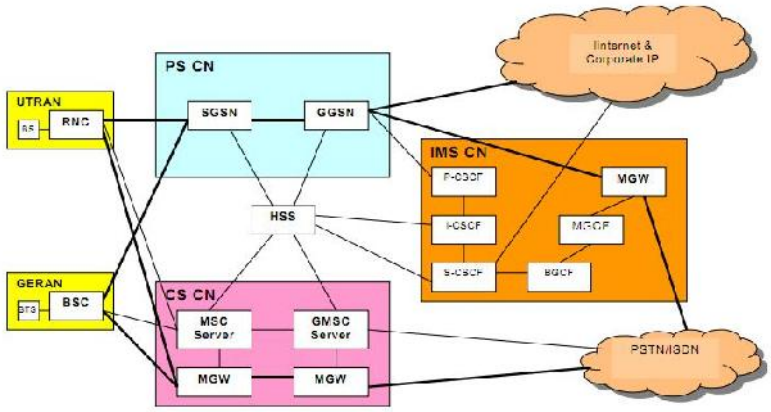


Figure 3-5: Introduction of IMS (3GPP R5)

Abbildung 13: 3GPP-Release5, Quelle: "Overview of UMTS", Guoyou He

[23] Dr. Stephan Rupp, Franz-Josef Banet „Schritt für Schritt; Die Entwicklung von GSM zu UMTS“, Alcatel, Stuttgart 2001

Das „IP Multimedia Subsystem“ (IMS) in der Release5 soll schrittweise die „Circuit Switched“ (CS) und „Paket Switched“ (PS) Domain in einem Kern-Netzwerk vereinen.

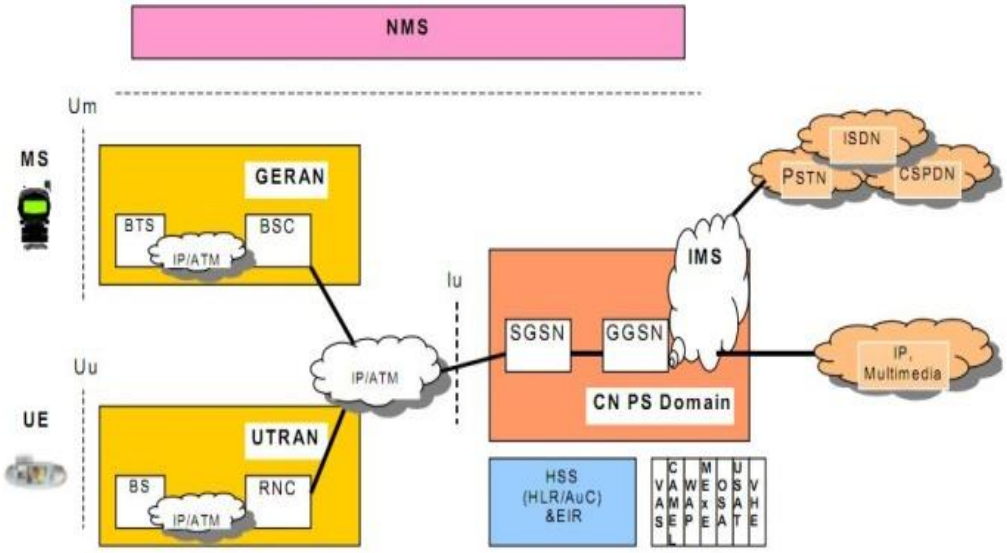


Abbildung 14: All IP Vision Release6, Quelle: "Overview of UMTS", Guoyou He

In der Ausbaustufe mit der Release6 werden alle Daten im GERAN und im UTRAN paketvermittelt (ATM/IP) an das SGSN übertragen[24].

[24] Guoyou He “Overview of UMTS”, Helsinki University of Technology Tech-Paper 2003, Seite 11

[AV-A09] Die sich durch die geforderte Abwärtskompatibilität ergebenden Kombinationen von Hand-Over Prozeduren zwischen den unterschiedlichen Architekturen 2G bis 4G in den jeweiligen Ausbaustufen wirken sich kontraproduktiv auf die Sicherheit von UMTS aus[25]. Im Allgemeinen kann von einer Abschwächung der Sicherheitsfunktionen bei einem Hand-Over in das jeweils darunterliegende Netz ausgegangen werden, also zum Beispiel beim Wechsel von einem 3G- zu einem 2G-Funknetz.

[AV-A10] Ein automatischer „Fall-Back to Circuit Switched“[26] (beziehungsweise „Fall-Back to GSM“) ist für UTMS und LTE vorgesehen. Zur Sprachübertragung wird in einen leitungsvermittelten Dienst (CS) gewechselt und bei Beendigung wieder in das schnellere Netz (PS) umgeschaltet.

[25] Ulrike Meyer (University of Technology, Darmstadt), Susanne Wetzel (Stevens Institute of Technology, USA) “ON THE IMPACT OF GSM ENCRYPTION AND MITM ATTACKS ON THE SECURITY OF INTEROPERATING GSM/UMTS Networks”

[26] Technische Spezifikation 3GPP TS 23.272

2.1.4. GPRS Core Network

Nach einem „GPRS-Attach“, das ähnlich der „IMSI-Attach“ Prozedur abläuft, wird eine P-TMSI erzeugt, um das mobile-Endgerät eindeutig identifizieren zu können. Die Zuweisung einer IP-Adresse sowie einem „Gateway GPRS Support Node“ (GGSN) wird in der „Serving GPRS Support Node“ (SGSN) vorgenommen.

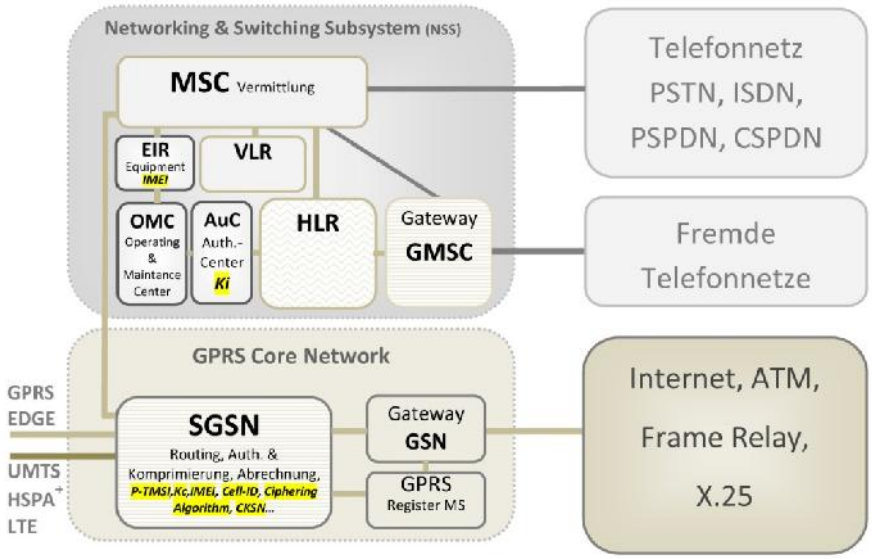


Abbildung 15: Mobilfunk Kern-Netz für den paketvermittelten Teil

Der Grundsätzliche Unterschied zu einem leistungsvermittelten Netz besteht im Routing der Datenströme. Bei GSM wird zunächst der Weg von der Quelle zur Senke zu einem Kommunikationskanal zusammengeschlossen. Bei der Paketvermittlung werden die Daten zuerst in mehrere Teile zerlegt und einzeln über eine vorher nicht vorhersagbare Route gesendet.

Die Daten auf dem Übertragungsweg vom Smartphone zum SGNS sind mit GEA/3 verschlüsselt. Der Empfänger sammelt die Pakete ein und reiht sie in der richtigen Reihenfolge wieder zusammen. Dadurch können beim Senden von Echtzeitdaten wie Sprache und Video gewisse Leistungsprobleme auftreten. Um dies zu vermeiden wurden Qualitätsanforderungen, sogenannte „Quality of Service[27]“ (QoS), festgelegt. Dieses Netzwerk unterstützt „Mobility Management“ (MM) zum Tracking der Endgeräte, „Session Management“ (SMM), Billing (Abrechnung) und

[27] ITU-T E.800, 09-2008, “Terms and definitions related to quality of service and network performance including dependability”

„Transport Management“. Wenn das TCP/IP-Protokoll benutzt wird, können einem Endgerät mehrere IP-Adressen zugewiesen werden. Über das „Point-to-Point Protocol“ (PPP) kann ein Tunnel zwischen Sender und Empfänger aufgebaut werden.

Auf der anderen Seite gibt es aber auch Vorteile, da kein kompletter Kommunikationskanal belegt wird, egal ob gerade Daten ausgetauscht werden oder nicht. GPRS findet somit zum Beispiel bei MMS- (siehe Kapitel 2.2.2.), E-Mail-, Messenger- und WWW-Dienste Verwendung. Über das GGSN wird eine Verbindung ins Internet bereitgestellt.

Es gibt folgende Dienstkategorien:

- Der „Point-to-Point“ (PTP) Dienst, überträgt IP-Pakete zwischen 2 Teilnehmer.
- Bei „Point-to-Multipoint“ (PTM) gibt es einen Sender und eine Empfängergruppe.

Eine simultane Nutzung von GSM und GPRS ist je nach Endgeräte-Klasse möglich:

- Klasse A: simultane Nutzung von GPRS und GSM
- Klasse B: Anmeldung an beiden Diensten, jedoch kann nur ein Dienst gleichzeitig genutzt werden.
- Klasse C: ausschließlich GPRS oder GSM mit Ausnahme von SMS

[AV-A11] Die mit GEA/1, GEA/2 und GEA/3 verschlüsselte Datenübertragung bei GRPS beziehungsweise EDGE kann auf der Luftschnittstelle abgehört werden, wie es vom Chaos Computer Camp 2011 gezeigt wurde[28].

[AV-A12] Die Datenübertragung zwischen Mobilteil und Mobilfunknetz wird im Gegensatz zu GSM nicht im BTS, sondern erst im SGSN entschlüsselt. Manche Provider unterlassen die GEA-Verschlüsselung, um die Nutzung von VOIP-Diensten zu erkennen und zu blockieren.

[28] Karsten Nohl und Luca Melette “1868_110810.SRLabs-Camp-GRPS_Intercept.pdf”, Chaos Computer Camp 2011

2.2. SMS-, MMS-Nachrichten und Signalisierungen im Telefonnetz

2.2.1. SMS-Kurznachrichten

Der SMS-Kurznachrichtendienst ist Teil der GSM (Phase 2)-Spezifikation[29]. Eine SMS besteht aus maximal 160 Zeichen, die jeweils in 7 Bit kodiert wurden. Dies ermöglicht insgesamt 128 (2^7 Kombinationen) Zeichen, die als ASCII-Zeichensatz[30] [31] bezeichnet werden. Es stehen somit 1120 Bit als Nutzdaten zur Verfügung. (140 Zeichen bei 8bit, ISO-8859-1 oder 70 Zeichen bei 16bit für Unicode).

Die Übertragung zwischen Smartphone und Basisstation findet im Signalisierungskanal (SDCCH oder SACCH) der U_m-Schnittstelle statt. Dadurch muss kein Traffic-Channel (TCH) belegt werden, wenn eine Kurznachricht gesendet oder empfangen werden soll.

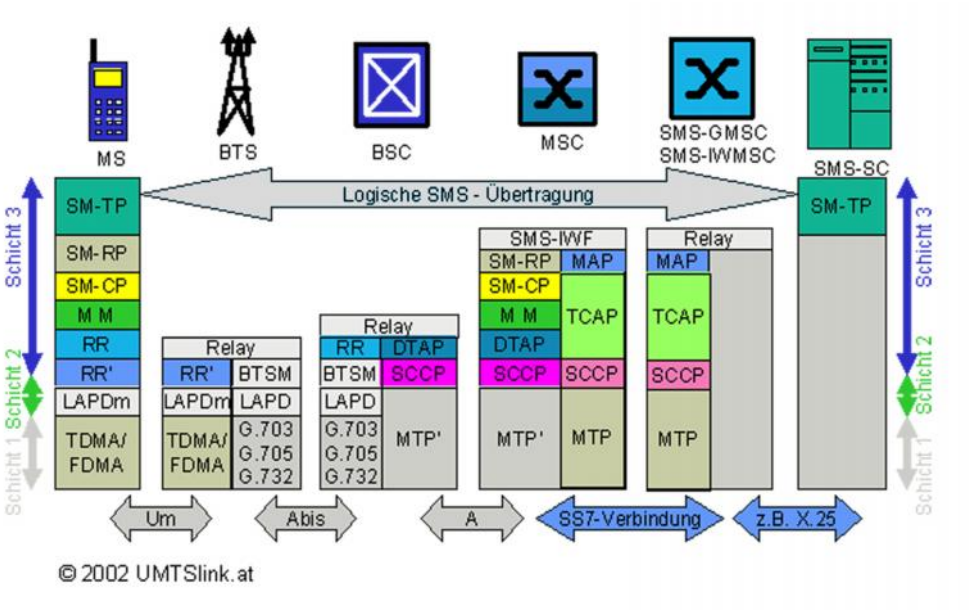


Abbildung 16: SMS-Übertragung im Netzwerk, Quelle: UMTSlink.at

Im Kern-Netz kann die Nachricht als „Message Signal Unit" (MSU) über das „Signaling System No 7" (SS7[32]) weitergeleitet werden. Die MSU-Pakete sind 272 Byte groß, wobei 140 Byte für Nutzdaten übrig bleiben. Deshalb ist die Größe einer

[29] ETSI Standard GSM 04.11, GSM 03.40 und 3GPP TS 24.011 V11
[30] Auch bekannt als IA-5-Alphabet, ISO-7-Bit-Code, USASCII-Code oder CCITT-Code Nr. 5
[31] Siehe Anhang Abbildung „ASCI-Zeichen 7-Bit"
[32] Spezifikation ITU-T-Standards Q.700 bis Q.795

SMS auf 1120 Bit beschränkt. Bei dem SS7 handelt es sich um ein „Out of Band Signalling“[33], dass unter anderem bei GSM, ISDN und ATM benutzt wird.

Das SMS-Center empfängt die Nachricht, speichert sie und versucht direkt die Nachricht zuzustellen. Dieser Betrieb wird als „Store and Forward“ bezeichnet. Wenn über ein IP-Netz zugestellt werden soll, wird die SMS mittels „Short Message Peer-to-Peer“ (SMPP) Protokoll an ein SMS-Gateway und weiter zum Empfänger ausgeliefert.

Es gibt drei Betriebsarten, je nachdem wer gerade Quelle und wer Senke ist.

- Vom ME gesendete SMS werden „Mobile Originated“ (SMS-MO) übertragen.
- Jede SMS zum Endgerät wird als „Mobile Terminated“ (SMS-MT) übertragen.
- Als dritten Betriebsmodus steht der „Cell-Broadcast“ zur Verfügung. Der Provider kann so zum Beispiel Informationen über die Verkehrslage an alle Kunden gleichzeitig senden, die sich in der Funkzelle befinden. Für SMS-CB stehen maximal 93 Zeichen zur Verfügung. Es muss eine Themen-ID gesetzt sein, damit die Empfänger die Nachricht angezeigt bekommen.

Jede Nachricht kann im ASCII-Format (7-Bit-Code) oder als PDU (Protocol Description Unit) in der 7, 8 oder 16-Bit Zeichenkodierung versendet werden. Es stehen 6 verschiedene PDU-Typen[34] zur Verfügung um Nachrichten zwischen den beteiligten Netzwerkkomponenten auszutauschen.

Es gibt auch hier systemimmanente Mängel, die auf die Architektur des SMS-Dienstes und dessen Spezifikation selbst zurückzuführen sind.

[AV-B01] Eine Identifikation ist nur durch die Telefonnummer des Absenders möglich. So können SMS unter falschem Namen versendet werden (Phishing/Spoofing).

[AV-B02] Der Versand zum SMS-Center sowie auch die Speicherung erfolgt unverschlüsselt.

[33] „Außenband-Signalisierung“, Übermitteln der Steuerdaten in einem anderen Übertragungskanal als die Nutzdaten.
[34] Siehe Anhang Tabelle „PDU Typen beim SMS-Versand“

[AV-B03] Werden die Kurznachrichten über einen Gateway an eine E-Mail Adresse oder eine Webschnittstelle weitergeleitet, können die unverschlüsselten Daten ebenfalls mitgelesen werden.

[AV-B04] Eine SMS kann auch direkt, also ohne Service-Center von einem Endgerät zum anderen gesendet werden. Außerdem kann der „SMS Cell Broadcast Service[35]“ dazu genutzt werden.

[AV-B05] Durch das Wireless Application Protokoll[36] (WAP) kann in einer SMS auch eine „Uniform Resource Identifier“ (URI) versendet werden. Dieser sogenannte WAP-Push kann ein Link auf eine Internetseite oder auch auf eine ausführbare Datei sein. Bei GPRS, EDGE oder UMTS werden „Service Indication“ (SI), „Cache Operations“ (CO) und „Service Loading“ (SL) anstatt SMS verwendet, um einen WAP-Push vom Server an den Client zu senden. Der Nutzer sieht keinen Unterschied, ob es sich um eine normale SMS handelt oder um einen WAP-Push. Bei der Verwendung eines „Service Load“ kann vom Nutzer unbemerkt ein Installationsprozess angestoßen werden.

Eine Ausnahme bietet „Research in Motion“ (RIM). Wenn Absender und Empfänger Blackberry-Geräte besitzen und einen Blackberry-Enterprise-Server zur Kommunikation benutzen, können E-Mails, MMS und SMS verschlüsselt per Push übertragen werden. Diese „Managed-Services“ stehen mittlerweile auch für Privatanwender zur Verfügung.

[35] Spezifikation 3GPP TS 23.041 (2010-06)
[36] Spezifikation von WAP 1.0, 1.1 und 1.2 durch das WAPforum.org

Es gibt folgende Nachrichtentypen die nur im PDU-Mode versendet werden können.

- Eine Concatenated SMS besteht aus mehreren Kurznachrichten. Hierdurch können auch größere Dateien, mit mehr als 1120 Bit versendet werden. (SMS1+SMS2+SMS3+…SMSn)
- **[AV-B06]** Die „Flash-SMS[37]“ dienen zum Beispiel dazu, das aktuelle Guthaben einer Pre-Paid Karte anzuzeigen. Sie wird sofort auf dem Display angezeigt und nicht gespeichert.
- **[AV-B07]** Eine „Stille SMS“ ist für den Nutzer unsichtbar. Ähnlich eines Netzwerkpings auf eine bestimmte Adresse, antwortet das mobile Endgerät mit einer Quittung. Zur Ortung eines Smartphones benötigt man jedoch die dabei angefallenen Verbindungsdaten des Providers.

[AV-B08] SMS-Injection[38], wurde in einer Sicherheitsanalyse von Collin Mulliner und Charlie Miller beschrieben. Sie versendeten eine SMS, von einem Endgerät, direkt an das Endgerät. Dies wurde mit einer „SMS_Deliver Message“, die normalerweise vom SMSC an das Endgerät gesendet wird, durchgeführt (siehe Anhang Abbildung: PDU Typen). Diese Methode besteht aus einer Kombination des Angriffs-Vektors B04 und einer PDU-Message zum Einschleusen des eigentlichen Codes.

[AV-B09] Ein anderes Szenario, das verschiedenen Schwachstellen kombiniert, wird von Georgia Weidman als „Bot-Netzwerk für Smartphones[39]“ beschrieben. Über SMS werden die Mobilteile ferngesteuert und können so auch die Infrastruktur des Providers angreifen (Denial of Service, DDoS).

[37] Siehe Anhang Tabelle „Beispiel einer SMS Nachricht“
[38] Collin Mulliner (TU-Berlin) und Charlie Miller “Injecting SMS Messages into Smart Phones for Security Analysis”, 2009
[39] Georgia Weidman “Transparent Botnet Control for Smartphones over SMS”, 2011

Die Nutzung von SMS hat gegenüber MMS mehrere Vorteile.

- Global standardisierter Kommunikationsdienst
- Webdienst zum günstigen SMS Versand über das Internet
- Hohes Vertrauen der Nutzer
- Ressourcen schonend bei der Übertragung
- Zusammen mit der WAP-Push Technologie gibt es ausreichende Möglichkeiten ein System zu manipulieren.

Bei einer EMS-Nachricht „Enhanced Message Service“, die als Vorgänger der MMS gesehen wird, können auch Bilder, Töne und Animationen gesendet werden.

2.2.2. USSD, MMI und GSM Steuercodes

USSD[40,41] (Unstructured Supplementary Service Data) Codes können von Provider, Hersteller und APP-Entwickler genutzt werden. Zum Beispiel bei der Abfrage des Guthabens von Pre-Paid Karten oder für Mobile Banking Anwendungen.

Die GSM Codes unterstützen Funktionen, wie es sie auch bei ISDN gibt. Rufnummernübermittlung (COLR/COLP), Fangschaltung böswilliger Anrufer (MCID) (vorherige Freischaltung muss vom Provider erfolgen), Konferenzschaltung (CONF), Rufumleitung (CFU), Halten einer Verbindung (CH) und vieles mehr.

Die dritte Gruppe bilden die gerätespezifischen MMI[42]-Codes, um zum Beispiel die IMEI abzufragen. Diese Codes werden in das Feld der anzurufenden Telefonnummer eingetragen und mit der Anruftaste bestätigt. Bei manchen ME genügt schon die Eingabe der Nummer um die Funktion auszuführen.

Die GSM und USSD Codes werden an das HLR gesendet. Über die genaue Implementierung der beiden Techniken entscheidet der Provider.

---

[40] ETSI 300 625, “Digital cellular telecommunications system (Phase 2); Unstructured Supplementary Service Data (USSD) – Stage 1 (GSM 02.90 version 4.1.1)”, 10-1997
[41] 3GPP TS 22.090, “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Unstructured Supplementary Service Data (USSD)”; Stage 1 (Release 10)
[42] ETSI TS 122 030, “Digital cellular telecommunications system (Phase 2+)”, 05-2011

[AV-B10] Ein Sicherheitsproblem entsteht, wenn dieser Code ohne Wissen des Nutzers ausgeführt wird. Ein Beispiel bietet das Android Betriebssystem, bei dem durch den Aufruf einer präparierten Webseite der USSD Code ausgeführt wird, der zum Beispiel die SIM Karte sperrt. Das erste Problem ist aber der selbstständige Aufruf der Webseite und erst an zweiter Stelle der USSD Code.

Es gibt aber auch andere Schnittstellen über die Code zur Ausführung gebracht werden kann, wie der RFID Transponder, Push-SMS oder auch die Kamera beim Fotografieren eines QR-Codes.

2.2.3. MMS Nachrichten

Bei einer MMS[43] werden auch Videos oder Live-Streams per WAP-Push übertragen. Die Übertragung findet jedoch nicht im Signalisierungsband, sondern im paketvermittelten Abschnitt statt. Nach der „GRPS-Attach" Prozedur (siehe Kap. 2.1.4.) wird durch den so genannten „Primary PDP Context" (Packet Data Protocol) eine Route zum zuständigen „Access Point Node" (APN) aufgebaut. Mit dem anschließenden „Secondary PDP Context" kann der eigentliche Inhalt zum MMS-Center übermitteln werden. Es können mehrere „Primary- und Secondary PDP Contexts" parallel mit verschiedenen APN's aufgebaut werden.

Die Schnittstelle zwischen Smartphone und MMS-Center arbeitet mit dem WAP-Protokoll. Neu eintreffende MMS werden zuvor mit einer SMS im WAP-Push angekündigt, damit der Nutzer dem Download der MMS zustimmen kann.

Die Infrastruktur für den MMS-Betrieb ist jedoch viel aufwendiger und teurer als die SMS-Infrastruktur. Das MMS-Center besteht aus einem MMS-Relay, Message-Store, MMS-Server und verschiedenen Datenbanken. Die multimedialen Inhalte müssen über das „Transcoding-Interface"[44] für das jeweilige Zielgerät optimiert werden. Hierzu müssen alle gerätespezifischen Daten wie Displayauflösung und unterstützte Audio- und Videoformate verfügbar sein. WAP 2.0[45] Browser können

[43] Open Mobile Alliance V1.3 Specification: MMS Architecture Overview, 2001
und 3GPP TS 22.140 (Stage1) und TS 23.140 (Stage2)
[44] OMA Standard Transcoding Interface v 1.0 OMA-TS-STI-V1_0
[45] Spezifikation von WAP 2.0 durch die Open Mobile Aliance (OMA), www.openmobilealliance.org

per http und SSL Webseiten übertragen und anzeigen. Mittlerweile werden Internetseiten aber über einen gerätespezifischen Browser-Client angezeigt.

[AV-B11] Auch bei MMS-Diensten können sich Absender und MMS-Center nicht authentifizieren.

[AV-B12] Informationen über das Smartphone können am WAP-Gateway abgefragt werden. Dazu gehören die IP-Adresse sowie das Hard- und Softwareprofil. Das Angriffspotential besteht vor allem bei dem Standard WAP 1.1.

[AV-B13] Kein Screening von MMS-Headern beim Transport durch das Mobilfunknetz.

[AV-B14] WAP-Push entlädt den Akku[46]

Wird ebenfalls durch eine Kombination aus verschiedenen Angriffs-Vektoren auf zwei Ebenen realisiert. Zuerst muss das Smartphone-Modell und die IP ermittelt werden. Danach wird durch andauernde Zustellversuche einer MMS auf dem dafür vorgesehen UDP-Port das Smartphone zu einer Antwort verleitet, wodurch es sich laut Untersuchen etwa 22-mal schneller entlädt als im Normalbertrieb. Weil dieser Angriff so existenziell gefährlich sein kann, wird er in der weiterführenden Untersuchung mit einbezogen werden.

[AV-B15] Bei der Synchronisation von E-Mail-Konten, Kalendern, Kontakten und anderen Dateien bestehen ähnliche Sicherheitsrisiken, wie sie von Computersystemen mit Internetverbindung bekannt sind. Eine Firewall ist beim Mobilfunk jedoch an den Gateways der Provider und nicht im Endgerät selbst implementiert. So blockieren viele Service Provider bestimmte Standard Ports, über die Spam-Mails empfangen werden können. Diese Dienste sind Bestandteil des MDM (Mobile Device Management) Konzeptes, das entweder der Service Provider oder eine firmeneigene Enterprise-Umgebung bereitstellt.

[46] R. Racic, D. Ma, Hao Chen (University of California, Davis) "Exploiting MMS Vulnerabilities to Stealthily Exhaust Mobile Phone's Battery", 2006

2.2.4. Signalisierungen im Mobilfunknetz

Das Zugangsfunknetz ist bereits im Teil 2.1. beschrieben worden. Zur Vervollständigung sollen hier kurz die Bestandteile des „Networking & Switching Subsystem“ (NSS) und des „GPRS Core Network“ beschrieben werden. Im NNS sind alle Komponenten zur Sprachübertragung, Rufvermittlung, Benutzerverwaltung und Abrechnung angesiedelt. Das „GPRS Core Network“ stellt ausschließlich Datenverbindungen zur Verfügung.

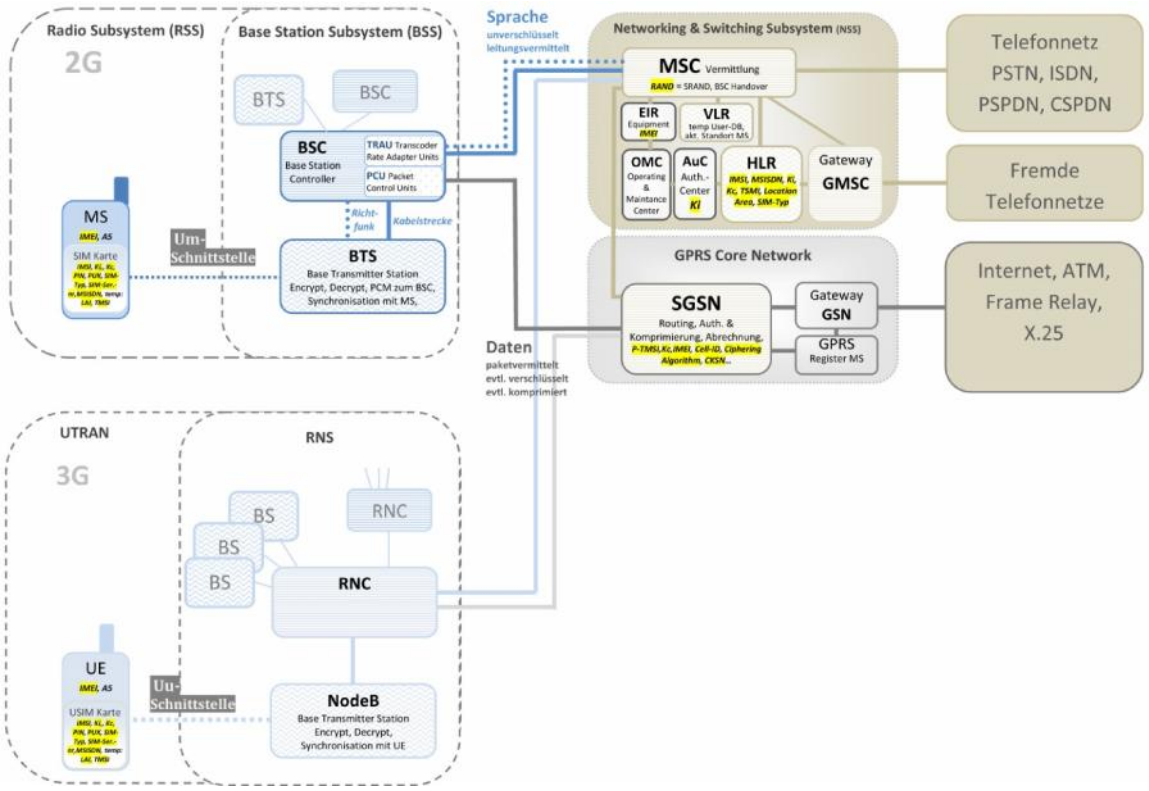


Abbildung 17: 2G und 3G Mobilfunknetz (Release99)

- Das „Mobile Switching Center“ (MSC) das bei GSM und bei UMTS bis zur Release5 zum Einsatz kommt, dient als zentrale Vermittlungsstelle. Später wird bei UMTS diese Funktion gemeinsam mit dem SGSN im „Media Gateway“ (MGW) vereint. Die MSC eines Providers stehen auch untereinander in direkter Verbindung.
- Das „Home Location Register“ (HLR) besteht aus einer Kundendatenbank, die Informationen wie die IMSI, MSISDN und kundenspezifische Diensteinstellungen beinhaltet. Dazu kommen temporäre Daten wie die Adressen der Netzwerkkomponenten und das „Authentication-Triple“ bzw.

„Authentication-Vector“. Bei einem eingehenden Anruf wird zuerst das HLR versuchen, den Teilnehmer im Netzwerk zu identifizieren und den Ruf an den zuständigen MSC-Bereich weiterzuleiten. Das MSC wiederum lokalisiert den Teilnehmer im zugehörigen RSS-, UTRAN-Netz.

- Das „Visitor Location Register“ (VLR) besteht aus einer Datenbank, die meistens direkt im MSC angesiedelt ist und die aktuell angemeldeten Teilnehmer hält. Das VLR bezieht zu Beginn folgende Daten des Teilnehmers aus dem HLR: IMSI, MSISDN, TMSI, MSRN (Mobile Station Roaming Number), LAI, MSC-Adresse, HLR-Adresse, Diensteinstellungen bzw. gebuchte Leistungen und deren Abrechnung im Billing Center.
- Das „Equipment Identity Register“ (EIR) verwaltet drei Listen zur Identifikation von IMEI Nummern. Die schwarze Liste beinhaltet die gesperrten Endgeräte. Die IMEIs der weißen Liste hingegen dürfen sich mit dem Netzwerk verbinden. Die graue Liste beinhaltet die Endgeräte, die unter Beobachtung stehen. Provider tauschen ihre Listen nicht untereinander aus. Außerdem kann die IMEI-Nummer des Mobilteils verändert werden.
- Das GPRS-Kern-Netz bedient sich der Datenbanken und der Infrastruktur des NSS, benutzt aber zur Übertragung der Nutzdaten andere Protokolle.
- Ein wichtiges Subsystem, das noch nicht besprochen wurde, ist das „Operation Support Subsystem“ (OSS). Dieser Teil ist für die Abrechnung und die Wartung des Systems zuständig. Im „Operating Maintenance Center“ (OMC) findet die Gebührenerfassung statt. Das OMC ist besonders gesichert und wird vom Personal mit beschränkten Zugriffsrechten verwaltet.

Ab der Release5 des 3GPP-Standards wird das „Next Generation Network[47]“ (NGN) eingeführt. Die unterschiedlichen Infrastrukturen, die zum Betrieb von Festnetz, Mobilfunk und Breitbandkabelnetzen benutzt werden, sollen aus Kosten- und Effizienzgründen in einer NGN-Spezifikation vereint werden. Für PSTN und ISDN-

[47] ETSI TR 180 005, “Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN)”, bzw .. TISPAN Work Item “DTR/TISPAN-00005-NGN-R2NGN-Release 1”

Dienste werden dann Schnittstellen emuliert, damit die Abwärtskompatibilität für ältere Geräte gewahrt bleibt. Auch die SS7 Protokolle zur Signalisierung und Vermittlung werden im vollen Umfang weiter unterstützt. Das UTRAN Release6 und das LTE-Netz Release8 werden in der folgenden Abbildung gegenübergestellt. Die Vermittlungsaufgaben übernimmt bei LTE das „Mobile Management Entity“ (MME). Die Nutzdaten werden auf direktem Weg, zwischen der Funkschnittstelle (eNodeB) und der „Envolved Packet System Gateway“ (PDN-GW) ausgetauscht.

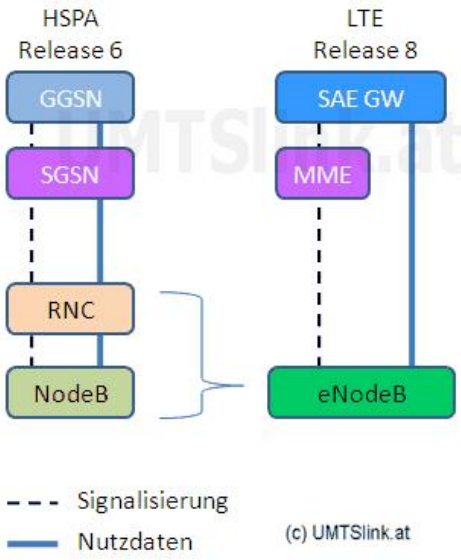


Abbildung 18: Signalisierungen HSPA Rel. 6 und LTE Rel.8, Quelle: UMTSlink.at

Der Transport der einzelnen Datenpakete findet bei LTE ausschließlich über die UDP/IP-Protokollebenen statt. Durch die Reduzierung von Komponenten und Schnittstellen werden die Investitions- und Betriebskosten der LTE-Technologie weiter gesenkt.

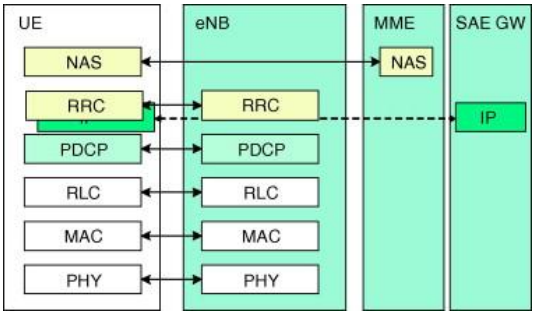


Abbildung 19: LTE-Protokoll-Stack

Quelle: Computer Communication “The International Journal for the Computer and Telecommunications Industry”

[AV-C01] In den GSM Netzabschnitten zwischen BTS, BSC und MSC sind die Daten nicht verschlüsselt und werden bei Bedarf über Richtfunkstrecken übertragen, wodurch an diesen Stellen ein passives Mithören oder das Abfangen des Session-Keys möglich ist.

[AV-C02] Schutz aller Daten (Nutz-, Signalisierungs- und Managementdaten) im Kern-Netz ist auch bei UMTS nicht zwingend vorgeschrieben.

[AV-C03] Über Drittanbieter[48], die einen direkten Zugriff auf Teile des Kern-Netzes erhalten, können ebenfalls Sicherheitsprobleme entstehen.

Ein Angreifer kann auch versuchen direkt das Smartphone im Mobilfunknetz anzugreifen. Die Telekom[49] betreibt sogenannten „Honepot's" um Angreifer in eine Falle zu locken. Durch den Gebrauch von IP- und Port-Scannern können sich Angreifer mit einem fremden Smartphone verbinden und eventuell sogar mit Schadecode infizieren. Die Honeypot`s bestehen aus virtuellen Abbildern von schutzlosen Mobilen Endgeräten. Zum einen können so Angriff in Echtzeit Analysiert werden und zum anderen wird die Aufmerksamkeit von den „echten" Endgeräten abgelenkt.

2.2.5. Signalisierungen aus fremden Netzen

Mit fremden Netzen ist das Festnetz (PSTN „Public Switched Telephone Network"), das Internet und die Mobilfunknetze anderer Provider gemeint.

[AV-C04] Die „Caller ID-Spoofing" Methode nutzt den Umstand aus, dass der Angerufene nur anhand der Telefonnummer den Anrufer identifiziert kann. Unter Nutzung einer VoIP-Gateway kann die frei gewählt werden. Auch das Anhören einer fremden Mailbox kann über „ID-Spoofing" ermöglicht werden.

[AV-C05] „Early-Media-Stream", das unter anderem zur Preisansage vor einem Verbindungsaufbau dient, kann dazu ausgenutzt werden, kostenlos zu Telefonieren[50]. Dabei fallen keine Verbindungsdaten an, die gespeichert werden könnten. Das eigentliche Problem besteht jedoch darin, dass das Mikrofon

[48] Whatevermobile.com bietet neben SMS-Services auch „certSMS" und „Over-The-Air" Konfigurationen an.
[49] Siehe C't "Fallensteller, Honeypots zur Analyse von Angriffen auf mobile Endgeräte", Ausgabe 15 vom 02.07.2012, Seite 134/135
[50] G. Camarillo, E. Schulzrinne, „Early Media and Ringtone Generation in the Session Initiation Protocol (SIP)", 2004

während der Wartezeit schon geöffnet ist und der Angerufene bereits zuhören kann. Die technische Realisation ist aber nicht unerheblich. Hierzu sind Telefonanlagen nötig die solche Leistungsmerkmale unterstützen. Eine alternative ist die Open Source Software „Asterisk“ auf die später genauer eingegangen wird.

[AV-C06] Die SS7-Protokolle und Signalisierungen dienen zur Vermittlung und Routing im Mobilfunknetz sowie bei der kabelgebundenen Kommunikation bei ISDN oder VoIP. Grundsätzlich besitzen die Signalisierungen beim Rufaufbau keinerlei Sicherheitsmechanismen und keine kryptische Verfahren, um die Datenintegrität und Vertraulichkeit zu schützen. SS7 vermittelt auch das Authentifizieren, Autorisieren und die Abrechnungsdaten, wenn sich ein Nutzer mit seinem Smartphone beziehungsweise mit seiner SIM-Karte an einer Basisstation eines ausländischen Roaming Partners anmeldet.

2.2.6. Lawful Interception

Hiermit ist die legale Überwachung von Einzelpersonen oder auch Personengruppen durch eine staatliche Behörde, der sogenannten „Law Enforcement Agency“ (LEA), gemeint. Damit Anbieter in Europa überhaupt eine Lizenz zum kommerziellen Betrieb eines öffentlichen Netzwerkes bekommen, müssen sie sogenannte LI-Schnittstellen bereitstellen.

Zur Telekommunikationsüberwachung zählen das Mithören von Telefonaten sowie das Mitlesen von SMS, E-Mails, Faxnachrichten und des übrigen Datenverkehrs. Alle Informationen über das sogenannte „Target“ wie zum Beispiel die Betriebszeiten, Lokalisation, IMEI, IMSI und die PUK der SIM-Karte müssen der LEA zugänglich gemacht werden. Damit das System weltweit funktioniert und so wenig Kosten wie möglich verursacht, wurde ein einheitlicher Standard entwickelt.

Ein internationales Komitee (TC LI) aus Polizei- und Nachrichtendiensten führt das Pflichtenheft mit allen Funktionen und Schnittstellen, die bereit gestellt werden müssen. Die Arbeitsgruppe „SA3 LI“ setzt die Vorgaben dann in einen technischen Standard um. Diese Gruppe besteht aus Firmen wie Vodafone, Nokia-Siemens, Alcatel-Lucent oder Ericsson. Aus den nationalen Gesetzen des jeweiligen Landes lässt sich die Konfiguration solcher LI-Systeme ableiten. Zum Beispiel bei der Reglung zur Vorratsdatenspeicherung gibt es sehr große Unterschiede zwischen den Europäischen Staaten.

In Europa wurde die Spezifikation[51] vom European Telecommunications Standards Institute standardisiert. In den USA ist hierzu das „Communications Assistance for Law Enforcement Act“ (CALEA) und in den ehemaligen GUS Staaten das „System for Operational Investigative Activities“ (SORM) zuständig.

[51] ETSI TS 101 671 und ES 201 671 „Telecommunications Security; Lawful Interception (LI); Handover Interface for the Lawful Interception of Telecommunications Traffic”

Die ETSI-Spezifikation beschreibt die Funktionsweise des „Handover Interface“ (HI). Die LEA muss zuerst von einer autorisierten Stelle wie zum Beispiel einem Gericht eine Genehmigung zum Abhören erhalten. Diese wird dem Provider vorgelegt, der dann verpflichtet ist alle im Netzwerk anfallenden Daten des Targets als Kopie an das „Handover Interface“ (HI) zu senden.

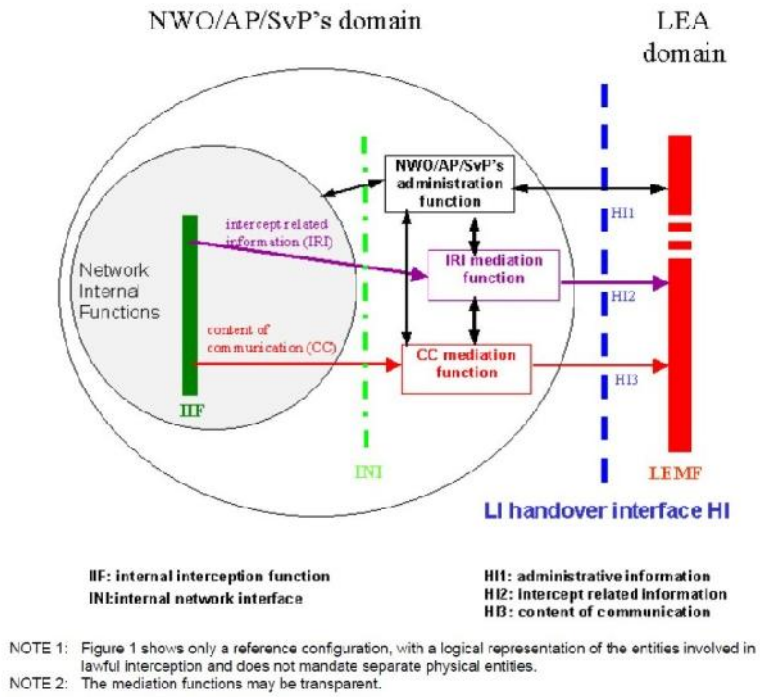


Abbildung 20: HI-Referenzmodell

Quelle: ETSI TS 101 671 V3.9.1. “Technical Specification Telecommunications security[52]”

HI1 repräsentiert die administrative Schnittstelle der LEA auf das Netzwerk des Providers. Über HI2 erhält die LEA Verbindungsdaten „Intercept Related Information“ (IRI), also alle Verbindungsdaten, nicht dem eigentlichen Inhalt (CC). Dieser wird über die HI3 Schnittstelle zur LEA Domain geleitet. Die HI-Schnittstelle muss in allen Geräten, die Vermittlungsaufgaben erfüllen, integriert werden, wie zum Beispiel der MSC und SGSN. Werden mehrere Anfragen für die gleiche Identität gestellt, dürfen die einzelnen Behörden nichts von den anderen Abhöraktionen bemerken.

Weitere Mobilfunkrelevante ETSI-Standards für LI finden sich in TS 143 033[53] (Release5) und TS 133 106[54] (UMTS/LTE).

[52] Quelle: ETSI Technical Specification Telecommunications security; Lawful Interception (LI); “Handover interface for the lawful interception of telecommunications traffic”, Abschnitt 5, Abbildung 1, ETSI TS 101 671 V3.9.1. [11-2011]

Die zum Betrieb der LI-Infrastruktur benötigten Hard- und Software wird sowohl von Firmen der Arbeitsgruppe SA3 LI wie auch von anderen Spezialfirmen hergestellt. Dokumentationen zu diesen Produkten sind nur von CISCO erhältlich. Produktinformationen von anderen Herstellern befinden sich bei Wikileaks.org unter „The Spyfiles[55]“.

[AV-D01] „Unlawful-Interception“ - der Missbrauch durch unbefugte Dritte. Angriffspunkte hierzu gibt es einige, da Anfragen durch die Behörde über das „Simple Network Management Protocol“ (SMTP) an den Provider übermittelt werden kann. Hierüber könnten auch fremde eine Anfrage starten (Spoofing). Hinzu kommt, dass die unterschiedlichen LI-Implementierungen der Hersteller Fehler enthalten die, solange sie vom Provider nicht geschlossen werden, durch unautorisierte Personen benutzt werden können. So war es auch möglich, die griechische Regierung in den Jahren 2004 und 2005 abzuhören. Hierzu wurde eine Schwachstelle im MSC der Firma Ericsson ausgenutzt und mittels Schadsoftware sogar die LI-Schnittstelle abgehört[56].

[AV-D02] Die Branche der LI-Hersteller bietet auch eine Vielzahl von mobilen Abhöranlagen wie den IMSI-Catcher. Diese können ohne die vorherige Zustimmung durch das Gericht oder die Hilfe eines Netz-Betreibers eingesetzt werden.

[AV-D03] Sogenannte „Zero-Day-Exploits[57]“ stellen ebenfalls recht zuverlässige Methoden bereit, um ein ME gezielt mit Schadsoftware zu infizieren. Sie werden von Softwarefirmen zum defensiven Schutz sowie zum offensiven Einsatz angeboten. In Deutschland wird der Einsatz von Spionageprogrammen durch das Quellen-TKÜ Gesetz ermöglicht.

---

[53] ETSI Standard TS 143 033 “Digital cellular telecommunications system (Phase 2+); Lawful Interception; Stage 2 (3GPP TS 43.033 version 6.0.0 Release 6)”. 12-2004
[54] ETSI Standard TS 133 106 “Universal Mobile Telecommunications System (UMTS); LTE; Lawful interception requirements”, 05-2011
[55] The Spyfiles, URL: wikileaks.org/the-spyfiles.html
[56] IEEE Spectrum Article „Athens Affair“, July 2007
[57] Zum Beispiel „Exploit Service“ der Firma VUPEN (www.vupen.com). Siehe Anhang Abbildung 6-1 „0-Day-Exloits der Firma VUPEN“ und Abbildung 6-2 „ Voraussetzungen“

[AV-D04] Die LEA-Domain könnte von außen angreifbar sein, da hier laut Spezifikation vom Hersteller ein Remotezugang implementiert werden kann. Dazu kommen mögliche Angriffe von Insidern, die das LEA für eigene Zwecke missbrauchen könnten. Die Arbeit von Tom Cross[58] zeigt hierzu verschiedene Ansätze.

[AV-D05] Neben diesen ETSI-Spezifikationen sind Informationen der sogenannte „Klein Declaration[59]“ bekannt geworden. Bei diesem Verfahren werden zunächst alle Daten, die im Glasfaser-Backbone übertragen werden gesplittet und auf eigenen Serverfarmen abgespeichert. Die anfallenden Datenmengen werden unter sehr großen Rechenaufwand ausgewertet. Hierzu sind nur Geheimdienste wie die NSA (National Security Agency) und der FSB (Nachfolger des KGB) fähig. Mit modernen Systemen kann eine Person oder ein Personenkreis aus tausenden Individuen herausgefiltert und in Echtzeit überwacht werden. Die benötigte Hard- und Software ist ebenfalls auf Wikileaks veröffentlicht.

Das letzte Hindernis für die LI könnte die Verschlüsselung durch die Kommunikationspartner an den Endpunkten darstellen, wie es zum Beispiel bei Secure-VoIP oder beim Versand von E-Mails der Fall sein kann. Laut Standard ist hierzu eine Schlüsselhinterlegung[60] vorgesehen, was aber zumindest offiziell von Teilen der Industrie bis heute abgelehnt wird. Sicher ist jedoch, dass bei kommerziellen VoIP-Angeboten ein Master-Key für LEA’s bereitgehalten wird.

[58] Tom Cross, „Exploiting Lawful Interception to Wiretap the Internet“, 2010
[59] Die Bezeichnung ist nach dem AT&T Ingenieur Mark Klein benannt, der als erster die Überwachungstechniken der NSA outete, indem er geheime Dokumente eines „Spy-Rooms“ Veröffentlichte und vor Gericht eine eidesstattliche Erklärung (Declaration) abgab.
[60] Key Recovery: Mit einem hinterlegten Schlüssel könnten Behörden in Echtzeit Nachrichten und Telefonate entschlüsseln.

Die Firma Telogic betreibt die Infrastruktur für verschiedene „Mobile Virtual Network Operator“ (MVNOs). Diese als Mobilfunk-Discounter bekannten Unternehmen bieten unter anderem auch reine Datendienste an und realisieren ihre Sprachdienste mit Mobile-VoIP.

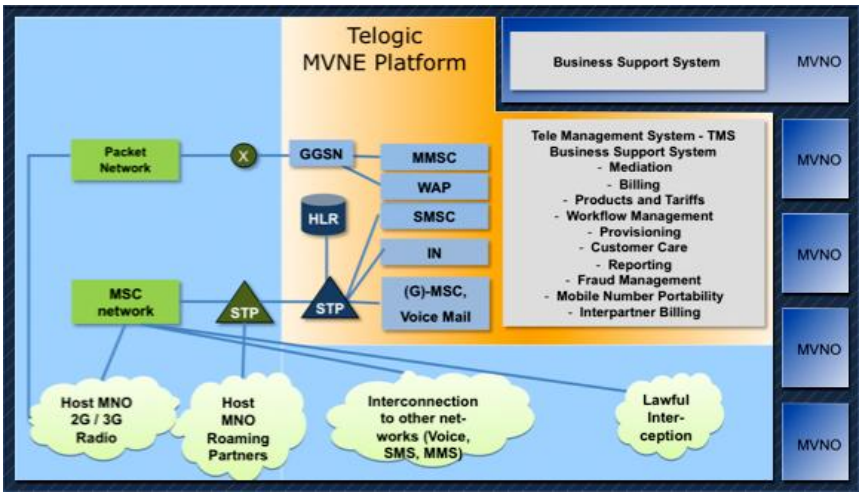


Abbildung 21: MVNE-Platform mit LI, Quelle: Firma Telogic

Wie es internationalen Firmen in Ländern wie Indien, UAE, USA oder auch in England ergehen kann, zeigt das Beispiel BlackBerry[61], der sich mittlerweile mit den Regierungen geeinigt hat.

Die Messenger-Software Skype kann den Stream noch vor der Verschlüsselung auf spezielle Server leiten, die den Behörden zugänglich sind. Microsoft, der neue Eigentümer dieser Firma, hat schon im Jahre 2009 ein Patent[62] angemeldet, dass eine Schnittstelle beschreibt um VoIP Gespräche einfacher belauschen zu können.

Bei allen kommerziellen Angeboten kann davon ausgegangen werden, dass entweder ein Masterkey bekannt ist oder über eine Backdoor in der Software auf Daten zugegriffen werden kann[63].

---

[61] In Indien und den UAE wurde damit gedroht, die Verschlüsselung durch Blackberry-Services zu Verbieten. Quelle: http://www.guardian.co.uk/business/2010/aug/02/blackberry-ban-uae-gulf-states Später hieß es jedoch, nach Verhandlungen mit RIM, dass es kein Verbot gäbe. http://www.bbc.com/news/technology-11499755 In Saudi Arabien wurde das Verbot aufgehoben, nachdem RIM einige Server innerhalb des Landes platziert hatten.

[62] Ghanem; George; (Redmond, WA) ; Bizga; Lawrence Felix; (Monroe, WA) ; Khanchandani; Niraj K.; (Redmond, WA), US-Patent application number: 20110153809, “Legal Intercept”, 23.12.2009

[63] Es gibt aber auch andere Ansätze VoIP zu Entschlüsseln. Siehe Andrew M. White, Austin R. Matthews, Kevin Z. Snow, Fabian Monrose, “Phonotactic Reconstruction of Encrypted VoIP Conversations”,2011

2.3. Schnittstellen am Smartphone

Grundsätzlich besteht ein Smartphone, ähnlich einem Computer, aus verschiedenen Speichereinheiten (RAM/ROM/SD), Schnittstellen und spezialisierten Arithmetik- und Steuereinheiten, die unterschiedliche Aufgaben realisieren. Es gibt aber auch grundlegende Unterschiede, auf die hier kurz eingegangen werden soll.

Ein Smartphone besitzt zwei zentrale RISC-Prozessoren[64] die jeweils für bestimmte Schnittstellen zuständig sind. Der „Application-Processor“ (AP), in der Regel eine ARM-Architektur[65], übernimmt die zentrale Steuerung unter einem Betriebssystem wie zum Beispiel Android, iOS oder Windows Phone.

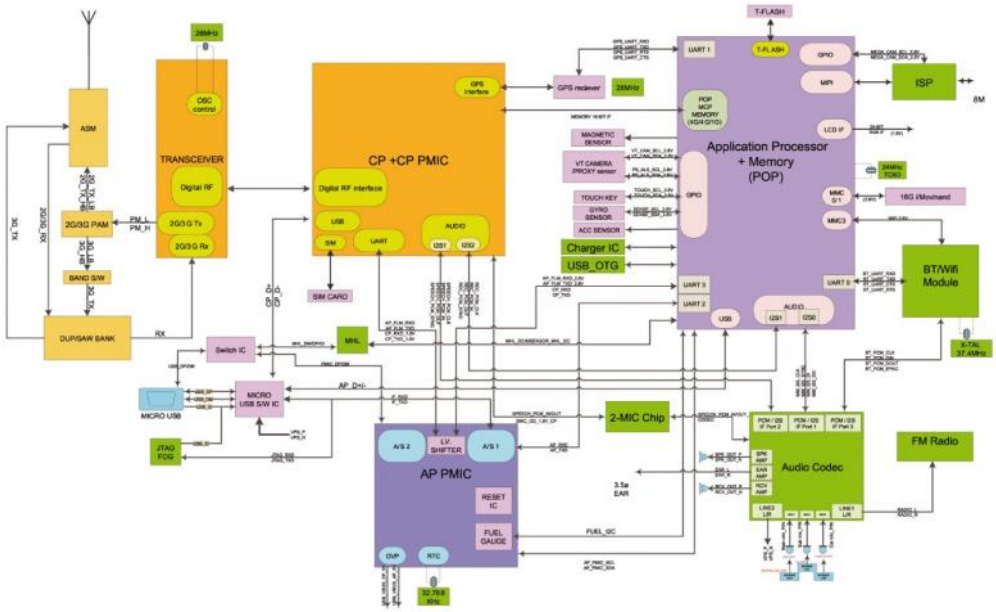


Abbildung 22: Blockdiagramm Samsung S2 Quelle: Samsung GT-i9100 Service Manual

Der „Baseband Processor“ (BB) ist für die Echtzeitverarbeitung der Sende- und Empfangseinheit und der Sprachcodierung für den Mobilfunk zuständig und wird deshalb mit einem „Realtime Operating System“ (RTOS) betrieben. Dieser Bereich ist über die Luftschnittstelle zugänglich und direkt mit der SIM-Kartenschnittstelle verbunden, wie in Abbildung 22 und 23 zu sehen ist. So entsteht ein autonomer Teilbereich, der auch als Radio oder Modem bezeichnet wird.

[64] Reduced Instruction Set Computer: Der vereinfachte Befehlssatz dieses Designs, ermöglicht einen geringeren Stromverbrauch gegenüber CISC-Systemen (Complex Instruction Set Computer).
[65] Advanced RISC Machines, wird als Lizenz von der Firma „ARM Limited“ an verschiedene Chip-Hersteller verkauft.

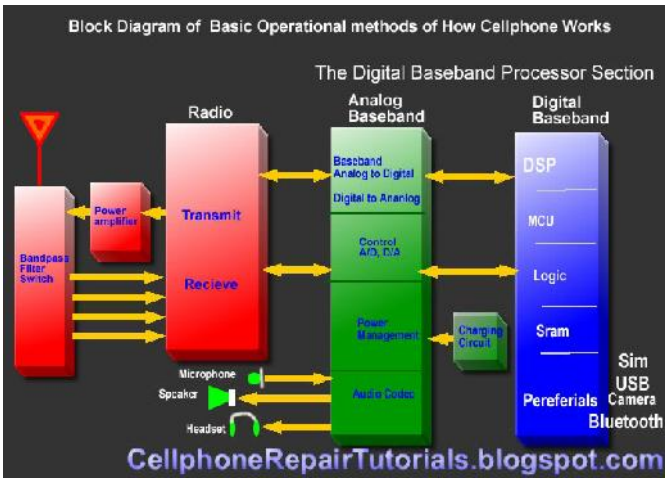


Abbildung 23: Arbeitsweise des BP

Quelle: Cellphone Repair Tutorials.blogspot.com

2.3.1. Sende- und Empfangseinheiten für den Mobilfunk

Die Angriffsmöglichkeiten auf der U_m und U_u Luftschnittstelle zwischen Smartphone und Basisstation wurde bereits im Kapitel 2.1. beschrieben. Ein Angriff könnte aber auch direkt über den RF-Empfänger auf das Smartphone erfolgen. Hierdurch könnte die SIM-Karte manipuliert werden, wie im folgenden Abschnitt „SIM- und USIM-Smartcard“ beschrieben wird.

Angriffsmethoden auf den Baseband-Prozessor werden in den letzten Jahren immer häufiger veröffentlicht. Zunächst muss eine Verbindung zum Smartpone hergestellt werden. Hierfür gibt es bekannte Lösungen, die bereits im Abschnitt „IMSI-Catcher“ beschrieben wurden. Anschließend wird durch das sogenannte „Baseband-Fuzzing[66]“ versucht, ein ungewöhnliches Verhalten oder Systemabstürze zu provozieren. Auch das „Reverse Engineering“ kann Aufschluss über Schwächen und Fehler eines Systems geben, wie es in verschiedenen Untersuchungen beschrieben wird[67]. Des Weiteren gibt es das „Flooding“, um das Mobilfunknetz oder die SIM-Karte mit Anfragen zu überlasten[68]. Da es nur relativ

[66] Professor Barton Miller, Universität von Wisconsin-Madison, 1989 entwickelte die als Fuzzing bekannte Methode. Hierzu werden manipulierte oder zufällige Datenpakete an einen Empfänger gesendet, um so Sicherheitslücken (Exploits) aufzudecken.
[67] Ralf Philipp Weinmann „All your Baseband are belong to us“, 2011 und “Baseband Attacks: Remote Exploration of Memory Corruptions in Cellular Protocol Stacks”, USENIX Workshop 2012
[68] Grugq “Base Jumping – Attacking the GSM baseband and base Station“, 2010 http://bit.ly/9LaMMd [08-2012]

wenig Hersteller[69] von diesen Modulen gibt, würde ein Fehler in der Firm- oder Hardware eine Reihe von Geräten treffen.

Einen einzelnen Angriffsvektor zu formulieren ist jedoch nicht einfach, weil immer erst eine gerätespezifische Schwachstelle gefunden werden muss. Jedoch gibt es eine Reihe von grundlegenden Funktionsweisen, die für spätere Erkennungs- und Abwehrstrategien interessant sein könnten.

[AV-E01] Diese Recheneinheit besitzt umfassende Zugriffsrechte auf alle Speichereinheiten und Sensoren. Im „Privileged Mode“ kann sie die Kontrolle über das Smartphone erhalten. Dokumentationen zu diesen Prozessoren oder gar sicherheitsrelevante Informationen werden nicht veröffentlicht (Security By Obscurity). Angriffe könnten aber auch vom AP aus erfolgen, was im Zusammenhang mit dem verwendeten Smartphone Betriebssystem untersucht werden muss.

[AV-E02] Die als „Roving-Bug“ bekannte Angriffsmethode wurde im Jahre 2006 das erste Mal offiziell eingesetzt[70]. Hierbei wird das Mikrofon des Mobiltelefons aktiviert und die Audiosignale an einen Server übertragen. Wie dieser Vorgang genau realisiert wird, ist aber nicht dokumentiert. Am wahrscheinlichsten ist eine Aktivierung über die Installation von Java-Code auf der SIM Karte. Diese Technik wird in einem Artikel[71] des Fraunhofer-Instituts für Sichere Informationstechnologie (SIT) und auch im BSI-Gefährdungskatalog beschrieben. Wobei der BSI sogar in Betracht zieht, dass schon bei der Entwicklung, also beim Hersteller solche Funktionen implementiert worden sein könnten. Zitat[72]: „*Eine versteckte, nicht dokumentierte Abhörfunktion könnte schon bei der Entwicklung des Gerätes (bewusst oder unbewusst) in die Steuersoftware einprogrammiert sein*“. Eine wissenschaftliche Arbeit über ein „Roving Bugnet[73]“ wurde von Ryan Farley und Xinyuan Wang publiziert.

---

[69] Qualcomm, Mediatek, Texas Instruments und Infineon teilen sich den Großteil des Marktes.
[70] Declan McCullagh "FBI Taps Cell Phone Mic as Eavesdropping Tool", ZDNET (Dec. 1, 2006)
[71] Jens Heider, Rachid El Khayari „Geht Ihr Smartphone fremd? Übersicht der Angriffsvektoren für Geräte im Unternehmenseinsatz“
[72] Bundesamt für Informationstechnik, „Gefährdungskatalog“, Abschnitt G5 Vorsätzliche Handlungen, G5.96 Manipulation von Mobilfunktelefonen, Stand 2005 [08-2012]
[73] Ryan Farley und Xinyuan Wang, „Roving Bugnet: Distributed Surveillance Threat and Mitigation”, 2009

2.3.2. SIM- und USIM-Smartcard

Mit der SIM-Karte[74] beziehungsweise mit der USIM[75] (UMTS- und LTE-Netze), erhält der Nutzer Zugriff auf das Mobilfunknetz. Die Daten und Programme auf der Chipkarte können aus der Tabelle im Anhang entnommen werden. Die eigentliche Schnittstelle der Smartcard besteht aus 8 Kontakten, von denen zur Zeit nur 6 genutzt werden.

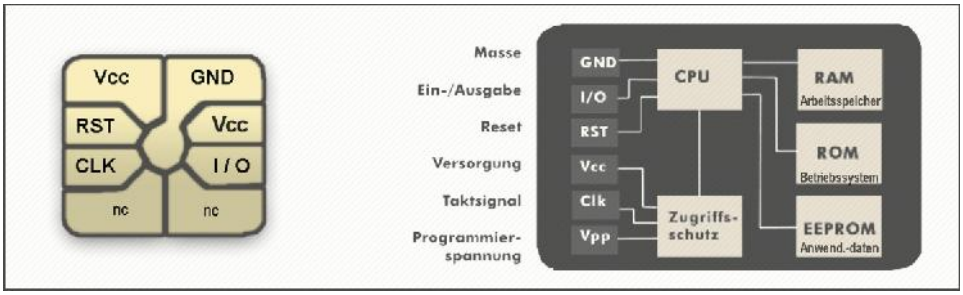


Abbildung 24: Smartcard Schnittstelle und Blockschaltbild

Jede Smartcard verfügt über einen eigenen Mikroprozessor, RAM, ein ROM für das Betriebssystem und ein E²PROM zur Speicherung von Nutzerdaten[76]. Physikalisch kann ausschließlich über die Schnittstelle der CPU zugegriffen werden. Das direkte Auslesen des „Identity Key" Ki ist somit nicht möglich.

[AV-E03] Der Identity Key konnte bei alten Smartcards mit Comp-128-Implementierungen berechnet werden, wenn man im Besitz der Smartcard ist. Mittlerweile gibt es COMP-128 v2 und v3, die als sichere Methode gelten. Das Klonen von SIM-Karten ist somit nur möglich, wenn ein Fehler in der Implementierung gefunden wird, für den der Service Provider verantwortlich ist.

Eine andere technisch sehr aufwendige Methode bekannt als "Differential Power Analysis", wurde von IBM angewandt. Durch Messen des Stromverbrauchs während der Zugriffe konnte Ki berechnet werden.

[74] Spezifikation: ETSI TS 100 977, "Specification of the Subscriber Identity Module – Mobile Equipment (SIM-ME) Interface"
[75] Spezifikation: ETSI TS 102 671, „Smart Cards: Machine to Machine UICC; Physical and logical characteristics (Release 9)"
[76] Siehe Anhang Tabelle A06 Daten der SIM-Karte

Bei dem schon erwähnten „Dynamic SIM-Cloning“ erlangt der MITM-Angreifer auch Zugriff auf eingehende Telefonate. Der IMSI-Attach Vorgang wird hierbei vom „gecatchten“ ME kommend direkt an die „echte“ BTS weitervermittelt. Auch die zurückgesendete Zufallszahl RAND wird wieder direkt weitergereicht, damit die SIM-Karte den gültigen Wert für SRES berechnen kann. Erst wenn dieser Wert der dynamischen SIM-Karte bekannt ist, kann sie die Anmelde-Prozedur an der BTS erfolgreich abschließen. Damit ist der Angreifer dann unter einer falschen Identität am Mobilfunknetz angemeldet und kann auf fremde Kosten Telefonate initiieren. Die zeitliche Verzögerung der IMSI-Attach Prozedur löst normalerweise einen „Timeout“ der „dynamischen“ SIM-Karte aus. In der Master Thesis von Adam Kostrzewa[77] wurde dieser Schutzmechanismus umgangen, indem über die Bluetooth Schnittstelle mit der SIM-Karte kommuniziert wurde.

[AV-E04] Auslesen der Smartcard über die Funkschnittstelle. Kontaktdaten, eventuell SMS und angerufene Nummern sind auf der SIM-Karte gespeichert.

[AV-E05] Das sogenannte „Over the Air“–Verfahren (OTA) ermöglicht das Manipulieren der GPRS-, E-Mail- oder MMS-Einstellungen. Wie schon im Kapitel 2.2. unter SMS und MMS erwähnt kann unbemerkt eine SMS empfangen werden, die vom ME an die SIM-Karte weitergereicht wird. Auch die Installation von Java-Code auf der SIM-Karte ist möglich.

[AV-E06] Bei “Firmware Over The Air” (FOTA) wird eine SMS als WAP-Push gesendet, um ein Firmware-Update auszuliefern. Auch das Ausliefern von Software-Patches wird unterstützt.

[77] Adam Kostrewa „Development of a man in the middle attack on the GSM Um-Interface“, Master Thesis, Technische Universität Berlin 2011

2.3.3. Sonstige Schnittstellen

Bluetooth

Die Bluetooth[78] Schnittstelle verfügt über ein großes Repertoire an Profilen und Protokollen, um die Kommunikation mit unterschiedlichen Geräteklassen wie ISDN-Telefone, Drucker oder Internetrouter zu realisieren. Die Bezeichnungen „Bluejacking“, „Bluesnarfing“, „Toothing“ und „BlueScanner“ beschreiben nur die gängigsten Methoden um sich Zugriff auf fremde Daten zu verschaffen oder um kostenlose Telefonate zu führen.

Bei einer Ad-Hoc-Verbindung zwischen 2 Smartphones erfolgt zuerst das sogenannte „Pairing“, bei dem mittels Challenge-Response-Verfahren ein 128 Bit langer Schlüssel festgelegt wird.

Die Datenverschlüsselung erfolgt dann mit einem Stromchiffre-Verfahren. Von den 128 Bit werden in der Praxis aber nur maximal 84 Bit genutzt. Zusätzlich überträgt Bluetooth mit dem Frequenzspreizverfahren „Frequency Hopping“, um durch ständiges Ändern der Sendefrequenz ein passives Mithören zu erschweren. Mit einem Multifrequenz-Scanner ist eine Aufzeichnung zur späteren Analyse und Entschlüsselung möglich. Die Reichweite kann in der Praxis bis zu 400 Meter betragen.

[AV-E07] Über das Bluetooth-Interface können Anrufe an ein Head-Set, eine Fernsprechanlage oder einen Funkverstärker übertragen werden. Mittels „SIM Access Profile“ (SAP) kann direkt auf die SIM Karte eingewirkt werden. Die meisten Smartphones unterstützen dieses Protokoll jedoch nicht.

[AV-E08] Eine aktivierte Bluetooth-Schnittstelle kann auf viele Arten angegriffen werden. Methoden, die aus dem Bereich der Computertechnik stammen, sind nicht Gegenstand der Untersuchung.

[78] IEEE 802 15.1, “Institute of Electrical and Electronic Engeneers”, Standard der Bluetooth SIG (Special Interest Group), 2,4 GHz Frequenzband

Wireless LAN

Auch im WLAN[79] ist ein MITM-Angriff möglich. Das Interface ist bei den meisten Nutzern aktiviert und verbindet sich automatisch mit bekannten Access Points. Es bestehen ähnliche Risiken wie bei konventionellen Computersystemen. Aber auch mobilfunkspezifische Angriffe sind möglich.

[AV-E09] „Cross-Service Attack" Die Arbeit „Using Labeling to Prevent Cross-Service Attacks Against Smart Phones[80]" demonstriert einen Angriff auf die WLAN Schnittstelle, um das Mobiltelefon aus der Ferne zu steuern und einen Anruf zu initiieren.

Auch der Webbrowser kann direkt auf Sensoren und Schnittstellen zugreifen. Web- Frameworks wie Phone Gap sind mittlerweile dazu fähig, native Funktionen zu nutzen die sonst nur „echten" APPs vorbehalten war.

NFC (Near Field Communication)

Dieser RFID-Chip[81] besteht aus einer Antenne, einem Controller und einem wiederbeschreibbarem Speicher. Das Bauteil kann als passiver Tag sowie als Tag-Reader betrieben werden. Sicherheitsrisiken entstehen zum Beispiel, wenn sich die Kreditkartendaten auf diesem Chip befinden, was eigentlich als hauptsächlicher Einsatzzweck gedacht ist.

[AV-E10] Diese Daten sind weder verschlüsselt noch sind sie durch ein Passwort geschützt und können so theoretisch von jeder Person, die nahe genug an den Chip kommt ausgelesen werden. Auch das Ausführen von Hyperlinks die auf den Chip kopiert werden ist je nach verwendeten Betriebssystem und installierten APPs möglich.

[79] IEEE 802.11a, b, g und n, "Institute of Electrical and Electronic Engeneers", Standard für das 2,4 und 5GHz Frequenzband. "Wireless Local Area Network" oder auch als "Wi-Fi Hotspot" bezeichnet
[80] Collin Mulliner, Giovanni Vigna, David Dagon, and Wenke Lee, "Using Labeling to Prevent Cross-Service Attacks Against Smart Phones", R. Büschkes and P. Laskov (Eds.): DIMVA 2006, LNCS 4064, pp. 91–108, 2006. c Springer-Verlag Berlin Heidelberg 2006
[81] ETSI Spezifikation TS 102 312 v1.1.1. "Near Field Communication Interface and Protocol-2", 2004 und ETSI TS 102 190 v1.1.1. "Near Field Communication (NFC) IP-1; Interface and Protocol (NFCIP-1), 2003-03

Kamera / QR Code

Der QR Code[82] kann bis zu 2953 Byte Daten enthalten, die von der verwendeten Anwendung nach dem Einscannen in einen lesbaren Text umgewandelt wird.

[AV-E11] Der eigentliche Angriffsvektor besteht in dem ausführen des QR-Codes (Quick Response), hinter dem sich ein Webseitenlink oder eine Telefonnummer verbergen kann. Dabei ist es von der verwendeten APP abhängig, ob und wie diese Daten interpretiert werden. Auch das Ausführen von Java-Script ist möglich, wenn er als Link getarnt von der APP an den Browser übergeben wird. Um ein größeres Skript in einen QR Code zu wandeln, können vier Quadrate zu einem einzigen zusammengeführt werden, der dann fast 12 kByte enthalten kann.

Push to Talk over Cellular

Dieser Dienst wurde von der „Open Mobile Alliance“ (OMA) standardisiert. Die Nutzung funktioniert nach dem „Walkie-Talkie-Prinzip“, es gibt also nur eine begrenzte Zahl von Kommunikationspartnern, die sich ein Übertragungsmedium teilen müssen. Die Sprachdaten werden als IP-Pakete über das GPRS-Netz übertragen. Sowohl das Smartphone als auch der Provider müssen den Dienst unterstützen, was in Europa seit 2008 nicht mehr der Fall ist. In Asien und Amerika hingegen ist ein ähnlicher Dienst „Push To Talk“ (PTT) sehr weitverbreitet, der jedoch als iDEN-Bündelfunk realisiert wurde.

Motorola iDEN-Bündelfunk

Diese Schnittstelle wurde von Motorola entwickelt und unter anderem in Blackberry Mobiltelefone integriert. In Deutschland gibt es ein vergleichbares „Terrestrial Trunked Radio“ TETRA-Netz, dass von Behörden und Privatfirmen genutzt wird.

Bündelfunk und PTT werden in dieser Arbeit jedoch nicht weiter untersucht.

---

[82] Standard ISO (ISO/IEC 18004:2006), Die Bezeichnung „QR Code“ ist ein eingetragenes Warenzeichen der Firma „Denso Wave Incorporated“, Japan

2.4. Ortung und Positionsbestimmung

Es gibt drei unterschiedliche Techniken um eine Standortbestimmung durchzuführen: Handset-, Network- und SIM-Based. Hybride Verfahren kombinieren verschiedene Messungen, die im Weiteren beschrieben werden.

Eine überaus genaue Positionsbestimmung über A-GPS nutzt die in Smartphones integrierte GPS-Hardware und die im Mobilfunknetz vorliegende Information über die Satelliten, die an dieser Position empfangen werden können. Bei „GSM Assisted GPS“ werden die Ergebnisse der Messung des Smartphones an die Basisstation gesendet. Im Funknetz befinden sich zusätzliche Komponenten wie das Serving Mobile Location Center[83] (SMLC), Location Measurement Units (LMSC) und Gateway Mobile Location Center (GMLC) um die Location Services (LCS) bei GSM und UMTS realisieren zu können.

Die einfachste, aber auch ungenaueste Positionierungstechnik ist die Zellortung COO (Cell of Origin). Hier werden nur die geografischen Koordinaten der Funkzelle abgefragt, wodurch die Position des ME um 500 Meter bis zu mehreren Kilometern abweichen kann. Der Radius einer Funkzelle kann im Stadtgebiet einige hundert Meter und in ländlichen Gebieten über 20 km betragen und aus einer Vielzahl von BTS bestehen. Die Antennen können auch unterschiedliche Abstrahlwinkel besitzen, was als sektorisierte Basisstation bezeichnet wird.

Des Weiteren kann mit der Signalstärke RSSI (Receiver Signal Strength Indicator) der Abstand zu den Basisstationen berechnet werden. Mit einer Abweichung von etwa 150 Metern ist dieses Verfahren für viele Anwendungen noch zu ungenau.

Ist der Abstand zwischen zwei Stationen bekannt, ist eine Positionierung mit AoA (Angle of Arrival) möglich. Hierzu werden dann nur noch die vom Mobilteil empfangene RSSI Werte der beiden Stationen benötigt.

Die Messung der Signallaufzeiten der einzelnen Basisstationen zum ME ist eine weitere Lösung. Dabei beschreibt die „Round Trip Time“ (RTT) die Zeit, die das Signal von der BTS zum ME und wieder zurück zur BTS benötigt. Dadurch müssen für die Zeitmessung das ME und die BTS nicht synchronisiert werden. Diese

[83] 3GPP TS 04.31 “Serving Mobile Location Centre (SMLC), Radio Resource LCS Protocol (RRLP)”

Technik wird als ToA RTT (Time of Arrival) bezeichnet. Beide Methoden haben eine mittlere Ungenauigkeit von etwa 125 Metern.

Löst anstatt der BTS das Mobilteil das Signal zur Messung aus, spricht man vom „Time Difference of Arrival“ (TDoA). Damit kann die Position bis auf 50 Meter genau berechnet werden. Diese Verfahren können im späteren Teil „Erkennung und Ortung des IMSI-Catchers“ von Interesse sein.

Bei einem Anruf über die Notrufnummer 112 muss der Anrufer unmittelbar und zuverlässig geortet werden. Dies wird mittels den beschriebenen Verfahren oder E-OTD (Enhanced Observed Time Difference)-Messungen realisiert. E-OTD berechnet den zeitlichen Unterschied beim Eintreffen der Broadcasts der Basisstationen beim Mobilteil. Bei UMTS wird das System als „Observed Time Difference of Arrival“ (OTDOA) bezeichnet. Es gibt keinerlei Sicherheitsmechanismen, damit eine sofortige Messung nicht verzögert oder gar verhindert wird.

[AV-F01] Die vom Mobilfunknetz initiierte Ortung dient unter anderem zur Messung der Signalqualität am aktuellen Standort des ME. Auch wenn es sich dabei nicht um einen Angriff handelt, sollte nach einer Erkennungsmöglichkeit gesucht werden.

[AV-F02] Ein weiteres Mittel ist die Standortbestimmung durch eine Abfrage der WLAN Access Points in der Umgebung des Smartphones. Die ermittelten SSIDs können zur Ortung mit Informationen einer Datenbank wie Skyhook[84] verglichen werden. Um als Angreifer an diese Informationen der WLAN-Schnittstelle heranzukommen, kann ein API-Zugriff von einer APP oder eventuell einer Webseite genutzt werden.

[AV-F03] Die Ortung über die IMSI oder IMEI ist mit einem IMSI-Catcher möglich. Der Elaman 3GN[85] kann durch einen „Blind Call“ ein Smartphone orten, auch wenn es in einem „3G only“-Modus betrieben wird. Eindeutige Identifizierungen sind

[84] Quelle: www.skyhookwireless.com [Stand 11.08.2012]
[85] Quelle: „Elaman Newsletter“, Ausgabe 01/2011, Seite 21

aber auch durch die aktivierte WLAN (MAC-Adresse) oder Bluetooth (BD ADDR)-Schnittstelle möglich.

[AV-F04] Die stille SMS kann ebenfalls zur Ortung benutzt werden, wie es im Kapitel 2.2.1. unter [AV-B07] beschrieben ist. Um die Verbindungsdaten auswerten zu können, muss jedoch ein weiterer Zugriffspunkt direkt beim Provider bestehen.

Um zu überprüfen, ob sich das gesuchte Gerät an einem bestimmten Ort befindet, müsste dort der Pagin Channel (PCCH) abgehört werden, wie in der Untersuchung[86] „Location Leaks on the GSM Air Interface" beschrieben ist. Dieser Angriff wurde jedoch nicht mit einer stillen SMS durchgeführt, sondern durch einen Verbindungsaufbau, der kurz vor dem Klingelton abgebrochen wurde.

Das Signalling System No.7 kann auch direkt zur Ortung benutzt werden. Hierzu wird der Request „MAP_SEND_ROUTING_INFO_FOR_SM" an das Kern-Netz des Providers gesendet, das den aktuellen Aufenthaltsort kennen muss. Ein derartiger Angriff ist in einer Präsentation von Tobias Engel[87] im Jahre 2008 auf dem 25th CCC beschrieben worden.

Auf der Software-Ebene ergeben sich weitere Möglichkeiten. Das Betriebssystem verfügt über Dienste die ein Bewegungsprofil anlegen können oder wie im Beispiel IOS4 Positionsdaten im Klartext auf dem Smartphone und auch auf der iTunes Synchronisationsdatei abgelegt hat. Auf diese Daten kann aber vom Mobilfunknetz aus nicht direkt zugegriffen werden.

Auch wenn alle Funktionen wie GPS oder die Herstellerfunktionen zur Geräteortung deaktiviert sind, kann es immer noch anhand seiner IP geografisch geortet werden. Natürlich kann es hier zu größeren Abweichungen kommen, je nachdem ob das Smartphone im Mobilfunknetz oder an einem WLAN Hotspot angemeldet ist.

[AV-F05] Skype ist eine proprietäre VOIP- und Messenger Software, die durch Reverse Engineering und wissenschaftliche Veröffentlichungen zum Teil offen

[86] Denis Foo Kune, John Koelndorfer, Nicholas Hopper, Yongdae Kim „Location Leaks on the GSM Air Interface", 2012
[87] Tobias Engel, „Locating Mobile Phones using SS7", 2008, 25th CCC

gelegt werden konnte. Die sogenannte „deobfuscated[88]“ Skype55-Version ermöglicht es, die verwendete IP Adresse eines Skype-Nutzers zu ermitteln, ohne dass es die Person bemerken kann. Durch die Personensuche und dem anschließenden Profilaufruf wird der Online-Status des Nutzers direkt am Endgerät überprüft. Die anfallenden Verbindungsdaten können in der Debug-Protokolldatei eingesehen werden. Im zweiten Schritt kann die IP über einen der kostenlosen Webdienste lokalisiert werden.

[88] Der Begriff Obfuscator beschreibt die „Verschleierung“ des Quellcodes um Reverse Engineering zu erschweren. Der Deobfuscator ermöglicht die Rückführung in eine für Menschen verständliche Darstellungsform.

2.5 Zusammenfassung

Die untersuchten Angriffsvektoren wurden unter der Annahme zusammengestellt, dass der Angreifer nicht im Besitz des ME ist, mit Ausnahme der im Kapitel „SIM-Karte“ beschriebenen Manipulationsmöglichkeiten [AV-E03] bei SIM- und USIM-Smartcards.

Ein Teil der Angriffe sind nur im näheren Umfeld des ME möglich, andere können theoretisch weltweit von jedem Zugangspunkt aus dem Telefon- und Kommunikationsnetz erfolgen.

Die Bedrohungen lassen sich grundsätzlich in aktive und passive Angriffe unterscheiden. Passive Angriffe lassen sich naturgemäß fast nie erkennen. Sehr wohl kann aber eine Abwehrmaßnahme im Vorfeld möglich sein.

Die Summe von 56 Angriffsvektoren und 4 kombinierten Methoden ist zunächst einmal sehr hoch. Jedoch ist bei insgesamt 7 AVs kein direkter Angriff möglich und 12 AVs befinden sich im Mobilfunknetz, nicht im Smartphone. Die Verbleibenden 44 AVs können eventuell am Smartphone erkannt werden.

Es lassen sich 2 Problembereiche erkennen, für die jeweils eine Gesamtlösung gefunden werden muss.

Erstens alle unter AV-A identifizierten Schwachstellen, die das passive, aktive oder semi-aktive Abhören auf der Luftschnittstelle ermöglichen.

Zweitens alle Gefahren, die im Abschnitt AV-B beschrieben wurden. Diese Angriffe erfolgen in Form von SMS und WAP-Push aus dem Mobilfunknetz.

Der Abschnitt AV-E/SIM-Karte kann in Zusammenhang mit der unter AV-B beschriebenen Gefahren gebracht werden, da ein OTA oder FOTA schon an dieser Stelle erkannt werden könnte.

3 Angriffserkennung

Nachdem die Wirkungsweise der Angriffe beschrieben wurde, werden jetzt die dabei verwendeten Parameter und Variablen sowie deren Lokalisierung innerhalb eines Protokollrahmens identifiziert.

Hierfür werden zuerst die Unterschiede zum OSI-Referenzmodell und die Arbeitsweise der Protokolle im Mobilfunknetz kurz erläutert.

Die untersten zwei Protokollebenen entsprechen der Bitübertragungsschicht und der Sicherungsschicht des OSI-Referenzmodells.

Layer1 ist für die Synchronisation, Messungen der Signalqualität, BCCH Handling und Verarbeitung der TDMA-Rahmen auf den physikalischen Kanälen zuständig.

Der Data Link Layer (DLL) in der zweiten Schicht vermittelt zwischen den physikalischen und den logischen Kanälen der dritten Schicht.

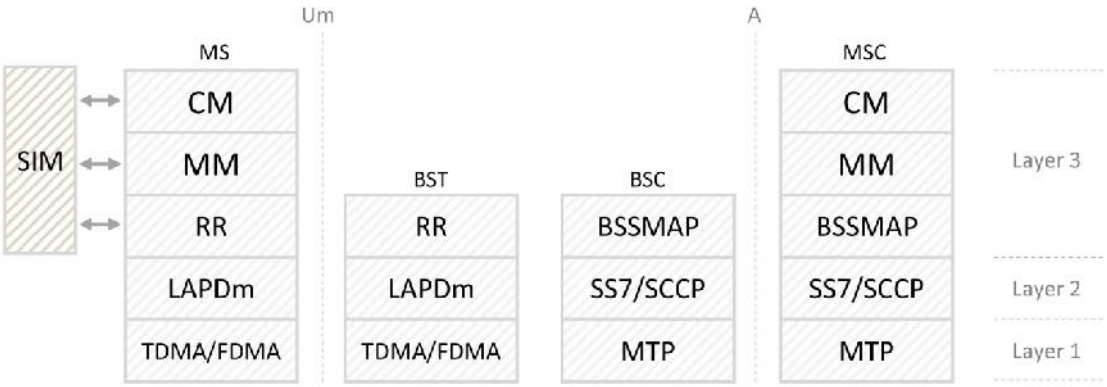


Abbildung 25: GSM Protokoll Schichten 1-3

Der Layer 3 (Signalisierungsschicht) hingegen unterteilt sich in:

- Radio Resource Layer (RR): Auf- und Abbau von dedizierten Verbindungen zwischen MS und BTS.
- Mobility Management (MM): IMSI Attach, Location Update, Periodic Update, Lokalisierungen, zuweisen einer TMSI.
- Connection Management (CM) besitzt drei Instanzen:
    - Call Control (CC)
    - Short Message Service (SMS)

- Suplementary Services (SS) unter anderem für die Gebührenabrechnung

Die dritte Schicht (RR-Layer3) kann auch direkt auf bestimmte Kanäle der Bitübertragungsschicht zugreifen, um zum Beispiel Messungen der Signalqualität oder eine Ortung des MS durchführen zu können. Nur die Daten des MM und CM werden vom BTS und BSC transparent an das MSC weitergereicht.

Die UMTS Protokollschicht unterscheiden sich kaum.

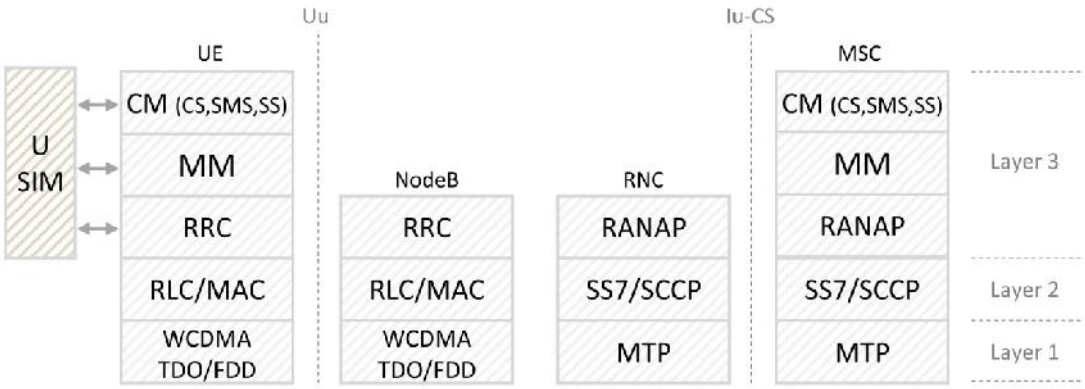


Abbildung 26: UMTS Protokoll Schichten 1-3

3.1. Daten- und Sprachübertragung

Der Themenkomplex „IMSI-Catcher“ und „MITM“ umfasst praktisch alle AVs, die unter „A“ aufgeführt sind. Diese werden im weiteren Verlauf als Angriffsvektoren der „Kategorie A“ bezeichnet.

Die Tabelle „Funktionen der fB-Detection-Software" nimmt alle Funktionen auf, die eine Erkennung ermöglichen könnten. Die dazugehörigen Textstellen werden durch [FBxx] gekennzeichnet.

„fB“ steht für fake Basestation und vereint alle Angriffe durch IMSI-Catcher als auch Semi-Aktive und MITM Impersonation.

3.1.1. Erkennen einer „fake“ Basisstation bzw. eines MITM-Attacks

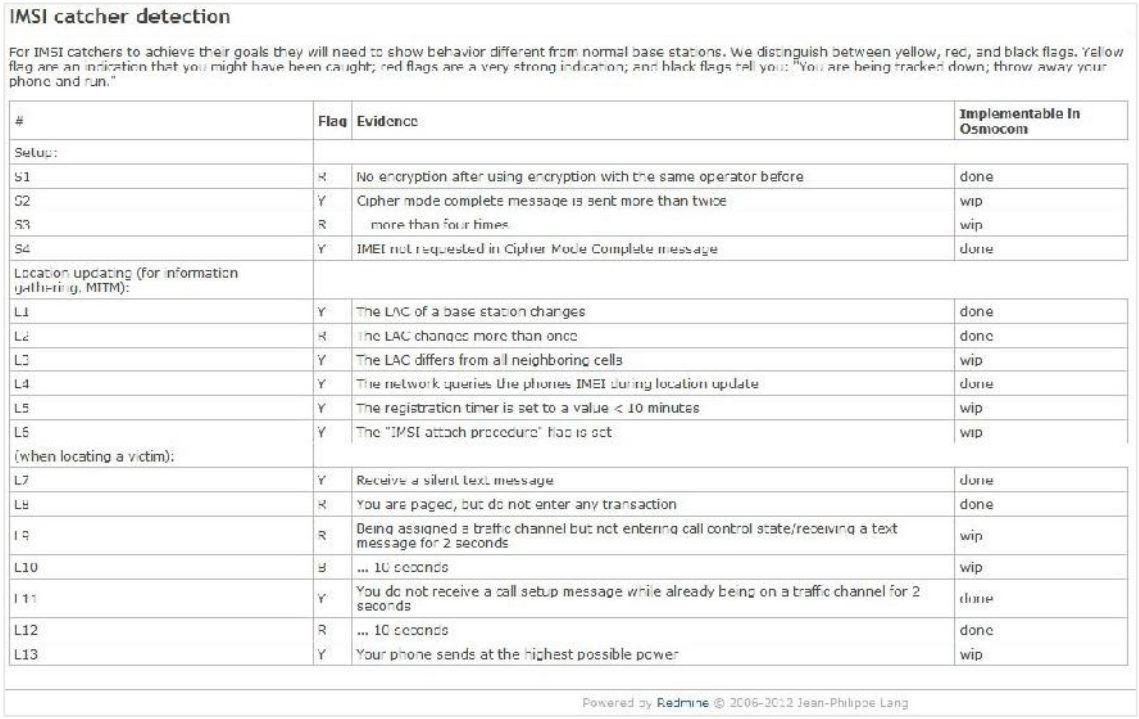
EK-A01 Die Erkennung eines Implementierungsfehlers der Algorithmen A3/A8 ist am Endgerät nicht möglich.

EK-A02 Auch wenn dieser Angriff durch die fehlende „Mutual Authentication“ eine zentrale Bedrohung darstellt, gibt es keine Standardlösung für eine Erkennung.

EK-A02.1 [FB01] Ein grundlegender Ansatz ist die Analyse der vom Funknetz gesendeten Signale auf der Bitübertragungsschicht. Hierdurch können die Informationen (LAI, Cell-ID, RSSI, BSIC, ARFCN, Signal to Noise, Bitfehlerhäufigkeit) im Broadcast Channel BCCH[89] und PBCCH (bei GPRS) ermittelt werden. Es können nur die Stationen des eigenen Providers ermittelt werden. Alle anderen Kanäle können erst ausgelesen werden, wenn sich das ME verbunden hat.

Ein Projekt, das die Arbeitsweisen eines IMSI-Catchers untersucht und eine Reihe von Erkennungsmerkmalen zusammengestellt hat, ist der „Catcher-Catcher[90]“. Die Software wurde unter Nutzung der Open-Source-Software osmocomBB[91] entwickelt und ist leider nicht kompatibel zu den gängigen Betriebssystemen für Smartphones. Die Erkenntnisse aus diesem Projekt können für die Ausarbeitung einer Strategie sehr hilfreich sein, wie die Tabelle auf der nächsten Seite zeigt.

[89] 3GPP TS 45.002 “Radio Access Network; Multiplexing and multiple access on the radio path” (Release 9)
[90] Projekt “Catcher-Catcher”, opensource.srlabs.de/projects/catcher
[91] Projekt “osmocomBB”, bb.osmocom.org/trac/



IMSI catcher detection

For IMSI catchers to achieve their goals they will need to show behavior different from normal base stations. We distinguish between yellow, red, and black flags. Yellow flag are an indication that you might have been caught; red flags are a very strong indication; and black flags tell you: "You are being tracked down; throw away your phone and run."

#	Flag	Evidence	Implementable in Osmocom
Setup:			
S1	R	No encryption after using encryption with the same operator before	done
S2	Y	Cipher mode complete message is sent more than twice	wip
S3	R	... more than four times	wip
S4	Y	IMEI not requested in Cipher Mode Complete message	done
Location updating (for information gathering, MITM):			
L1	Y	The LAC of a base station changes	done
L2	R	The LAC changes more than once	done
L3	Y	The LAC differs from all neighboring cells	wip
L4	Y	The network queries the phones IMEI during location update	done
L5	Y	The registration timer is set to a value < 10 minutes	wip
L6	Y	The "IMSI attach procedure" flag is set	wip
(when locating a victim):			
L7	Y	Receive a silent text message	done
L8	R	You are paged, but do not enter any transaction	done
L9	R	Being assigned a traffic channel but not entering call control state/receiving a text message for 2 seconds	wip
L10	R	... 10 seconds	wip
L11	Y	You do not receive a call setup message while already being on a traffic channel for 2 seconds	done
L12	R	... 10 seconds	done
L13	Y	Your phone sends at the highest possible power	wip

Powered by Redmine © 2006-2012 Jean-Philippe Lang

Abbildung 27: IMSI Catcher Detection, Quelle: Catcher Catcher Projekt Wiki

Die Flag-Zeile gibt mit den drei Signalfarben gelb, rot und schwarz an, wie hoch die Wahrscheinlichkeit ist, „gecatched“ worden zu sein. Diese Tabelle bietet zwar eine gute Grundlage, setzt jedoch voraus, dass alle nötigen Daten direkt am Sende-/Empfangsteil des ME ermittelt werden können. Außerdem muss das ME mit der potentiell „falschen“ Basisstation verbunden sein, um diese Merkmale feststellen zu können.

Der Angriff hat aber schon begonnen, bevor die Verbindung zu Stande gekommen ist. Typische Ereignisse, wie zum Beispiel ein plötzlicher Anstieg der Sendestärke oder der Empfang einer stillen SMS, könnten einen Prozess anstoßen, der Anomalitäten und so den Angriffsvorgang als Ganzes erkennt. Auch unter Berücksichtigung des Energiebedarfs wäre bei einer späteren Realisation als Software eine Aufteilung in einen Standby-Modus und einen aktiven Modus sinnvoll.

[FB02] Der Angreifer hört zuerst den Broadcast Channel der verfügbaren BTS ab, um dann die Identität der schwächsten BTS zu übernehmen. Deshalb kann auch ein plötzlicher Anstieg des RSS-Wertes einer BTS ein erster Indikator sein. In diesem Fall würde sich die Signalstärke um ein Vielfaches erhöhen.

[FB03] Professionelle fB benutzen „originale“ Zellen IDs und führen auch eine Tabelle aller Nachbarzellen, was eine Erkennung erschweren soll. Die Nachbarschaftstabelle in der fB täuscht dem ME vor, dass es kein stärkeres Signal einer fremden BTS gibt und veranlasst das ME, mit der fB verbunden zu bleiben. Dieser Unterschied könnte durch eine Plausibilitätsprüfung zur Erkennung genutzt werden. Jedoch führen viele Provider gar keine BCCH_ARFCN_NC(n)-Tabelle in den Basisstationen.

[FB04] Auch wenn das ME mit der fB verbunden ist, muss die falsche Basisstation weiterhin ihren Broadcast senden, damit sich das abgehörte ME nicht an einer anderen Basisstation anmeldet. Alle ME in der Umgebung versuchen sich ebenfalls über den PRACH zu verbinden, bekommen aber auch nach mehrmaliger Anfrage kein „Assignment“ zurückgesendet. Es kommt also keine Verbindung zustande. Je nachdem wie umfangreich die Abhöreinrichtung des Angreifers ausgestattet ist, müssten alle anderen ME abgewiesen werden, weil für sie nicht genügend Verbindungen zum Telefonnetz bereitgestellt werden können. Dieses Verhalten würde bei allen Geräten (bzw. IMSIs) auftreten, die vom Angreifer bereits als „uninteressant“ eingestuft wurden. Wenn das gesuchte Endgerät bereits identifiziert wurde, könnte dieses Merkmal häufiger auftreten.

Eine aufwendige, wenn auch effektive Lösung ist in dem Patent mit dem Namen „MAN-IN-THE-MIDDLE DETECTOR AND A METHOD USING IT[92]“ beschrieben. Dieses System erstellt einen geografischen Fingerabdruck von jeder Basisstation, die sich im Empfangsbereich befindet. Die ermittelten Daten werden abgespeichert, um spätere Veränderungen gegenüber dem originalen Fingerprint zu erkennen. Nachdem die Grundfunktionen der fB-Software implementiert wurden, könnte in einem zweiten Schritt ein ähnliches Verfahren für eine verbesserte Erkennung verwendet werden. Danach müsste man sich dann nicht mehr erst verbinden, um eine Erkennung zu ermöglichen.

Zusätzlich zur dieser eher physikalischen Herangehensweise gibt es auch einen geografischen und einen informellen Lösungsansatz.

[92] Jukka Lotvonen, Juha Kumpula, Markus Ahokangas und Janne Pauna; Patent US 2009/0104889A1, “MAN-IN-THE-MIDDLE DETECTOR AND A METHOD USING IT”, 23.04.2009

EK-A02.2 Die falsche Basisstation muss möglichst nahe an dem abzuhörenden Mobiltelefon positioniert werden. Dafür sind zwei Tatsachen verantwortlich: Je näher sich die fB an der „originalen“ BTS befindet, desto mehr Sendeleistung benötigt sie, damit sich das MS für die fB entscheidet. Je größer die Sendeleistung und damit der Empfangsradius ist, desto mehr ME könnten gestört werden und zeitweise nicht mehr für das Mobilfunknetz erreichbar sein. Damit kann von zwei unterschiedlichen Positionen von zwei identisch erscheinenden BTS ausgegangen werden.

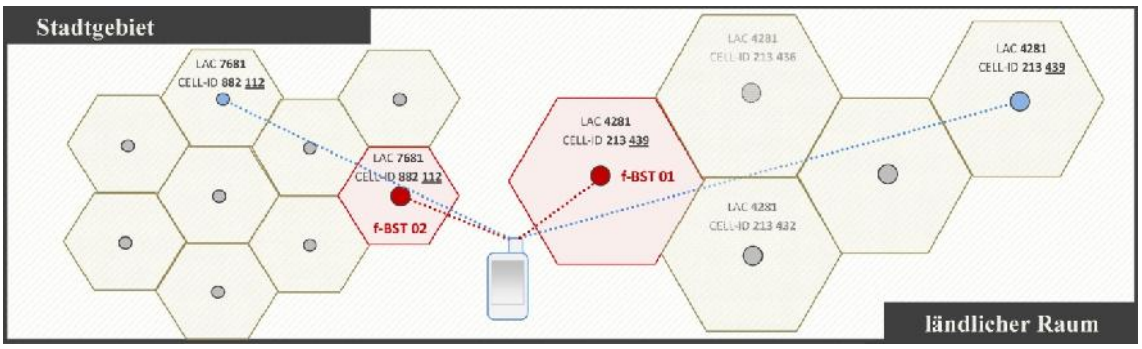


Abbildung 28: Differenz zwischen falscher und echter BTS; Quelle: Die Werte sind mit G-MoN (Android APP) Ermittelt worden.

[FB05] Über den Abstand zwischen dem Smartphone und einer BTS könnte eine Messung des RSSI-Wertes Auskunft geben. Laut Untersuchung von Kiran G.S, Bhoolakshmi M und G. Varaprasad[93] kann über ein sogenanntes „Hello Packet-Delay“, das an die BTS gesendet wird, eine Abstandsmessung zwischen dem ME und einer Basisstationen erfolgen. Ein plötzlicher Anstieg der Signalstärke (wie unter EK-FB01) würde in dieser Darstellung als eine Verkürzung des Abstandes zwischen ME und Basisstation interpretiert werden.

[FB06] Ein weiterer Ansatzpunkt könnte die TDoA oder die E-OTD-Lokalisierung bieten. Auffälligkeiten wie zum Beispiel eine BTS, die nicht antwortet oder zwei Antworten einer BTS könnten Aufschluss über eine fB geben. Ein professionelles Mittel, um alle Mobilfunkstationen in der Umgebung zu ermitteln, bietet die Firma

[93] Kiran G.S, Bhoolakshmi M und G. Varaprasad “Algorithm for Finding the Mobile Phone in a Cellular Network“, 2007

Rohde & Schwarz[94]. Leider sind keine Einzelheiten über die genaue Funktionsweise dokumentiert.

[94] Rohde & Schwarz, Produktkataloge: „Automatic BTS localization for 2G and 3G mobile radio networks, TSMX-PPS, TSMQ, TSMU, TSML und die Software ROME S4

EK-A02.3 [FB07] Ein echter Vorteil kann durch das Zusammenwirken von mehreren ME und das Teilen der ermittelten Daten untereinander entstehen, was als „Informelle Ebene“ zusammengefasst wird.

Die Position und Identität der Basisstationen kann mit frei zugänglichen Standortinformationen im Internet verglichen werden. Die Datenbank der Bundesnetzagentur könnte hierzu die nötigen Informationen bieten. Leider stellt die Agentur nur eine Kartenansicht[95] zur Verfügung. Des Weiteren gibt es verschiedene Open-Source-Datenbanken sowie kostenpflichtige Angebote.

Zwei Projekte, die als Datenstamm in Frage kommen würden, sind openCellID[96] und Opensignal[97]. Mit OpenCellID (Creative Commons License) wurden schon viele Projekte realisiert und es gibt eine API-Schnittstelle für Datenbankabfragen. Der Download einer RAW-Datei mit allen verfügbaren Standortdaten ist ebenfalls möglich. openSignal hingegen verfügt über eine relativ große Community, die mit der frei erhältlichen Smartphone App die Informationen der Datenbank aktuell hält.

Zwei speziellere Varianten des Angriffs sollen auch in die Erkennung mit einbezogen werden:

[FB08] Durch das „dynamic SIM-Cloning“, kommt es zu einer Verzögerung beim Authentifizierungsvorgang. Die SIM Karte erwartet während der Challenge Response eine unmittelbare Antwort vom Mobilfunknetz, ansonsten wird der Vorgang abgebrochen. Manipulationen können durch folgende Merkmale aufgedeckt werden: bei größeren Abweichungen gegenüber dem statistischen Mittelwert für die Dauer des Vorgangs oder durch das Zählen der missglückten Authentisierungsversuche.

[FB09] Eine weitere Gruppe von Abhöreinrichtungen sind die Semi-Aktiven, die sich nicht direkt zwischen den Verbindungspartnern befinden, sondern den Datenstrom passiv entschlüsseln, wie in AV-A06 und AV-A11 beschrieben ist. Eine Erkennung wird erst durch den aktiven Teil der Station möglich. Da sich der A5/1 leicht entschlüsseln lässt versucht der Angreifer dafür zu sorgen, dass das

[95] Kartenansicht der Sendestationen, emf2.bundesnetzagentur.de/karte.html [28.08.2012]
[96] OpenCellID, Open-Source Datenbank inkl. API, siehe: opencellid.org [28.08.2012]
[97] Opensignal, Weltweite Mobilfunkabdeckung, siehe: opensignal.com [28.08.2012]

Smartphone mit einem 2G Netz verbunden bleibt. Dies kann mit einem „Fall-Back to GSM“ (A10) und eventuell sogar durch einen Hand-Over zu 2G (A09) im „Dedicated Mode“ ermöglicht werden.

EK-A03.1 Die IMSI wird bei den drei Verfahren IMSI-Attach, Location Update und Periodic Location Update im Klartext gesendet. Das Verhältnis zwischen der Anzahl von versendeten IMSIs und TSMIs sollte nicht stark von einem statistischen Mittelwert abweichen. Dieses Verhältnis beträgt „1 zu 9“ in der schon erwähnten Untersuchung von Denis Foo Kune „Location Leaks on the GSM Air Interface“[98] aus dem Jahre 2012. Weitere Datenerhebungen stehen noch aus, um die Praxistauglichkeit beurteilen zu können.

Table 1. General observations on the GSM PCCH

	T-Mobile LAC 747b	AT&T LAC 7d11
Paging Requests - IMSI	27,120	8,897
Paging Requests - TMSI	257,159	84,526
Paging Requests Type 1	284,279	91,539
Paging Requests Type 2	1635	26
Paging Requests Type 3	0	1
Immediate Assignments	207,991	10,962
Observation period	24 hours	24 hours

Abbildung 29: Verhältnis IMSI und TMSI

Quelle: Denis Foo Kune, John Koelndorfer, Nicholas Hopper, Youngdae Kim, “Location Leaks on the GSM Air Interface“, siehe: 4.1 Measurement Platform

Das Zeitintervall, zwischen dem ein „Periodic Location Update“ stattfindet, wird vom Provider auf der SIM Karte gespeichert. Durch Verlängerung des Intervalls oder durch das Blockieren des Location Updates kann erreicht werden, dass die IMSI möglichst selten gesendet werden muss.

Das Mobilfunknetz versucht immer, das ME zuerst in der letzten bekannten Zelle zu suchen. Erst wenn das MS dann nicht erreichbar wäre, würden alle weiteren Anrufer die Auskunft erhalten, dass der Teilnehmer zurzeit nicht erreichbar ist. Jetzt muss das ME erst wieder ein Location Update durchführen, bevor Anrufe wieder an diese Zelle weitergeleitet werden.

[98] Denis Foo Kune, John Koelndorfer, Nicholas Hopper, Youngdae Kim, “Location Leaks on the GSM Air Interface”, 2012

Das Verhalten verfälscht jedoch die Werte, die zur Berechnung unter EK-A03.1 und A03.2 benutzt werden. Dieser Modus sollte nur in Ausnahmesituationen gewählt werden. Die Protokollierung für die statistische Auswertung sollte währenddessen deaktiviert sein.

EK-A03.2 [FB10] Die ermittelten Werte sollten jedoch in Zusammenhang mit der geografischen Position gebracht werden, wodurch ebenfalls ein „Fingerprint" angelegt werden kann. Das häufige Abfragen der IMSI kommt nicht nur bei der Verwendung eines IMSI Catchers vor, sondern auch bei der Ortung von mobilen Endgeräten.

EK-A04 [FB11] Der Einsatz eines Jammers könnte durch das Auftreten von plötzlichen Frequenzstörungen bzw. der Verringerung des Signal-Rauschabstands erkannt werden. Eventuell wird nur das zwischen 1900 – 2200 MHz liegende UMTS-Frequenzband gestört, um die mobilen Endgeräte zu einem Verbindungsversuch mit einer 2G Basisstation zu zwingen. Eine Warnung könnte auf dem Display ausgegeben werden.

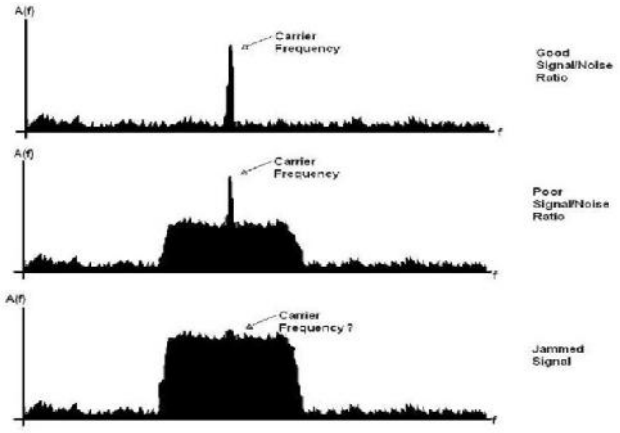


Abbildung 30: Frequency Jamming

Quelle: NSA „Mobility_Capability_Pkg_Vers.1.1[99]", Seite 49, Kapitel 4.5.5

EK-A05 [FB12] Dieser AV zeigt, dass auch die NodeB und bei LTE-Netzen die eNodeB in der Datenbank mitgeführt werden sollten. Bei einer Femtozelle könnte eine Warnung ausgegeben werden, dass es sich um eine Basisstation handeln kann, die sich im Privatbesitz befindet.

[99] National Security Agency, Secure VoIP, "Mobility_Capability_Pkg_Vers.1.1", 2012

3.1.2. Verbindungsverschlüsselung

EK-A06 Das passive Abhören auf der Luftschnittstelle kann nicht erkannt werden.

EK-A07 Der Cipher-Indikator könnte für eine Erkennung sehr hilfreich sein. Es gibt neben der schon beschriebenen Methode laut GSM-Standard eine andere Möglichkeit, den verwendeten Algorithmus zu ermitteln. Direkt nach der IMSI-Attach-Prozedur gibt das MSC die Verschlüsselung vor. In Abb. 5 ist der Verbindungsaufbau mit einem Catcher zu sehen. Auch hier wird im „Cipher Mode Command" der Algorithmus vom Netzwerk vorgegeben. Der Catcher blockiert es und sendet stattdessen „No Ciphering" an das ME. Zu beachten ist, dass auch während des Telefonierens der Algorithmus geändert werden kann.

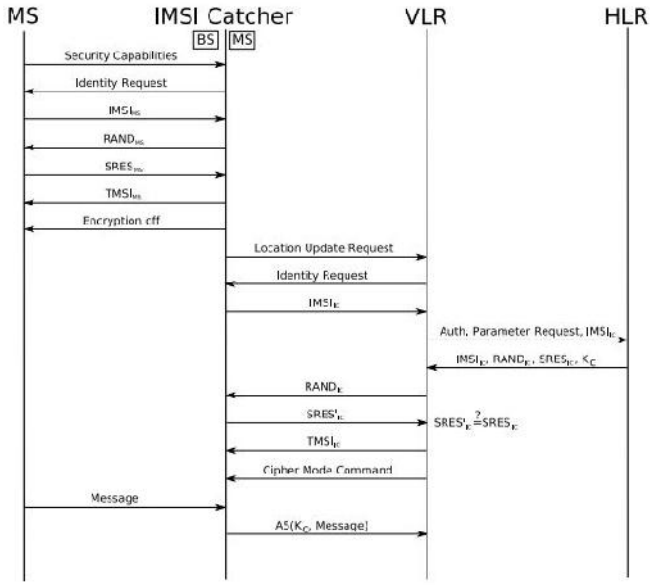


Abbildung 31: Blockieren des Cipher-Modus

Quelle: Daehyun Strobel, „IMSI Catcher", 2007[100]" Figure 4.1

Die Kommunikation findet, wie auch bei den zuvor genannten Variablen, in der zweiten (LAPDm) und der dritten Netzwerkschicht statt, die sich auf 3 Ebenen weiter aufteilt. Details zu den Protokollschichten werden in der Zusammenfassung besprochen.

EK-A08: Die Erkennung ist nicht mit Standardmitteln möglich. Nur auf den unteren Protokollebenen, direkt an der Schnittstelle kann eine Erkennng stattfinden.

[100] Daehyun Strobel, „IMSI Catcher", Seminararbeit Ruhr-Universität Bochum, 2007

3.1.3. GSM/UMTS Hand Over und Fallbackt to GSM

EK-A09 Ein Hand-Over stellt an sich keinen Angriff dar. Dennoch kann der Vorgang genutzt werden, um eine aktive Verbindung zu „hijacken“. Weil dieser Angriff nur während des Telefonierens auftreten kann, kann ein akustisches Signal bei einem Hand-Over in ein niedrigeres Netz informieren. (3G>2G) Eine Erkennung kann durch das regelmäßige Abfragen (Polling) des aktuellen Mobilfunksystems realisiert werden.

EK-A10 „Fall-Back to GSM“. Diese Funktion wird zum Beispiel von Semi-Aktiven Monitoring Systemen[101] benutzt, um das Opfer zu einer Verbindung mit einem 2G-Netz zu zwingen. Der aktive Teil des Systems kann hierzu auch ein „Paging Request“ senden, damit das Smartphone auf die eingehende Verbindung wartet und mit der BTS verbunden bleibt [FB09].

3.1.4. GPRS Core Network

EK-A11: Das Abhören der Datenverbindung auf der Luftschnittstelle kann nicht erkannt werden.

EK-A12: GEA/0 bei Datenverbindungen muss auf dem Display angezeigt werden, ähnlich wie es unter dem Punkt A07 für Sprachverbindungen beschrieben ist.

3.1.5. Zusammenfassung

Die Erkennung von Angriffen der Kategorie A kann durch die Analyse der drei Ebenen ermöglicht werden:

- A02.1 physikalische Ebene
- A02.2 geografische Ebene
- A02.3 informelle Ebene

Die ermittelten Daten müssen in ein Bewertungssystem überführt werden. Für jede BTS wird ein Score-Wert geführt, der die Wahrscheinlichkeit widerspiegelt, dass es sich um eine maskierte Basisstation handeln könnte.

[101] Siehe Webshop: www.grandicelli.it, Produkt: SCL 5020SE, Semi-Active GSM Monitoring System

Jedes Merkmal das in der Tabelle „Funktionen der fB-Detection“ aufgeführt ist erhält einen Wert zwischen 10-50 Punkten, wobei 50 Punkte immer noch dem Flag „yellow“ der Catcher-Catcher Tabelle entspricht. Ein Scoring von 51 bis 99 Punkte entspricht einem Flag „red“.

Das folgende Zustandsdiagramm beschreibt den Ablauf einer Erkennung mit Hilfe der zuvor beschriebenen Funktionen. Im „Listening“-Zustand findet eine Kontrolle statt, die möglichst ressourcenschonend im Hintergrund laufen kann. Das „Ereignis Typ1“ ändert den Zustand zu „Attention“, worauf die aktive Erkennung gestartet werden kann. Am Ende steht der Benutzer vor der Entscheidung, wie er sich im weiteren Verlauf verhalten möchte.

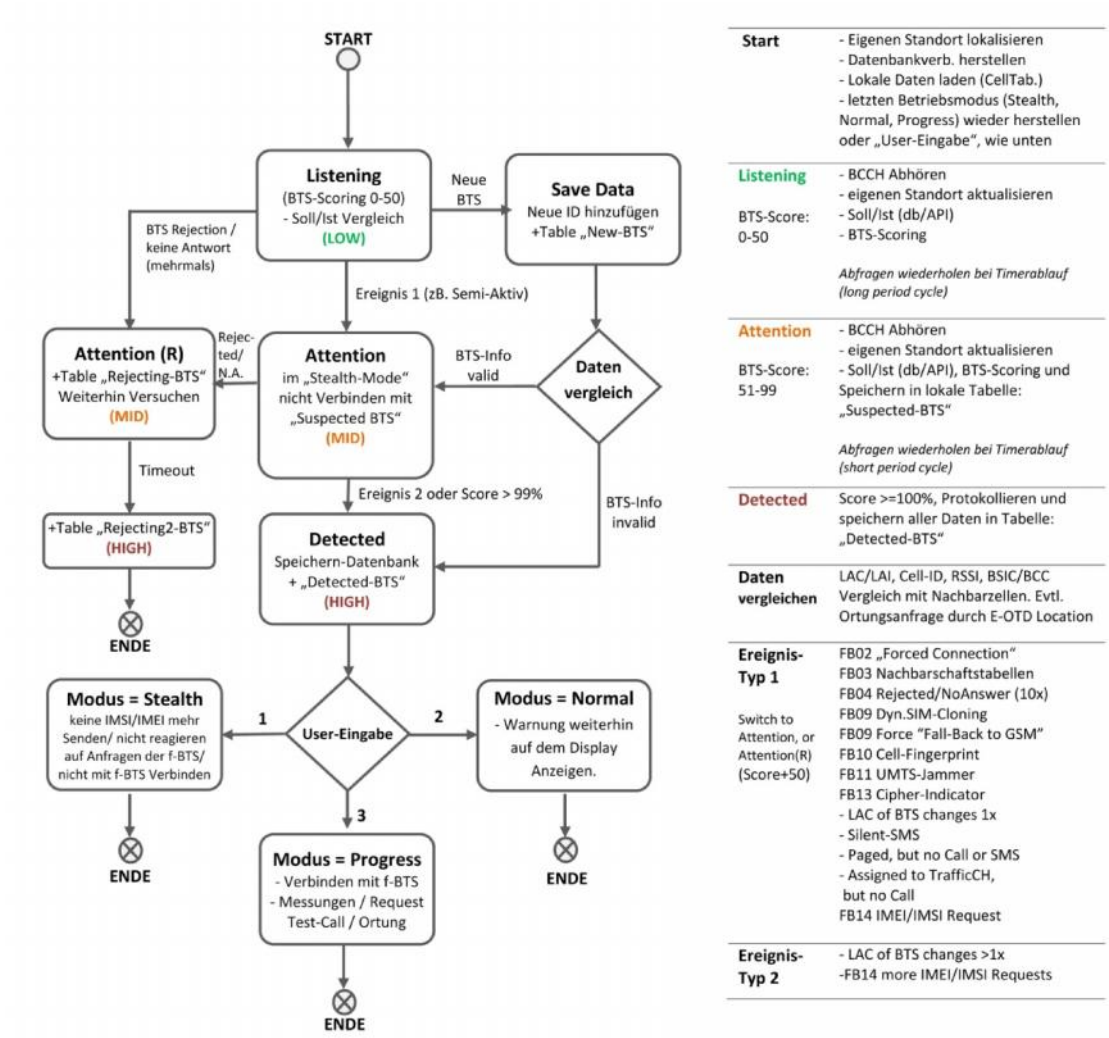


Abbildung 32: Zustandsdiagramm fB-Detection Software

3.2. SMS, MMS und Signalisierungen im Telefonnetz

Die Angriffsvektoren B01 bis B14 werden unter dem Begriff „Kategorie B“ zusammengefasst.

3.2.1. SMS Kurznachrichten

Generell sind bei allen eintreffenden SMS-Nachrichten die Felder „ Message Type Indicator“ (TP-MIT), „Protocol Identifier“ (TP-PID) und „Data Coding Scheme“[102] (TP-DCS) interessant, die im hexadezimalen Zahlensystem repräsentiert werden. Der Protocol Identifier schreibt unter anderem vor, ob es sich um eine Nachricht für den Nutzer handelt oder um Steuercodes für das Endgerät. Im Coding Scheme ist die Zeichenkodierung angegeben, in dem der Inhalt der Nachricht dargestellt werden muss. Zu unterscheiden sind die „CS-SMS“ und „PP-SMS“, je nachdem ob sie über die Leitungs- (CS) oder die paketvermittelte (PP) Verbindung übertragen werden. „SMS-CB“ sind Cell-Broadcast-Nachrichten, die an alle Endgeräte einer Funkzelle gesendet werden.

Die Angriffsvektoren **B01, B02**, **B03** und **B04** sind systembedingt, hierfür ist keine Erkennung notwendig. Die Identifizierung des wirklichen Absenders einer SMS-Nachricht ist am Smartphone nicht möglich. Nur der Provider könnte anhand der Verbindungsdaten den Absender zurückverfolgen.

EK-B05 Wird der WAP-Push-Link über den leitungsvermittelten Teil übertragen, beinhaltet er eine SMS, wodurch eine Erkennung mit den gleichen Mitteln möglich ist, wie es später unter EK-B06 und EK-B07 beschrieben wird.

Wird diese Dienstnachricht paketvermittelt, als Service-Indication- (SI) oder Service-Load- (SL) WAP-Push gesendet, muss die IP-Adresse des Empfängers bekannt sein, was nur bei einer aktiven Datenverbindung der Fall ist. Der Empfang von SL-WAP-Push ist bei vielen Geräten bereits in den Werkseinstellungen des Clients deaktiviert[103].

---

[102] Siehe Anhang Tabelle „Codierungsgruppen des DCS“
[103] WAP-Forum, “Service Loading – Wireless Application Protocol (WAP-168-ServiceLoad-20010721-a)”, 31.07.2001

Die Analyse der eintreffenden Daten müsste erst von einem „Intrusion Detection System“ (IDS) durchgeführt werden. Eine Smartphone-Firewall-Applikation könnte verdächtige Nachrichten, die über die Datenverbindung eintreffen, filtern. Sinnvoller wäre es dieses System im Providernetz zu platzieren, um die ohnehin beschränkten Ressourcen der Smartphones zu schonen.

Ob es sich um einen vertrauenswürdigen Link handelt, der im WAP-Push gesendet wurde, ist nicht ohne weiteres feststellbar. Die Lösung könnte in einem Spam-Filter bestehen, wie er bei E-Mail- Diensten eingesetzt wird.

EK-B06 Eine Flash-SMS sollte sich optisch deutlich von allen anderen Pop-up-Fenstern unterscheiden, wie sie zum Beispiel bei Systemmeldungen oder Benachrichtigungen auf dem Home-Bildschirm erscheinen, damit sie nicht für Phishing-Attacken genutzt werden kann. Der Text einer Flash-SMS muss im Unicode-Zeichensatz codiert sein und die Message Class „0“ besitzen. Beides wird im „TP-DCS“ Feld mit dem hexadezimalen Wert 0x18 angegeben. Anhand dieser PDU-Message ist die spätere Erkennung beim Empfänger möglich.

EK-B07 Die Stille SMS kann ebenfalls durch die PDU-Message erkannt werden, die auch in diesem Fall 16-Bit-kodiert ist und im „TP-DCS“ Feld den Wert „0xC0“ besitzt, damit die eingegangene Nachricht nicht auf dem Display angezeigt wird.

EK-B08 Die SMS-Injection kann nur anhand der schon erwähnten PDU-Analyse erkannt werden.

EK-B09 Das SMS-Botnet könnte ebenfalls anhand der PDU-Message enttarnt werden. Alle ein- und ausgehenden Nachrichten würden dann dem Nutzer angezeigt werden.

3.2.2. USSD und GSM Steuercodes

Die Steuer Codes dürfen vom Betriebssystem nicht automatisch ausgeführt werden. Die Erkennung muss in diesem Fall für jede Art von automatisch ausgeführtem Code erfolgen.

3.2.3. MMS Nachrichten

Die Sicherheitsmerkmale **B10** bis **B11** fehlen bei den von Providern angebotenen MMS-Diensten.

EK-B12 Smartphones unterstützen WAP 2.0, wobei auch die Gegenstelle über den Standard verfügen muss, wenn eine sichere Verbindung zustande kommen soll.

Eine Firewall-APP im Endgerät könnte zusätzlichen Schutz bieten.

Eine Erkennung von Angriffen, die auf das Gateway des Providers erfolgen, ist nicht möglich.

EK-B13 Ähnlich der SMS-PDU-Analyse könnten auch MMS-Nachrichten anhand der sogenannten „M-Retrieve.conf"-PDU[104] analysiert werden. Die eigentliche Gefahr geht bei einer MMS aber eher vom Inhalt der Nachricht aus, als von ihrem Header.

Der Aufruf einer Webseite oder einer anderen APP sollte abgefangen werden. Zur Erkennung von Schädlingen kann eine Anti-Virus-Software für Smartphones eingesetzt werden, die bereits von verschiedenen Anbietern verfügbar ist.

EK-B14 Das schnelle Entladen des Akkus müsste dem Nutzer signalisiert werden. Mit einem festgelegten Abfrage-Intervall und der durchschnittlichen Entladungszeit könnten ungewöhnlich große Abweichungen erkannt werden.

In diesem Fall könnte auch die Firewall die ständigen Zustellungsversuche am UDP-Port erkennen und blockieren.

AV-B15 Eine geeignete Firewall und Anti-Virus-Software kann auch hier zur Erkennung eingesetzt werden.

[104] OMA WAP MMS Encapsulation Protocol V1.1. Kap. 6.3. "Retrieval Of Multimedia Message"

3.2.4. Signalisierungen im Mobilfunknetz

Die Netzwerkkomponenten, die aus Eigeninteresse des Service Providers besonders abgesichert werden, sind das OMC (Operating & Maintance Center), HLR, VLR und MSC. Diese Sicherheitsvorkehrungen betreffen eher den Bereich „Billing“ und weniger den Schutz der Kundendaten. Eine Erkennung durch den Nutzer ist nicht möglich.

EK-C01, C02, C03 Eine Erkennung im Kern-Netz ist nicht möglich. Nur die durch ein kompromittiertes Netzwerk ermöglichten Angriffe auf das Smartphone könnten erkannt werden.

3.2.5. Signalisierungen aus fremden Netzen

Es kann im Allgemeinen davon ausgegangen werden, dass Daten innerhalb eines Providernetzes weniger streng kontrolliert werden als Daten, die über die jeweiligen Gateways aus fremden Netzen eintreffen.

EK-C04 Die Rufnummer wird hier als „Call-ID“ vom Anrufer und zusätzlich durch den Provider „Network-Provided“ übertragen. Eine Erkennung der Rufnummer-Unterdrückung ist durch das verwendete Leistungsmerkmal „CLIPns“ (CLIP-no-screening) möglich. Es ist aber zu beachten, dass auch die Rufnummern 0180 und 0190 auf dieser „CLIPns“-Technik realisiert werden. So würde jeder Anruf von einer Servicerufnummer auch eine Warnung vor „ID-Spoofing“ erzeugen. Die echte „Network-Provided“-Telefonnummer kann am Smartphone nicht erkannt werden. Nur der Provider kann durch eine „Fangschaltung“, die an der Vermittlungsstelle eingerichtet wird, die echte Nummer in Erfahrung bringen.

EK-C05 Eine Erkennung am Smartphone ist eigentlich nicht nötig. Nur wenn das Smartphone ohne Wissen des Besitzers einen Anruf zu einer „manipulierten“ Nummer initiieren würde, könnte diese Abhöraktion hinterher nicht anhand der Einzelverbindungen nachgewiesen werden. Dieser Angriff ist aber eher

unwahrscheinlich, weil dazu weitere Manipulationen nötig wären, um nicht direkt durch den Benutzer erkannt zu werden.

EK-C06 Das SS7-Signalisierungsnetz bietet wenige Sicherheitsfunktionen, da es zu einer Zeit entwickelt wurde, in der es nicht denkbar war, dass fremde Dienstleister Zugang zu diesem Netzabschnitt bekommen könnten. Es gibt lediglich ein „Traffic-Screening“[105], bei dem die Daten des Nutzers analysiert werden können. An dieser Stelle wird nach verdächtigen Vorgängen sowie nach Parametern gesucht, die ein Sicherheitsrisiko darstellen könnten. Zusätzlich gibt es die Funktion „Traffic-Monitoring[106]“ die aber eher zur Qualitätssicherung dient.

Um das Smartphone vor Signalisierungen aus dem Mobilfunknetz zu schützen und eine mögliche Erkennung der AV der Kategorie C zu ermöglichen, müssten Sicherheitskonzepte wie IDS und Firewalls für die Mobilfunkschnittstellen implementiert werden. Im weiteren Verlauf wird dieser Lösungsansatz als „Layer 2/3 Firewall & IDS“ bezeichnet.

3.2.6. Lawful Interception

Folgende Vorgaben wurden bereits vor der Entwicklung festgelegt: dem Nutzer von Sprach- und Datendiensten dürfen Abhöraktionen oder Manipulationen auf keinen Fall auffallen. Auch wenn mehrere Behörden gleichzeitig eine Quelle überwachen, darf das für keine Behörde ersichtlich sein. Die abgefangenen Daten sollen vom Provider unverschlüsselt an das HI weitergeleitet werden. Dem Personal des Service Providers dürfen die Identitäten der abgehörten Personen nicht bekannt sein.

EK-D01 Ob ein Smartphone abgehört wird, könnte nur durch den anfallenden Datenverkehr an den HI-Schnittstellen erkannt werden. Hierzu ist aber ein physikalischer Zugriff auf die Hardware notwendig. Eventuell ist das auch an den BSC im Zugangsnetz möglich, da jede vermittelnde Einheit ein HI-Interface besitzen muss. Ein passives Mithören von Dritten kann am Smartphone nicht

[105] Lee Dryburgh, Jeff Hewelt, “Signaling System No.7: Protocol, Architecture and Services”, 2005, Capter 15: “SS7 Security and Monitoring”, Cisco Press, ISBN-10: 1-58705-040-4
[106] Lee Dryburgh, Jeff Hewelt, “Signaling System No.7: Protocol, Architecture and Services”, Capter 15: “SS7 Security and Monitoring”

erkannt werden, solange die LI-Domain und das Kern-Netzwerk optimal funktionieren.

EK-D02 Bei passiven Verfahren ist keine Erkennung möglich. Bei MITM-Angriffen auf der Funkstrecke ist eine Erkennung, wie im Kapitel 3.1.1. beschrieben, möglich.

EK-D03 Dieser Angriffsvektor könnte theoretisch mittels klassischen Techniken der „Intrusion Detection" erkannt werden. In der Praxis würden die ausgenutzten Sicherheitslücken wahrscheinlich nicht auffallen, solange der Betrieb des ME nicht beeinträchtigt wird.

EK-D04 Eine Erkennung wäre nur möglich, wenn die LEA-Domain hierzu manipuliert wurde und zum Beispiel ein Protokoll aller abgehörten Telefonnummern anfertigt und diese Daten unbemerkt versendet. In der Praxis wäre das sehr schwer realisierbar.

EK-D05/D06 Eine Erkennung ist nicht möglich.

3.2.7. Zusammenfassung

Bei MMS und den Varianten des WAP-Push, die über paketvermittelte Verbindungen übertragen werden, gibt es Erkennungsmethoden, die schon im Bereich Internet- und Computertechnik eingesetzt werden. Teilweise sind diese Lösungen bereits im Betriebssystem oder als Smartphone-APP realisiert.

Es konnten aber auch mobilfunkspezifische Vorkehrungen beschrieben werden, die noch nicht realisiert wurden.

PDU-Filter/Inspection: Ankommende Nachrichten müssen nach den vorher erwähnten Merkmalen durchsucht werden. Am wichtigsten ist es die Nachrichten anzuzeigen, die dem Nutzer normalerweise verborgen bleiben.

SMS-Spam Filter: Die Nutzdaten der eintreffenden SMS-Nachrichten müssen nach bestimmten Schlüsselwörtern und eventuell enthaltenen URI durchsucht werden. Die Absenderadresse könnte mit den vorhandenen Kontakten im Adressbuch verglichen und unbekannte Absender optisch hervorgehoben werden. Um Spam erkennen zu können müssten ähnliche Methoden etabliert werden, wie sie bei E-Mail-Diensten schon lange eingesetzt werden.

Layer 2/3 Firewall & IDS: Die Analyse der unteren drei Protokollschichten der 2G- und 3G-Mobilfunknetze ist sicherlich die anspruchsvollste Aufgabe. Der Empfang der Daten findet in dem schon beschriebenen isolierten Baseband-Bereich statt, der auch als Modem bezeichnet wird. Wie der Zugriff hierauf realisiert werden kann, ist abhängig von dem verwendeten Betriebssystem und deshalb Gegenstand der Untersuchung in Kapitel 5.

3.3. Schnittstellen am Smartphone

3.3.1. Sende- und Empfangseinheiten für den Mobilfunk

EK-E01 Angriffe die direkt auf das Empfangsteil abzielen sind mit den verfügbaren Mitteln eines Smartphones nicht zu erkennen. Auch spezielle Applikationen für Smartphones erkennen nur die Angriffe auf den höheren Protokollschichten wie TCP/IP.

EK-E02 Dieser Angriff setzt sich aus verschiedenen Vektoren zusammen[107]. Die Aktionen, die durch die Schadsoftware ausgeführt werden, sind: Aktivierung des Mikrofons, Verbindungsaufbau über die SIM-Karte (Call-Control) oder auch das Senden der Audiodaten über WLAN zu einem späteren Zeitpunkt.

Das offene Mikrofon kann in den meisten Fällen nicht erkannt werden. Wie auf dem Blockdiagramm des S2 in Abbildung 22 zu sehen ist, gibt es direkte Verbindungen zwischen dem digitalen Signalprozessor (DSP) zur A/D Wandlung (Audio Codec) und dem Baseband-Prozessor (CP+CP PMIC). So könnte theoretisch eine Aktivierung über die Funkschnittstelle erfolgen, die vom Betriebssystem nicht erkannt werden kann.

Das Senden der Daten im Hintergrund über WLAN oder eine Datenverbindung würde den meisten Nutzern wahrscheinlich nicht auffallen, auch wenn ein kleines Icon auf dem Display darauf hinweist. Die Daten könnten aber auch unbemerkt über den leitungsvermittelten Teil übertragen werden.

Beide Angriffe könnten ausschließlich durch eine „Layer 2/3 Firewall und IDS“ erkannt werden.

[107] Ryan Farley und Xinyuan Wank, „Roving Bugnet: Distributed Surveillance Threat and Mitigation“

EK-E03 Eine Erkennung am Smartphone ist nicht möglich.

3.3.2. SIM- und USIM-Smartcard

Durch die Analyse der PDU-Messages (siehe Kapitel 3.2) können auch die Angriffsvektoren **E04, E05** und **E06** erkannt werden. Der Unterschied zu den AVs im Abschnitt B besteht in dem „Envelope-Mode“, durch den eine SMS direkt (transparent) an die SIM-Karte weitergeleitet wird.

Drei Bedingungen müssen hierzu erfüllt sein[108]:

- TP-PID = 0x7F
- TP-DCS = Class 2 8-Bit
- SIM Service Tabelle muss den Eintrag „Data Download via SMS Point-to-Point” enthalten und der Dienst muss aktiviert sein. Ansonsten wird die SMS im Bereich des EF_{SMS} gespeichert.
- Bei SMS Cell Broadcast muss der Service „Data Download via SMS-CB“ in der Service Table der SIM-Karte aktiviert und der „Message Identifier“ in der EF_{CBMID} eingetragen sein, dann wird Cell Broadcast direkt an die SIM weitergeleitet, ohne auf dem Display angezeigt zu werden.

Laut ETSI GSM 3.40 Spezifikation Abschnitt 9.2. kann über den Short Message Transport Layer (SM-TL) jede eintreffende Nachricht vollständig empfangen werden.

EK-E05 Die OTA-Konfiguration sollte als Backup gespeichert werden, damit die Veränderungen im Nachhinein erkennbar sind.

Neben der Softwarelösung zur Erkennung gibt es auch Hardwarelösungen. Zur Erkennung an der SIM-Karten-Schnittstelle könnte ein als „Turbo-SIM“ oder auch „Proxy-SIM“ bekanntes Bauteil eingesetzt werden, dass als „Sniffer“ auch den Datenverkehr in umgekehrter Richtung, also von der SIM zum Modem, mitlesen kann. Die SIM-Karte benutzt sogenannte proaktive Mechanismen[109], die es ihr ermöglichen selbstständig die Kontrolle über das Smartphone zu erlangen. Die

[108] ETSI Standart GSM 11.14, “Digital cellular telecommunications system (Phase 2+); Specification of the SIM application toolkit for the Subscriber Identity Module – Mobile Equipment (SIM – ME) interface”, Kapitel 7.1 “SMS-PP data download”, V5.9.0, 11-1998
[109] ETSI GSM 11.14, Kapitel 4.2 “Proactive SIM”

Kommandos der SIM-Karte können ebenfalls erkannt und angezeigt werden. In Kapitel 5 wird näher darauf eingegangen.

3.3.3. Sonstige Schnittstellen

EK-E07 Das passive Abhören der Bluetooth-Schnittstelle kann nicht erkannt werden.

EK-E08 Ein Verbindungsversuch wird normalerweise vom ME erkannt und auf dem Display angezeigt. Die Erkennung eines Angriffs wäre relativ einfach, da hierfür von den Betriebssystemen ausreichende Programmierschnittstellen zur Verfügung gestellt werden. Eine Reihe von Softwarelösungen ist bereits als Smartphone-APP erhältlich.

EK-E09 Angriffe, die direkt auf die WLAN-Schnittstelle abzielen, sind für Angreifer sehr interessant, da dieses Interface bei den meisten Benutzern immer aktiviert ist und sich automatisch mit bekannten Netzen verbinden kann. Die WLAN-Schnittstelle könnte sich automatisch deaktivieren, wenn der Empfangsradius des Accesspoints verlassen wird. Durch eine regelmäßige Standortbestimmung könnte das Smartphone die Schnittstelle aktivieren, wenn es wieder in den Sendebereich eines bekannten Accesspoints eintrifft.

EK-E10 Der Vorgang des Auslesens kann erkannt werden, da hierzu immer erst ein Signal gesendet werden muss, um den Tag zum Senden der Information aufzufordern.

EK-E11 Die verwendete QR-APP muss die eingelesenen Daten zuerst anzeigen und erst nach Bestätigung des Nutzers ausführen.

3.4. Ortung und Positionsbestimmung

EK-F01 Die Kommunikation zwischen SMLC und mobilem Endgerät bei Ortungsvorgängen findet über RRLP[110] (Radio Resource Location Service Protocol) statt. Eine Erkennung von Ortungsversuchen wäre nur im Baseband Bereich möglich. Gewisse Standortdaten werden jedoch regelmäßig übertragen, wenn das Mobilfunknetz die Empfangsqualität am Endgerät ermittelt.

EK-F02 Der eigentliche Ortungsprozess läuft auf dem Smartphone ab. Zur Erkennung könnten die Zugriffe der verschiedenen Smartphone APPs auf die GPS-Schnittstelle protokolliert werden.

EK-F03 Die eindeutigen IDs (IMEI, IMSI, MAC, usw.) werden bei vielen Gelegenheiten unverschlüsselt gesendet. Die Erkennung eines potentiellen Angriffs ist zum Beispiel möglich, wenn die Abfrageintervalle außerhalb der normalen Parameter liegen.

EK-F04 Eine Erkennung ist nicht möglich.

EK-F05 Bei der Vielzahl von Smartphone APPs die zur Verfügung stehen, ist die Erkennung jeder möglichen Variante fast unmöglich. Gerade bei Messenger-APPs, die ständig mit unterschiedlichen Netzwerkkomponenten kommunizieren müssen, um zum Beispiel die Erreichbarkeit zu signalisieren oder Statusmeldungen zu senden, ist es sehr schwer einen Angriff zu erkennen.
Die ortsbezogenen Daten könnten unter Umständen auch beim Dienstanbieter ermittelt werden, ohne dass eine Anfrage an das Smartphone nötig ist.

[110] 3GPP TS 04.31 “Serving Mobile Location Centre (SMLC), Radio Resource LCS Protocol (RRLP)”

3.5. Zusammenfassung

Die Untersuchung hat einige systematische Vorkehrungen wie zum Beispiel Cipher Indicator, stille SMS und SL-Push identifizieren können, bei denen eine Erkennung eigentlich nicht vorgesehen ist. Aus verschiedenen Gründen sollen dem Nutzer bestimmte Ereignisse nicht angezeigt werden.

Für eine Erkennung muss die Funkverbindung möglichst direkt an den Schnittstellen auf den unteren Protokollebenen analysiert werden. Dieser Umstand erschwert die Erkennung der meisten Angriffsvektoren.

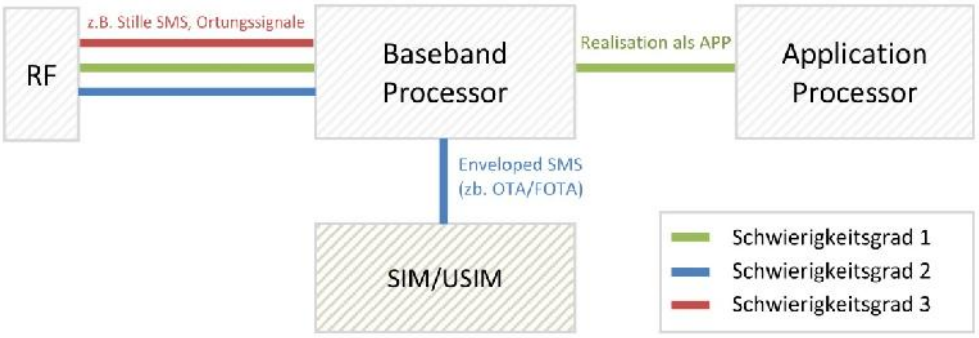


Abbildung 33: Zusammenfassung AV-Erkennung

Wichtige Informationen, wie der zugewiesene Cipher-Indicator und eine „Trust-Score“ der aktuell verbundenen Basisstation, sollten direkt auf dem Display ablesbar sein.

Die Vektoren der Kategorie C und D sind naturgemäß sehr schwer bis gar nicht am Smartphone zu erkennen. Maßnahmen zur Erkennung und Abwehr müssen von den Service-Providern ergriffen werden.

Die beschriebenen Lösungsansätze „fB-Detection“, „PDU-Filter“ und „Layer2/3 Firewall & IDS“ zur Erkennung werden im nächsten Kapitel weiter verfolgt.

4. Gegenmaßnahmen

Die Gegenmaßnahmen werden in zwei Gruppen unterteilt.
Zuerst werden die Maßnahmen untersucht, die als Reaktion auf einen bereits erkannten Angriff eingeleitet werden können. Dabei werden die Resultate des vorherigen Kapitels weitergeführt, für die in den meisten Fällen die Entwicklung einer eigenen Software Voraussetzung ist.

An zweiter Stelle folgen die prophylaktischen Vorkehrungen, um einen Angriff unmöglich zu machen. Zum Beispiel können Smartphones so konfiguriert werden, dass sie sich nur mit einer UMTS Basisstation verbinden. Der Angriffsversuch eines IMSI-Catchers könnte dann jedoch nicht mehr erkannt werden.

Beide Optionen sollen als Lösung in Betracht gezogen werden.

Gegenmaßnahmen sind durch folgende Komponenten möglich:

- Softwareentwicklung (Se)
- Konfiguration des Smartphones (Kf)
- Installation zusätzlicher Software (Si)
- Zusätzliche Hardware (Hw)
- Leistungen von Service Providern oder Drittanbieter (Da)

Im zweiten Teil werden die unterschiedlichen Sicherheitskonzepte der aktuellen Smartphone-Betriebssysteme sowie Infrastrukturelle Lösungen untersucht.

4.1. Gegenmaßnahmen zu den Angriffsvektoren

4.1.1. Kategorie A: IMSI-Catcher und Fake BTS

Die Entwicklung der „fB-Detector"-Software ist in Bezug auf die Logik und den damit verbundenen Programmieraufwand, mit einem relativ großen Ressourceneinsatz verbunden. Ob das Problem der Informationsbeschaffung auf den unteren Protokollschichten lösbar ist wird in Kapitel 4.2. und Kapitel 5.1. untersucht. Es ist aber schon abzusehen, dass nach alternativen Maßnahmen gesucht werden sollte, um die Angriffsvektoren der Kategorie A abwehren zu können.

Weitere Gegenmaßnahmen sind kurzfristig umsetzbar.

- Konfiguration des Smartphones (Kf) oder Installation zusätzlicher Software, um das Verbinden mit 2G-Basisstaionen zu unterbinden. Je nach Betriebssystem stehen hierzu Optionen in den Einstellungen bereit. Für ländliche Gebiete kommt die Lösung aber nicht in Frage, da hier zum größten Teil nur GSM/EDGE Basisstationen im Einsatz ist.
- Zusätzliche Verschlüsselung mittels VPN-Tunnel (Kf). Bei einer Sprachverbindung müssen beide Gesprächspartner zusätzliche Software einsetzen (Si). Zum Beispiel: PrivateGSM (iOS, Android, BB), Whispersystems[111] (Android)
- Ein bequemerer Weg ist die Wahl eines Providers, der Mobile VoIP[112] anbietet (Da). Herkömmliche Sprachanrufe können wie gewohnt geführt werden, die Übertragung findet jedoch ausschließlich über die Datenverbindung statt. Der Vorteil besteht darin, dass ausgehende Gespräche an jedes Smartphone weiter vermittelt werden können. Der Angerufene benötigt keine spezielle VoIP-Software, da es sich auf seiner Kommunikationsseite um einen gewöhnlichen (Circuit Switched) Anruf handelt.

[111] www.whispersys.com/ [Stand 19.11.2012]
[112] Angebote von „sipgate one" (www.sipgate.de/one) [Stand 01.11.2012] oder „*Solomo*" (MVNE) (ehem. Vistream) (www.solomo.de) [Stand 01.11.2012]

4.1.2. Kategorie B: SMS/PDU Analyse

GE-B01-B04 Webbasierende SMS-Dienste bieten zum Teil SMS-Verschlüsselung und nutzen signierte Zertifikate. (Da)

GE-B05–B09 PDU-Analyse und Spam Filter könnten nach der Erkennung alle nötigen Gegenmaßnahmen einleiten (Se), wie zum Beispiel das Blockieren der Push Nachricht oder das Speichern von Flash-SMS.

Jede eingehende PDU-Message sollte im SMS-Eingang angezeigt werden. Mit einer farblichen Kennzeichnung und einem eigenen Verzeichnisbaum im SMS-Nachrichteneingang kann die Übersichtlichkeit gewahrt bleiben.

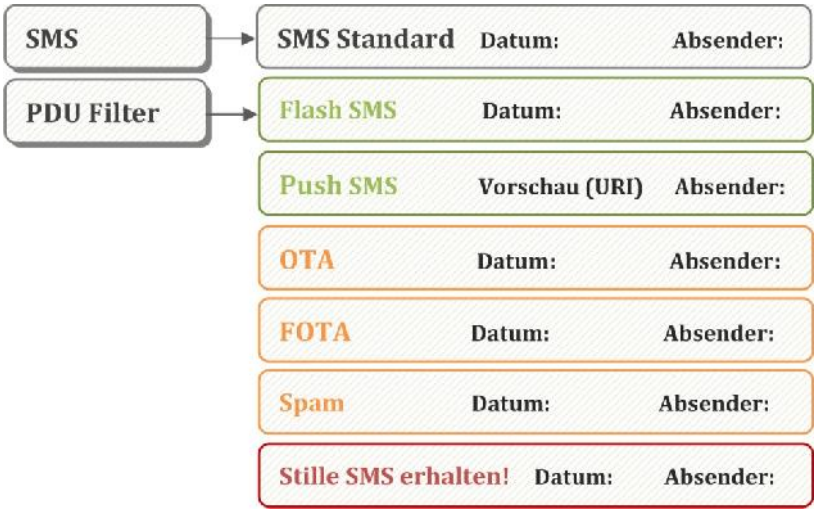


Abbildung 34: SMS Nachrichteneingang

Eine Flash-SMS sollte sich optisch deutlich von allen anderen Pop-up-Fenstern unterscheiden, wie sie zum Beispiel bei Systemmeldungen oder Benachrichtigungen auf dem Home-Bildschirm erscheinen, damit sie nicht für Phishing-Attacken genutzt werden kann.

Den kompletten Empfang von SMS-Nachrichten zu unterbinden ist in den meisten Fällen nicht möglich. Eine Ausnahme bieten sogenannte Home-Zone-Tarife, bei denen die eingehenden SMS an ein stationäres Endgerät in der Home-Zone geroutet werden können (Da). Ein weiterer „Workaround“ ist die Verwendung von mehreren SIM-Karten für die gleiche Telefonnummer (Multi-SIM). Im Gegensatz zu einem eingehenden Anruf werden SMS-Nachrichten nur an eine SIM-Karte

gesendet (Da). Zusätzlich wird ein GSM/UMTS Gateway benötigt, um die eingehenden SMS-Nachrichten an ein VoIP-Client zu senden. Diese Lösung wird in Kapitel 4.3.2. näher beschrieben.

GE-B10 Das Ausführen von USSD oder auch jedem anderen Code kann durch das Betriebssystem blockiert werden. Für Android Smartphones, bei denen die bekannte USSD Schwachstelle besteht, gibt es mehrere kostenlose APPs, die den Aufruf einer „Tel:URL" abfangen können (Si).

GE-B11-B12 Ähnlich der SMS-Lösung von Drittanbietern gibt es auch alternative MMS-Dienste (Da). Der MMS-Empfang kann im Gegensatz zu SMS deaktiviert werden (Kf).

GE-B13-B16 Der MMS-Service kann durch Anti-Virus-APPs und Verwendung einer Firewall-APP zusätzlich gesichert werden (Si).

Die Synchronisation von E-Mails, Adressbücher, Terminkalender und Verzeichnisdiensten kann wie gewohnt über die eigene Firmeninfrastruktur oder über einen Cloud-Dienst des Geräteherstellers oder des Providers erfolgen.

Ein hohes Maß an Sicherheit wird durch die Verwendung von MDM-Software erreicht, die in Kapitel 4.2. für die einzelnen Betriebssysteme untersucht wird.

4.1.3. Kategorie C: Mobilfunknetzwerk

Hier kann ausschließlich eine zusätzliche „Ende-zu-Ende"-Verschlüsselung unter Nutzung einer eigenen Public-Key-Infrastruktur (PKI) vor dem Abhören der Daten schützen. (Kf, Si). Die Sprachverschlüsselung mittels Krypto-SD-Karte oder APPs wird im Folgenden weiter untersucht. Standort und Verbindungsdaten können jedoch weiterhin erhoben werden.

4.1.4. Kategorie D: Lawful Interception

Eine Möglichkeit der Überwachung zu entgehen ist die Anonymisierung der eigenen Identität. Der BSI rät in seiner Publikation „Öffentliche Mobilfunknetze und ihre Sicherheitsaspekte"[113] zur Nutzung einer Prepaid-SIM-Karte, wenn eine

[113] BSI „Öffentliche Mobilfunknetze und ihre Sicherheitsaspekte"; Abschnitt „M.22 Verwendung von Prepaid-Karten zur Anonymisierung"; Seite 46

gewisse Anonymität gewahrt bleiben soll (Da). Beim Kauf dieser Karten wird kein Identitätsnachweis gefordert. Zur Online-Registrierung kann eine „generierte“[114] Personalausweisnummer benutzt werden. Das Aufladen des Prepaid Guthabens kann als Bareinzahlung erfolgen.

GE-D02 Für bestimmte Personengruppen stehen sogenannte „Krypto-Handys“ bereit, auf die im weiteren Verlauf genauer eingegangen wird (Hw).

4.1.5. Kategorie E, Schnittstellen am Smartphone

GE-E01 Geeignete Gegenmaßnahmen sind an dieser Schnittstelle nicht vorgesehen. Die Entwicklung eigener Software für den Baseband-Bereich ist nicht ohne Umwege möglich. Zum einen ist der Quellcode nicht erhältlich und zum anderen gibt es keine Programmierschnittstelle, die genutzt werden kann.

GE-E02 Wenn der Angriff über die SIM-Karte erfolgt könnte die Gegenmaßnahme darin bestehen, die Smartcard nicht direkt im Smartphone zu betreiben. Bluetooth Dual-SIM und GSM/UMTS-Router werden im folgenden Kapitel näher beschrieben.

GE-E03 Gegenmaßnahmen können nur durch den Provider erfolgen.

GE-E04-E06 Das Empfangen der „Service Load“ Nachrichten kann deaktiviert werden (Kf). Die Daten, die über das Mobilfunknetz eintreffen, werden zunächst von dem SIM Application Toolkit (STK) inspiziert und dann in einer „Java Virtual Machine“ interpretiert. Auf das STK kann vom Smartphone auf Applikationsebene zugegriffen werden. Das bedeutet, dass hier eventuell eine Möglichkeit geschaffen werden kann direkt auf das Baseband zugreifen zu können. Dieser Ansatz wird ebenfalls in Kapitel 5 weiter verfolgt.

GE-E05 Die OTA-Konfiguration sollte als Backup gespeichert werden, damit Veränderungen im Nachhinein rückgängig gemacht werden können (Kf, Si). Besser ist eine eigene MDM-Lösung, um die Administration zu ermöglichen. Dabei gibt es je nach Betriebssystem unterschiedliche Lösungen, die im zweiten Teil des Kapitels beschrieben werden.

[114] Die Berechnung einer gültigen Personalausweis ID kann auf verschiedenen Webseiten erfolgen. (hp.lise-meitner-gymnasium.de/static/mbirth-JavaScript/calcperso.html) Der Algorithmus wurde eigentlich zur Überprüfung von Personalausweis IDs veröffentlicht.

GE-E06 Änderungen an der Firmware sollten nur durch den Service Provider beziehungsweise den Gerätehersteller durchführbar sein. Bei der Verteilung von Softwareupdates wird im Allgemeinen auf bekannte Authentifizierungs- und Verschlüsselungsverfahren zurückgegriffen.

GE-E07/E08 Die korrekte Nutzung der Sicherheitsfunktionen, die Bluetooth ab Version 2.1 bietet, kann für einen ausreichenden Schutz sorgen (Kf, Si). Mittels Mobile Device Management können vom Administrator sogenannte „Policies" (Richtlinien) festgelegt werden. Dadurch werden Sicherheitsrichtlinien umgesetzt, die keine unsicheren Bluetooth Verbindungen zulassen.

GE-E09 Der im Kapitel 2 beschriebene „Cross Service Attack" benutzt als Gegenmaßnahme ein sogenanntes „Prozess Labeling" auf Kernel-Ebene, damit ein Prozess nicht gleichzeitig auf die WLAN- und die GSM-Schnittstelle zugreifen kann.

Eine Gegenmaßnahme bei potentiell unsicheren WLAN Access Points besteht in der Verwendung eines VPN-Tunnels (Virtual Private Network), um sich mit einem sicheren Netzwerk zu verbinden.

GE-E10 Es gibt bereits Lösungen in Form von technischen Spezifikationen, die in der Industrie bereits angewendet werden. Die Organisation „Global Platform Card Specification"[115] bietet Spezifikationen für Smart-Cards und NFC-Chips, die auch bei Banken und Behörden implementiert werden. Hier würden aber zusätzliche Lizensierungsgebühren für die Smartphone-Hersteller anfallen.

GE-E11 Die verwendete QR-APP sollte die eingelesenen Daten zuerst anzeigen und erst nach der Bestätigung des Nutzers ausführen.

Das Ausführen des Links, beziehungsweise der URI, darf nicht ohne Zustimmung des Nutzers erfolgen. Hierzu könnte auch der Webbrowser vor der Verbindung auf eine Nutzereingabe warten.

[115] Quelle: "*Global Platform*" www.globalplatform.org Stand[29.10.2012]

4.1.6. Kategorie F, Ortung und Positionsbestimmung

GE-F01 Die Handyortung seitens des Mobilfunknetzes könnte theoretisch unterbunden werden, indem das mobile Endgerät nicht mehr auf Anfragen aus dem Mobilfunknetz antwortet und selbst kein Location Update ausführt. Praktikabel ist die Lösung aber nicht, weil diese Signalisierungen eminent wichtig für die Verfügbarkeit der Dienste sind. Die aktuelle Cell-ID ist auch beim Provider im HLR gespeichert, damit eingehende Anrufe direkt vermittelt werden können. Der GPS Empfänger im Smartphone kann vom Baseband Prozessor zur Assisted-GPS Ortung genutzt werden. Auch hiergegen gibt es keine Maßnahme.

GE-F02 Die Zugriffsberechtigungen der jeweiligen Smartphone-APP auf die Standortinformation und Ortungsfunktionen muss mittels Betriebssystem kontrolliert und bei Bedarf blockiert werden. Besonders zu beachten ist dabei, dass auch über den Webbrowser auf gerätespezifische Sensoren zugegriffen werden kann. Auf die Zugriffskontrolle und die Interprozesskommunikation der Betriebssysteme wird in Kapitel 4.2. eingegangen.

GE-F03 Nicht genutzte Schnittstellen sollten deaktiviert werden (Kf).

GE-F04 Gegenmaßnahmen, die das Paging der Basisstation unterbinden, sind praktisch nicht möglich. Hierzu müsste vom ME ein „IMSI Detach“ gesendet werden, um sich vom Netz abzumelden.

GE-F05 Eine effiziente Gegenmaßnahme zu finden ist hier sehr schwer. Im Prinzip hilft nur die Deinstallation oder die Deaktivierung der gefährdeten APPs. Bei Messenger-Software sollte der Status auf „Offline“ stehen, um unnötigen Datenverkehr zu vermeiden und keine Standortinformationen preiszugeben. Eine wissenschaftliche Arbeit, „SpotME If You Can[116]“, beschreibt ein als „Location Obfuscation“ bezeichnetes Verfahren, dass versucht, den Standort des Endgerätes zu verschleiern. Abschließend ist anzumerken, dass die Lokalisation des Endgeräts ein elementarer Bestandteil im Mobilfunk-Konzept darstellt, der sich in den benutzen Protokollen und Mechanismen widerspiegelt. Gegenmaßnahmen am Smartphone sind praktisch nicht möglich.

[116] Daniele Quercia, Ilias Leontiadis, Liam McNamare, Cecilia Mascolo, Jon Crowcroft “SpotME If You Can: Randomized Responses for Location Obfuscation on Mobile Phones”, In: 31st International Conference on Distributed Computing Systems, S. 363-372. Univ. of Cambridge, UK

4.2. Sicherheitskonzepte von mobilen Betriebssystemen

Die zurzeit am häufigsten anzutreffenden Betriebssysteme sind Android, BlackBerry OS, Apple iOS und Windows Phone. Nur ein kleiner Anteil der im Gebrauch befindlichen Smartphones verfügt über die jeweils neueste Betriebssystemversion. Alle Betriebssysteme bis auf WP7 und BlackBerry sind für die ARM-Prozessorarchitektur entwickelt worden.

Android	BlackBerry	Apple iOS	Windows Phone
Aktuell: 4.2 „*Jelly Bean*“ 2.3.x „*Gingerbread*“ mit 55% noch sehr weit verbreitet[117]. 3.x.x. „*Honeycomb*“ ist speziell für Tablets	Aktuell: 7 Erscheinungstermin der Version 10 ist für Anfang 2013 geplant. Es soll sich um eine komplette Neuentwicklung handeln.	Aktuell: 6 Wegen der schnellen Verbreitung der OTA-Updates sind Apple-Gerätemeist auf dem neuesten Versionsstand.	Aktuell: 8 Bei Windows Phone sind OTA-Updates erst ab Version 8 möglich. Das Updaten von WP7 auf WP8 wird nicht unterstützt

Tabelle 1: Verbreitung der aktuellen Versionen (Stand 11-2012)

Secure Boot & Code Signing

Das Sicherheitskonzept beginnt bei allen Betriebssystemen in den jeweils aktuellsten Versionen schon beim Bootvorgang. Der Bootloader verhindert das Ausführen von unsigniertem Code, vor und während des Bootprozesses. Im Auslieferungszustand befindet sich dieser bei allen Geräten im Zustand „Locked“. Auch die komplette Verschlüsselung des Boot-ROM ist möglich, was ein „Unlock“ in vielen Fällen unmöglich macht. Hierunter zählen Smartphones von RIM und wenige Modelle von Motorola und HTC, die über ein Sicherheitselement verfügen das in die Hardware eingebettet ist.

[117] Quelle: „ Android Developer Guides“; developer.android.com/about/dashboards/index.html; Stand [22.10.2012]

Der Teil der Firmware, der nach dem Einschalten zuerst ausgeführt wird, befindet sich in dem fest verdrahteten Teil des Boot-ROM, der nachträglich nicht mehr geändert werden kann. Die weiteren Teile dieser „Boot Chain“ sorgen dafür, dass nur ein signiertes OS-Kernel in den Arbeitsspeicher geladen werden kann.

Dieser Bereich des Boot-ROMs kann durch das sogenannte „Flashen“ verändert werden, aber nur wenn sich der Bootloader im Status „Unlocked“ befindet. Bei Windows Phone (WP) und Apple i-Devices versuchen die Hersteller ein „Unlock“ durch den Anwender zu unterbinden. Nur die neueren BlackBerrys verfügen über eine Technik, die nicht umgangen werden kann.

Benutzerrechte

Die Verzeichnis- und Dateizugriffsrechte sind sehr stark eingeschränkt, sowohl für den Nutzer als auch für die Applikationen. „Super User“ beziehungsweise Administratorenrechte sind für den Smartphone-Nutzer nicht vorgesehen.

Die Administration erfolgt über Fernzugriff (Remote Management) von einem geeigneten MDM (Mobile Device Management) Server. MDM und MAM (Mobile Application Management) werden im Bereich „Mobile Unternehmenslösungen“ (Mobile Enterprise) eingesetzt.

Der Begriff “gerootet” bezeichnet den Zustand eines Smartphones, nachdem der Zugriff als Administrator ermöglicht wurde. Meistens müssen hierzu erst Fehler in der Software gefunden werden, um an die Root-Rechte zu gelangen.

Sicherheitskonzepte

Jede Anwendung wird in einer eigenen „Sandbox“ ausgeführt, wodurch die Inter-Prozesskommunikation kontrolliert und jeweils ein getrenntes Verzeichnis bereitgestellt wird. Der Zugriff einer APP auf persönliche Daten wie das Adressbuch oder die Standortinformationen wird von den verschiedenen Betriebssystemen sehr unterschiedlich gehandhabt.

ASLR (Address Randomizer) und DEP (Data Execution Prevention), die das Ausführen von Exploits und Malware verhindern sollen, sind in den jeweils aktuellsten Versionen implementiert. Bei Android ab der Version 4.0, iOS verfügt ab Version 3.1 über ASLR und ab der Version 5.0 über DEP.

Grundsätzlich besteht das Sicherheitskonzept aus mehreren Komponenten, die in den verschiedenen Betriebssystemen unterschiedlich implementiert wurden:

- Authentizität (Nachweis eines Dienstes oder Benutzers auf Echtheit)
- Datensicherheit (Vertraulichkeit, Integrität und Verfügbarkeit)
- Datenschutz (Wahrung der Anonymität gegenüber Dritten, Zugriffsbeschränkungen)

Telefonie

Das Modem setzt sich aus dem RF-Frontend (Sende-/Empfangsteil), Antennen switch, ABB (Analog Baseband) und dem DBB (Digital Baseband) zusammen. Das DBB besteht aus dem Baseband Prozessor, RAM, DSP (Digital Signal Processing) und dem ROM auf dem sich das Realtime-OS und die Hardwaretreiber befinden.

Das Signal trifft am Empfangsteil ein und wird im ABB abgetastet und quantisiert. Das digitalisierte Signal wird vom ABB an den DSP Chip geleitet. Der Baseband Prozessor kommuniziert meist über Shared Memory mit dem DSP, der für die wichtigsten Berechnungen wie Demodulation, Decoding, Fehlererkennung und Vorwärtskorrektur zuständig ist.

Die Kommunikation zwischen dem BP und AP erfolgt über eine oder mehrere serielle Verbindungen (UART) auf denen AT-Befehle[118] ausgetauscht werden.

Wie sich der Zugriff auf das Modem unterscheidet und welche Prozesse für Telefonie und SMS-Dienste zuständig sind wird im folgenden Abschnitt in Erfahrung gebracht.

[118] 3GPP Standard TS 27.007 „AT command set for User Equipment (UE)", 2012-03

4.2.1. Android

Android-Applikationen können mit Entwicklungsumgebungen wie *„Eclipse“* oder *„Aptana Studio“* in Java programmiert werden. Dazu muss das Java-SDK (Software Development Kit) und Android-SDK[119] installiert werden.

Der Compiler erzeugt einen Bytecode, der von jeder *„DALVIK Virtual Maschine“* ausgeführt werden kann. Die VM startet einen isolierten Prozess, der durch eine eindeutige UID (Unix User ID) referenziert ist.

Um bei Bedarf die Kommunikation zwischen den Prozessen zu ermöglichen, gibt es verschiedene Methoden, wie die „Explizit deklarierten Richtlinien“[120], die bei der Installation festgelegt werden, IPCs (Inter-Prozess-Kommunikation mit Intents, Service- und Broadcast-Receiver) und Shared UID[121], bei der mehrere APPs eines Entwicklers die gleiche Signatur erhalten. Es stehen also Mittel zur Verfügung, das Sandbox-Prinzip zu umgehen.

Android besteht in der untersten Schicht aus einem Linux-Kernel.

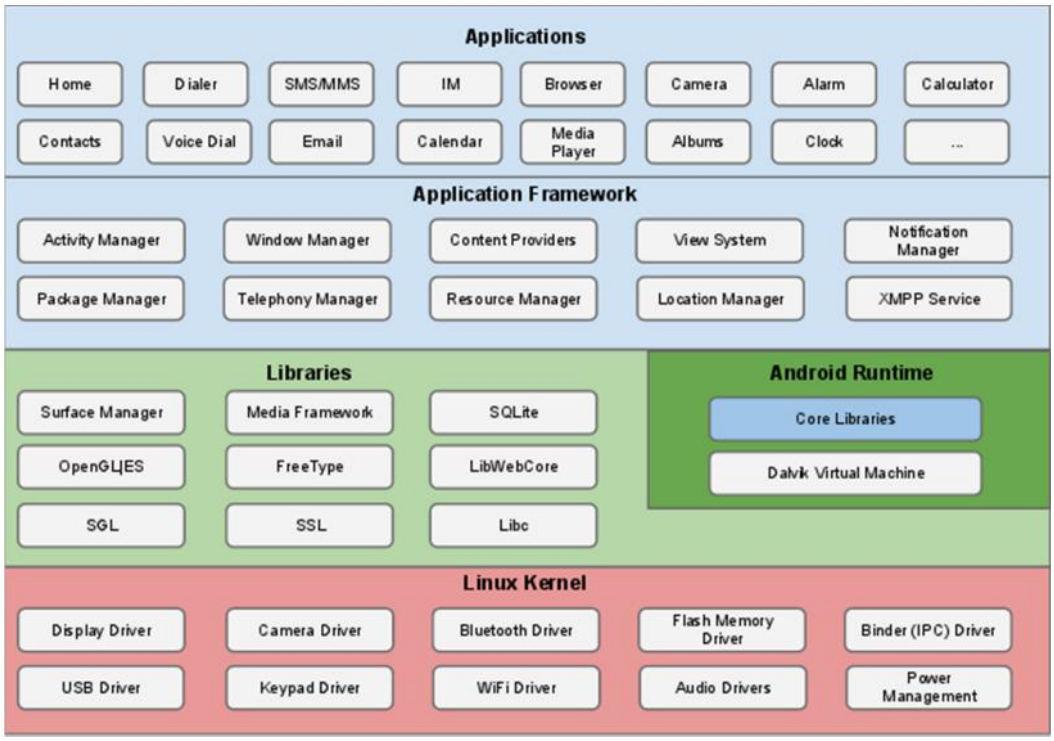


Abbildung 35: Die Betriebssystemschichten von Android, Quelle: OHA[118]

[119] Quelle: Open Handset Alliance www.openhandsetalliance.com/; Stand [01.11.2012]
[120] “AndroidManifest.xml” siehe Android Developer Guides: http://developer.android.com/guide/basics/what-is-android.html
[121] Siehe Android „Tech Info“ source.android.com/tech/security/index.html Stand [22.10.2012]

Besonderheiten der Android-Plattform

- NDK (Native Development Kit) für die Entwicklung mit C/C++
- Weitere Standards: WebKIT (Web-Browser), SQLite, Open GL 3D
- Die eigene Software kann vom Entwickler selbst signiert werden (Self Signed). Es gibt keine zentrale Vergabestelle von digital signierten Zertifikaten.
- Ein sogenanntes „Custom Rom“[122] besteht aus einem Softwarepaket, dass für ein bestimmtes Modell angepasst wurde. Der Linux-Kernel, die gewünschten APPs, das Radio-ROM (Firmware für das Baseband) und das Theme (optische Erscheinungsbild) werden mit einem Software-Kit, dem sogenannten „ROM-Kitchen“, zusammengeführt. Mit diesen Tools wäre es möglich, eine modifizierte Baseband-Software auf ein Smartphone aufzuspielen, um zum Beispiel an die Informationen des GSM-Protokoll-Stacks zu gelangen. ROM-Kitchen sind auch für WP7 verfügbar, jedoch in einem früheren Entwicklungsstadium.
- Die Distribution der eigenen APPs kann über den „Google Play Store“ oder auch über eine Reihe von alternativen Stores erfolgen. Die Installationsdatei mit der Endung .apk (Android Package) lässt sich aber auch lokal, also zum Beispiel von einer SD-Karte, starten.
- Das Konzept zum Ausliefern der Updates und Patches ist noch sehr lückenhaft in Bezug auf die breite Produktpalette an unterschiedlicher Hardware, für die Updates angepasst werden müssen. Ein Betriebssystem-Update auf die aktuelle Version 4.2 ist bei vielen Android-Smartphones nicht möglich.
- Die vorinstallierten Java-Anwendungen für Telefonie und SMS können jederzeit durch alternative APPs von Drittanbietern ausgetauscht werden. Gerätehersteller und Provider passen so das System nach Ihren Bedürfnissen an, was als Stock-ROM bezeichnet wird. Der Quellcode der eingefügten Applikationen wird in der Regel nicht veröffentlicht. Auch Android-Derivate, die ohne Google APPs auskommen, sind durch den geschlossenen Baseband-Bereich keine wirklich quelloffenen Systeme.

[122] Das „Customized ROM“ ist von einem „Stock ROM“, das vom Provider aufgespielt wird, zu unterscheiden.

Einzelne Hersteller ermöglichen die Freischaltung des Bootloaders. Darunter HTC, Motorola und Samsung, die auch alle ein eigenes SDK für ihre Smartphones anbieten. Oft werden diese Modelle als „Developer-Device“ bezeichnet.

Durch den quelloffenen Charakter gibt es bereits Dutzende Derivate und Portierungen von Android, die durch Projekte und Communities realisiert wurden.

Die SDKs der Hersteller, wie zum Beispiel die „Gorbi SDK“ von Qualcomm, können umfassender auf die systeminternen Funktionen zugreifen, bieten dann aber nur eine gerätespezifische Lösung.

Auf den „Project Hosting“-Webseiten von Google befinden sich über 5000 Projekte, die sich nur mit Android beschäftigen und eine gute Grundlage bieten, um zusätzliche Libraries, APIs oder Quellcode zu finden.

Die Gruppe „Secure Element Evaluation Kit for the Android Platform“ entwickelt eine „SmardCard API for Android“[123]. Die Erweiterungen bieten neben einer Komplettverschlüsselung der Daten auch ein eigenes PKI-Management.

Android wird sogar von der NSA als Basis genutzt, um ein sicheres „Mobility Capability Package“[124] für ihre Mitarbeiter zu entwickeln.

Im folgenden Abschnitt werden die wichtigsten Bereiche der Android-API untersucht, die für SMS-Dienste und Telefonie nötig sind. Danach sollte eine realistische Einschätzung möglich sein, in welchem Umfang die „fB-Detection“ oder der „PDU-Filter“ realisierbar ist.

Die API-Packages „android.telephony“[125] und „android.telephony.GSM“ stellen die wichtigsten Zugriffe bereit.

Für die Softwareentwicklung sind folgende Klassen interessant:

- “CipherSpi”, Service Provider Interface (SPI)
- „NeighboringCellInfo“, Methoden: getCid(), getLac() und getRssi()
- „TelephonyManager“ und „PhoneStateListener“
- „SmsMessage“, „SMSManager“ und „SmsMessage.SubmitPdu“
- „SignalStrength“, Methoden: getEvdoSnr(), getGsmBitErrorRate(), getGsmSignalStrength()

[123] http://code.google.com/p/seek-for-android
[124] NSA, “*Mobility_Capability_Pkg_(Version_1.1U)”*, Februar 2012
[125] Siehe http://developer.android.com/reference/android/telephony/

Das Package „javax.crypto“[126] beinhaltet Klassen („Cipher“, „CipherSpi“[127] und „NullCipher“) und Methoden (getAlgorithm(), getParameters()), mit denen der „Cipher Indicator“ einer Instanz ausgelesen werden kann.

Der „Radio Interface Layer“ (RIL) befindet sich zwischen dem *„Application Framework*“ und dem Baseband Device und besteht aus dem RIL Daemon (rild) und dem geräteabhängigen Vendor RIL.

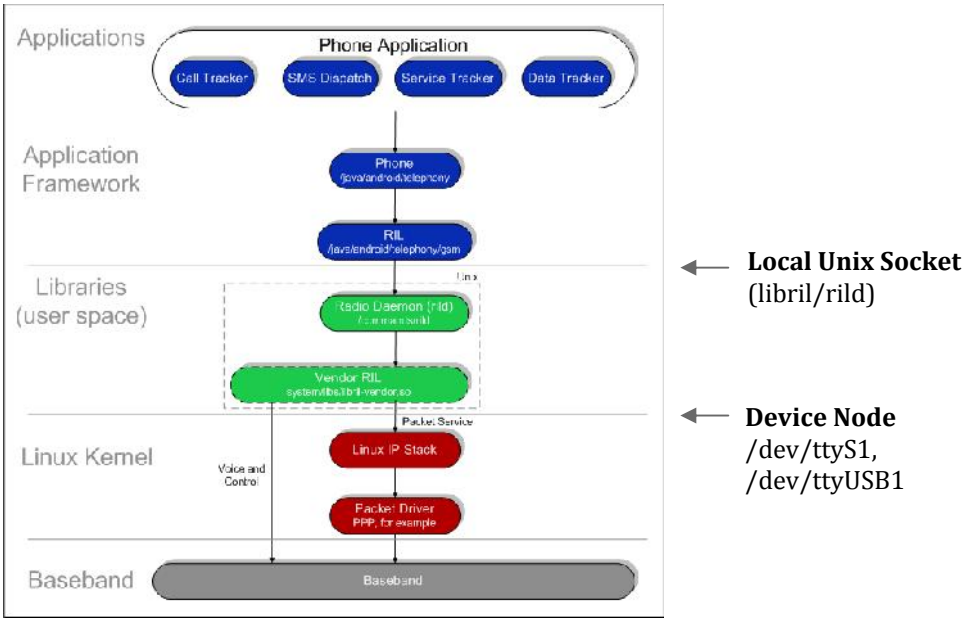


Abbildung 36: Android RIL Quelle: Quelle: OHA[118]

Die Kommunikation zwischen Telephony API (RILJ) und RIL Daemon findet über eine Socket-Verbindung statt. Der Vendor RIL greift über eine serielle Schnittstelle auf den Baseband-Prozessor zu und kommuniziert über AT-Befehle. Mit den Klassen „com.android.internal.telephony.RIL.RILSender“ und „com.android.internal.telephony.RIL.RILReceiver“ kann direkt auf eingehende und ausgehende Daten zugegriffen werden, die von dem hardwareanhängigen RIL-Layer zur Verfügung gestellt werden. Um die Daten abfangen zu können kann die „Man-in-the-middle“-Methode angewendet werden, wie sie in der Arbeit „Injecting SMS Messages into Smart Phones for Security Analysis[128]“ von Colin Mulliner beschrieben ist.

[126] Quelle: http://developer.android.com/reference/javax/crypto/package-summary.html
[127] Quelle: http://developer.android.com/reference/javax/crypto/CipherSpi.html Stand [01.11.2012]
[128] Collin Mulliner (TU-Berlin) und Charlie Miller “Injecting SMS Messages into Smart Phones for Security Analysis”, 2009

4.2.2. BlackBerry OS

Research in Motion bietet als einziger Anbieter ein Betriebssystem, dass nicht von einem Desktop-Vorgänger abgeleitet ist. Die Architektur ist sehr einfach und schlank gehalten. Es gibt vier Softwareschichten:

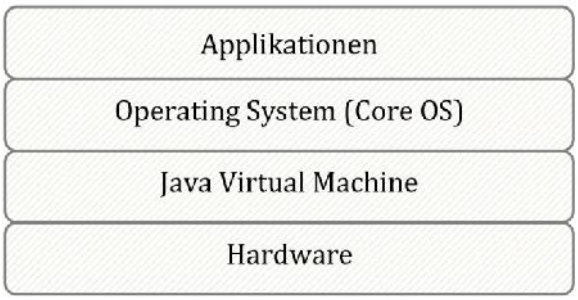


Abbildung 37: BlackBerry OS Layer

Als Entwicklungsumgebung steht aktuell das *„BlackBerry Java 7.1 SDK"*[129] zum kostenlosen Download bereit, wobei auch Eclipse oder Visual Studio als Entwicklungsumgebung genutzt werden können.

- Java ME (Micro Edition) von RIM und Native SDK (C/C++)
- Weitere Standards: Adobe AIR, WebKIT-Browser, SQLite, Open GL ES 2.0
- Nur wenige Systemdienste verfügen über Root-Rechte
- Im *„App World"* werden APPs von Drittanbietern angeboten
- Die kommende Version 10 des Betriebssystems wird auch eine Runtime für Android-APPs bereithalten.
- Der Bootloader, der Kernel und die Systemdienste werden nur ausgeführt wenn sie von RIM signiert sind
- Das „Unlocken[130]" des Bootloaders und das Rooten ist nur bei älteren Geräten (8000-9000) möglich.
- Neue Firmware kann über den *„BB Desktop-Manager"* eingespielt werden. Hierzu gibt es Flashfiles vom jeweiligen Provider oder auch direkt bei RIM.
- Mit *„Mobile Fusion"* können auch Android, iOS und Windows Phones in die Firmenumgebung eingebunden und administriert werden. Hierzu muss auf den „fremden" Systemen eine APP installiert werden.

[129] Quelle: developer.blackberry.com/develop/ Stand [04.11.2012]
[130] Software: MFI Multiloader oder Unlocker von Harald Kubovy Quelle: http://www.gsmfreeboard.com Stand [04.11.2012]

Mit BlackBerry Enterprise Service (BES) besitzt RIM eine sichere Infrastrukturlösung für das geschäftliche Umfeld. Für die Smartphones stehen ebenfalls Sicherheitskonzepte bereit, wie die Datenverschlüsselung (3DES, AES) auf dem Gerät und bei der Übertragung (SMS, E-Mail-Push und BlackBerry Messenger), Schutz vor „Buffer overflows“, NX/XN-Flag zur Prozesskontrolle[131], ASLR (Address Space Layout Randomization), Unterscheidung von Applikationstypen, Verwaltung von Zugriffsrechten (Security Policies), Remote Administration und Gerätemanagement. Eigenständige Lösungen[132] („InHouse“ mit eigener Infrastruktur) zur Sprachverschlüsselung und Anrufvermittlung gibt es auch von mehreren Drittanbietern. Den Internetzugang stellt RIM mittels APNs direkt im Mobilfunknetz des jeweiligen Providers bereit.

Wie im Firmenumfeld üblich, kann das BES zu jeder Zeit auf alle Informationen des Endgerätes zugreifen, SMS-Nachrichten, Standort- und Verbindungsdaten mit eingeschlossen.

Das hohe Sicherheitsniveau des Enterprise Service wurde von vielen Instituten und Behörden wie unter anderem TÜV, NATO und Fraunhofer-SIT bestätigt. Als Krypto-Handy darf es jedoch nicht eingesetzt werden. Der BlackBerry Internet Service (BIS), der für Privatnutzer angeboten wird, ist hingegen nicht abhörsicher.

In der BlackBerry Java 7.1 SDK[133] sind nur die nötigsten Klassen und Interfaces vertreten, um auf das Modem und die SIM-Karte zugreifen zu können.

Darunter die Klassen „net.rim.device.api.smartcard“, „net.rim.device.api.SMS“, „net.rim.device.api.RadioInfo“ und das Interface „javax.microedition.apdu“.

[131] Teufl, Dipl.-Ing. Peter, „Sicherheitsanalyse BlackBerry OS 5“, April 2010

[132] Quelle: „Cellcrypt Mobile Baseline“, www.cellcrypt.com/government/cellcrypt-mobile-baseline Stand [22.10.2012]

[133] Quelle: www.blackberry.com/developers/docs/7.1.0api/ Stand [04.11.2012]

4.2.3. Apple iOS

Apple bietet die kostenlose Entwicklungsumgebung *„Xcode“* an, mit der sowohl iDevices als auch Anwendungen für OS X entwickelt werden können. Das iOS SDK ist ebenfalls kostenlos. Der Entwickler muss sich registrieren und eine jährliche Gebühr entrichten. Danach kann die Anwendung über den APP-Store auch auf fremde Geräte installiert werden.

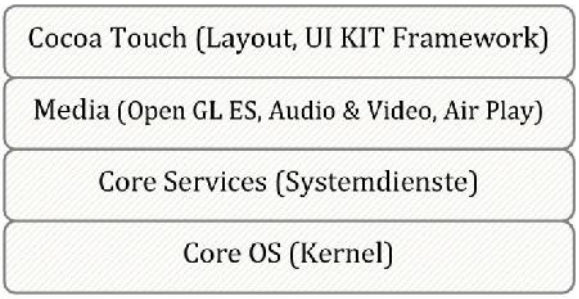


Abbildung 38: iOS Layer

- iOS ist ein Derivat des Mac OSX Betriebsystems, dass für ARM-Architektur optimiert wurde.
- Nativer Code ObjectiveC
- Sonstige Standards: WebKIT (Webbrowser)
- Java und Flash werden nicht unterstützt
- Geschlossenes System, dass die Entwicklung der Software, Herstellung der Hardware und den Vertrieb bis zum Endkunden vorsieht. Nur RIM verfolgt ein ähnliches Konzept.
- Das *„iOS Enterpise Developer Programm“* ermöglicht das Selbst-Signieren und Ausliefern eigener APPs (Mobile Application Management) ohne den Umweg über den Apple-Store.

Das Sandboxing-Konzept von Apple gibt nur ein einziges Regelwerk vor, das für alle APPs gleichermaßen gilt. Auch die eigenen Anwendungen für Telefonie, SMS und der Safari Webbrowser laufen in dem „mobile Mode“, der mit den wenigsten Rechten auskommen muss. Das “ComCenter“, das unter anderem für das Parsen der SMS-Nachrichten verantwortlich ist und direkt mit dem Modem kommuniziert, läuft im „wireless Mode“. Als „privileged user“, also mit Root-Rechten, werden nur die wichtigsten Prozesse ausgeführt.

Der Safari Browser besitzt keine Plugins oder Frameworks, um Web-fremde Formate wie zum Beispiel PDF anzuzeigen. Hierzu wird eine spezialisierte APP gestartet, die im Vergleich zu der PC-Version nur einen reduzierten Funktionsumfang bietet. Die mögliche Angriffsfläche durch Softwarefehler (Exploits) wird so auf ein Minimum reduziert[134]. Trotzdem wurde bis heute immer eine Möglichkeit gefunden das Gerät zu rooten, was bei iDevices als „Jailbreak" bezeichnet wird.
Bei einem Jailbreak werden neben dem zusätzlichen APP-Store „Cydia" auch weitere Anwendungen auf das Gerät installiert. Darunter eine „Command Line Shell", über die Zugriffe auf Dienste des Kernels möglich sind. Dazu wird ein SSH-Port geöffnet, über den man sich über das Netzwerk verbinden kann. Das Standardpasswort „alpine" wird wahrscheinlich von den wenigsten Nutzern geändert, was einem Eindringling eine Reihe von Angriffen ermöglicht.

Die Konfigurationsdaten sowie Passwörter für E-Mail Konto, WLAN, SMS-Center und VPN-Zugang können mit dem „iPhone Configuration Tool" in sogenannten „Mobile Configuration Profiles"[135] gespeichert werden. Die Daten werden verschlüsselt an das jeweilige Endgerät übertragen. Diese Konfigurationsskripte können von Entwicklern genutzt werden, um Einschränkungen des iOS Systems zu umgehen, wie es bei „Snappli" [136] oder „Wajam" [137] der Fall ist[138].

Für Enterprise-Lösungen gibt es ein MDM, bei dem auch Richtlinien (Policies) festgelegt werden können. Das MDM-Push-Zertifikat ist durch den kostenlosen „Certificate Signing Request" bei Apple erhältlich. Die Auslieferung der Push-Nachricht (MCP) durch den MDM-Server erfolgt auf TCP-Port 1640 des iPhones.

Softwareupdates werden vom „Apple Push Notification Server" (APNS) auf dem TCP-Port 5223 ausgeliefert. Die Quelle der Nachricht muss aus dem IP-Segment

---

[134] Charlie Miller, Dionysus Blazakis, Dino Dai Zovi, Stefan Esser, Vincenzo Iozzo, Ralf-Philipp Weinmann "iOS Hacker's Handbook", 2012, John Wiley & Sons, Inc., ISBN: 978-1-118-20412-2
[135] Quelle: developer.apple.com/library/ios/#featuredarticles/iPhoneConfigurationProfileRef/Introduction/Introduction.html Stand [06.11.2012]
[136] Quelle: snappli.com/ Stand [06.11.2012]
[137] Quelle: wajam.com/ Stand [06.11.2012]
[138] Rachel Metz, C't Artikel „An Apple vorbei" vom 02.11.2012 heise.de/-1737936 Stand [19.11.2012]

17.0.0.0/8 direkt von Apple stammen. Zum heutigen Zeitpunkt werden MCP über den TCP-Port 5223 gesendet. Diese Portadressen können sich aber im Laufe der Zeit ändern.
Bei jedem iPhone in der Standardkonfiguration, kann es zwei offene Ports[139] geben. Der UDP-Port 5353 für das von Apple entwickelte „Bonjour Protokoll“ und der TCP-Port 62078 für die Synchronisation mit iTunes.

Das „Core Telephony Framework [140]“ beinhaltet ebenfalls nur die üblichen Methoden, um auf das Modem und die SIM-Karte zugreifen zu können: “CTCall”, “CTCallCenter”, “CTTelefonyNetworkInfo”, „CTCarrier“ mit den Eigenschaften „allowsVOIP“ und „mobileCountryCode“.

Bei dem iOS Telephony Framework greift der ComCenter-Prozess direkt auf den RIL Daemon zu. Mittels Workarounds wie „Library Preloading“, „Terminal-in-the-middle“ und „Method interposition“ kann man an die RAW-Daten herankommen, bevor sie vom ComCenter-Prozess interpretiert werden. Eine genaue Beschreibung findet man ebenfalls in der Arbeit von Colin Mulliner[141].

[139] Dipl.-Ing. Peter Teufl „Sicherheitsanalyse iPhone“, 04-2010, Studie des A-SIT
[140] Quelle: /System/Library/Frameworks/CoreTelephony.framework
https://developer.apple.com/library/ios/#documentation/NetworkingInternet/Reference/CoreTelephonyFrameworkReference/_index.html#//apple_ref/doc/uid/TP40009603
[141] Collin Mulliner (TU-Berlin) und Charlie Miller “Injecting SMS Messages into Smart Phones for Security Analysis”, 2009

4.2.4. Windows Phone 7/8 OS

Die Microsoft-Entwicklungsumgebung *„Visual Studio Express 2010“*[142] beinhaltet die *„Windows Phone SDK 7.1“*, *„XNA“* sowie das *„Silverlight Framework“*.

Damit Softwareentwickler die nötigen Administrator-Zugriffsrechte am eigenen Windows Phone erhalten, muss der Entwickler einen Microsoft-Account besitzen und sich im Developer Center registrieren. Mit einem gültigen Zertifikat können bis zu drei Geräte zum Testen genutzt werden. Als Vertriebskanal dient, ähnlich wie bei Apple, ein zentraler „Point of Sale“, der als *„Marketplace“* bezeichnet wird. Für das Downloaden der APPs ist ein Windows-Live-Account Voraussetzung.

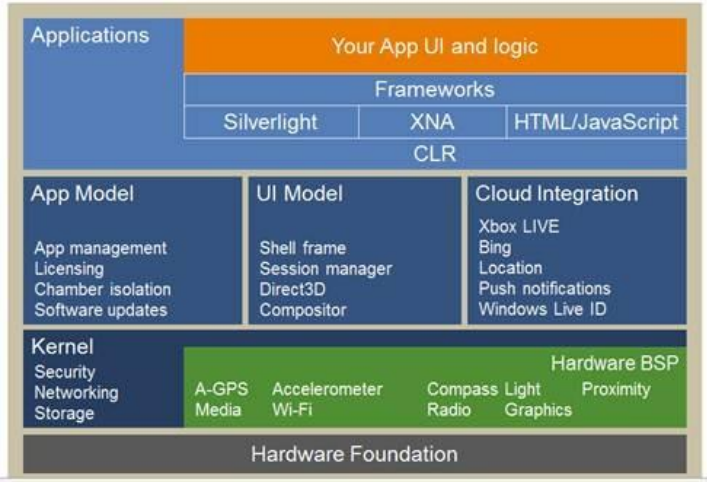


Abbildung 39: Windows Phone OS 7 Framework, Quelle: www.microsoft.com[143]

- WP7 OS ist eine Weiterentwicklung von WinCE (Windows Compact Embedded)
- Strikte Trennung des Speicherbereichs der Applikationen. Keine direkte Kommunikation zwischen den Applikationen möglich
- Drittanbieter APPs erhalten keinen Zugriff auf sensible Daten.
- WP7 bietet keine komplette Geräte-Verschlüsselung
- Ausschließlich VB.net und C#, (C/C++ nur bei WP8)

[142] Entwicklungsumgebung für WP7: www.microsoft.com/germany/express [23.11.2012]
[143] Webcast “Windows Phone 7 Grundlagen”, Link: www.microsoft.com/germany/msdn Stand [23.11.2012]

Die Untersuchung „*Windows Phone 7 Internals and Exploitability*“[144] bringt ein Problem zutage, dass durch Fehler der Treiber-Implementierung seitens der Gerätehersteller verursacht wird.
Mit Applikationen, die für das WP7 Betriebssystem entwickelt wurden ist der Zugriff auf mobilfunkspezifische Informationen wie die CellID nicht möglich.

WP8 OS besitzt den gleichen Kernel wie Windows 8 und Windows RT. Die ARM-Prozessor Architektur wird von Windows RT unterstützt. Nach minimalen Änderungen am Quellcode, sollen selbstentwickelte APPs auf Desktop, Tablets und auf Windows Phones laufen.
Zur Entwicklung steht auch hier das kostenlose „*Visual Studio Express 2012“*[145] und das „*Windows Phone SDK 8*“ zur Verfügung.

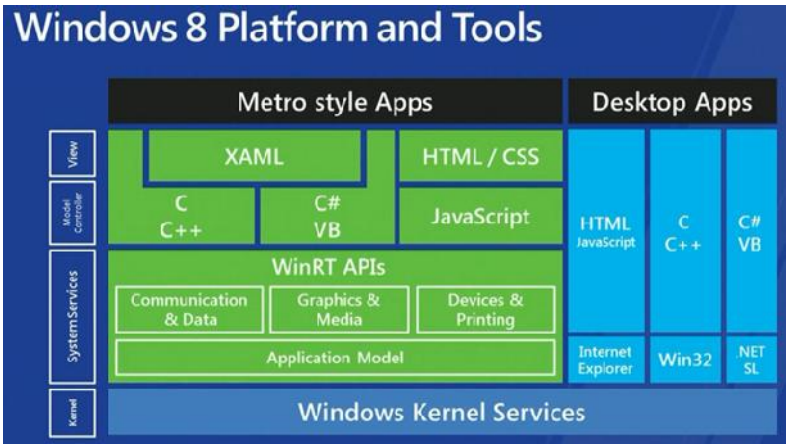


Abbildung 40: Windows 8 Platform and Tools, Quelle: www.buildwindows.com[146]

[144] Tsukasa Oi, Fourteenforty, “*Windows Phone 7 Internals and Exploitability”, 2011* Research Institute Inc. (FFRI)
[145] Entwicklungsumgebung für WP8: www.microsoft.com/visualstudio/deu/products/visual-studio-express-for-windows-phone [Stand 20.11.2012]
[146] Veröffentlicht auf der Microsoft „Build Konferenz“, 2011

4.3. Infrastrukturelle Gesamtkonzepte

4.3.1. Konzepte für die geschäftliche und behördliche Nutzung

Der BlackBerry Enterprise Service ist für große Unternehmen immer noch die erste Wahl wenn es darum geht, ein Smartphone in sichere Arbeitsprozesse einzubinden, auch wenn die iOS und Android Konkurrenz aufholt.

Muss hingegen eine erhöhte Geheimhaltungsstufe garantiert werden, kommen speziell entwickelte Endgeräte zum Einsatz. Die schon im vorhergehenden Teil angesprochenen „Krypto-Handys“[147] stehen seit über 10 Jahren zur Verfügung. Ein handelsübliches Gerät wird dazu modifiziert (gehärtet) und um sicherheitsrelevante Funktionen erweitert.

Komponenten:

- Verschlüsselung der lokalen Daten, Telefongespräche, SMS und E-Mails
- Schutz vor Veränderungen am Boot-ROM.
- Secure microSD-Speicherkarte mit signiertem Zertifikat
- Authentifizierung der Gesprächsteilnehmer
- Fernzugriff (Löschen) bei Diebstahl, sicheres Löschen/Überschreiben
- Härtung des Systems durch Blockieren von potenziell unsicheren Schnittstellen und Funktionen.
- Schließen von Backdoors und Exploits der Gerätesoftware
- Kernel-Protector, Prozesskontrolle und strenge Datenschutzrichtlinien

Ein zentraler Unterschied besteht in dem digitalen Zertifikat und einem Kryptografie-Controller, die sich beide in einem geschützten Bereich auf einer zusätzlichen Smartcard befindet, was auch als Hardware-Sicherheitsanker bezeichnet wird. Das darauf befindliche Zertifikat muss innerhalb einer Public Key Infrastruktur (PKI) erzeugt und verteilt werden.

Die Public Key Infrastruktur besteht aus:

[147] Eines der ersten „topSec“ Geräte wurde 2001 von Siemens und Rohde & Schwarz entwickelt, dass auf dem S35i Model basiert.

- Eine Zertifizierungsstelle (Certificate Authority) zum Erzeugen und Verwalten von digital signierten Zertifikaten
- Eine Registrierungsstelle (Registration Authority), die Zertifizierungsanträge prüft und gegebenenfalls an die Zertifizierungsstelle weiterreicht
- Einen Validierungsdienst (Validation Authority), der Zertifikate auf Echtheit überprüfen kann
- Einen Verzeichnisdienst (Directory Service), der die ausgestellten Zertifikate bereithält
- Zertifikatsperrliste (Certificate Revocation List) mit vorzeitig zurückgezogenen Zertifikaten
- Beim Inhaber (Subscriber) kann es sich um eine Person, Organisation, Hardware oder auch einen Serverdienst handeln
- Der Nutzer (Participant), der dem Zertifikat vertraut

Das erstellte Zertifikat besteht aus einem Schlüsselpaar, das sich aus dem öffentlichen Schlüssel (Public Key) und dem geheimen Schlüssel (Private Key) zusammensetzt.

- Der Public Key dient dem Absender zum Verschlüsseln einer Nachricht, die nur mit dem Private Key des Empfängers entschlüsselt werden kann.
- Der geheime Schlüssel des Absenders wird zur Signatur benutzt, damit der Empfänger sicher sein kann, dass der Absender authentisch ist.

Bei einem symmetrischen Kryptoverfahren hingegen, wie es bei der Challenge-Response Authentication im Kapitel 2 genutzt wird, besteht das Problem der Schlüsselverteilung, da jedes Kommunikationspaar einen gemeinsamen „Pre-Shared Key“ benötigt, der, wie der Name schon sagt, vorher ausgetauscht werden muss.
Bei einem asymmetrischen System können auch 1:n Relationen abgebildet werden, da ein öffentlicher Schlüssel von allen Absendern genutzt werden kann. Neben PKI werden auch HTTPS- und SSH-Verbindungen über asymmetrische Verfahren realisiert. Die nötige Infrastruktur wird im Normalfall von externen Dienstleister bereitgestellt.
Eine eigene PKI, um eine begrenzte Anzahl von Endgeräten untereinander zu authentisieren, kann sogar unter Nutzung von Open-Source-Software

bereitgestellt werden. Zur sicheren Kommunikation mit Geräten außerhalb der eigenen Gruppe müssen jedoch Stammzertifikate oder übergeordnete Zertifizierungsstellen genutzt werden.
Neben diesem hierarchischen gibt es auch ein verteiltes Vertrauensmodell (Web-of-Trust), bei dem sich die Nutzer untereinander als vertrauenswürdig einstufen können und es keine zentrale Zertifizierungsstelle gibt. In der Praxis hat das Modell aber auch Nachteile, da es zum einen manipuliert werden kann und zum anderen Rückschlüsse auf das Kommunikationsverhalten der Nutzer getroffen werden können.
Auf der anderen Seite ist das System aber robuster, wenn zum Beispiel einzelne Zertifikate kompromittiert werden. Gelangt bei dem hierarischen Modell ein Wurzelzertifikat in falsche Hände, kann das bedeuten, dass tausende Webseiten nicht mehr sicher sind.
Die Einbrüche bei großen Zertifizierungsdienstleistern wie VeriSign Inc[148] und Diginotar[149] zeigen, dass dieses Szenario durchaus eintreten kann.

Ein weiteres Argument ist die Schlüsselhinterlegung zur Lawful Interception, die nur durch den Betrieb einer eigenen Infrastruktur vermieden werden kann.

Grundsätzlich gilt das System aber als sicher, solange ausreichend lange Schlüssel verwendet werden. Theoretisch wäre es aber denkbar, dass es ein noch unbekanntes Faktorisierungsverfahren gibt, das in polynomieller Zeit den Private-Key ermitteln kann.

Ein weiteres Problem besteht darin, dass beide Seiten die gleichen Standards unterstützen müssen, um eine sichere Verbindung etablieren zu können.
SNS (Sichere netzübergreifende Sprachkommunikation) (vom BSI entwickelt) soll die Interoperabilität verschiedener Verschlüsselungssysteme ermöglichen. Dazu müssen sich die Endgeräte durch ein Verhandlungsverfahren beim Verbindungsaufbau zunächst auf einen gemeinsamen Betriebsmodus einigen.

[148] Reuters Artikel von Joseph Menn, „Key Internet operator VeriSign hit by hackers", 02.02.2012, www.reuters.com/article/2012/02/02/us-hacking-verisign-idUSTRE8110Z820120202 [Stand 24.11.2012]
[149] Reuters Artikel von Alexei Oreskovic, „Google to Iran: Change your password", 09.11.2011 www.reuters.com/article/2011/09/09/us-google-security-idUSTRE7885U320110909 [Stand 24.11.2012]

Ein Betriebsmodus[150] besteht aus einem Paket aus Diensten, Sprachkodierung und Sicherheitskonzept (Authentifizierung, Verschlüsselung), welches von den jeweiligen Endgeräten unterstützt wird.

Zunächst unterstützt das System TETRA-BOS[151] und den CSD-Kanal bei GSM. Somit können Sprachübertragungen und SMS-Nachrichten sicher übermittelt werden. Die nächste Version „SNS-over-IP" befindet sich seit 2012 in der Pilotphase. Mit dem „SNS-Starter-Kit" soll in Zukunft eine Entwicklungsumgebung zur Verfügung gestellt werden, die eine „Open-SNS Variante" enthält. Diese ist jedoch nicht für den VS-NfD (Verschlusssache, nur für den Dienstgebrauch) einsetzbar, weil der Starter-Kit nur den Teil des Aushandlungsprotokolls enthält und nicht die anschließende Verschlüsselung der Nutzdaten.

Krypto-Handys für den Dienstgebrauch, sogenannte „topSec"-Mobiltelefone für staatliche Einrichtungen, müssen höchsten Anforderungen entsprechen. Das von T-Systems entwickelte Simko (Sichere mobile Kommunikation) Konzept benutzt die SNS-Variante, die auch für den Dienstgebrauch zugelassen ist. Die Auswahl an Handy-Modellen ist jedoch sehr beschränkt. Die Hardwarebasis der Simko2 Handys wird von HTC geliefert. Für das neue Simko3 wird ein Samsung Galaxy S verwendet, das durch die Doppelkern-CPU zwei voneinander getrennte Teilbereiche realisieren soll. Ein Kern ist für die sicherheitsrelevanten Prozesse und Schnittstellen zuständig, der andere für Funktionen, die bei den Vorgängermodellen oft nur reduziert oder gar nicht vorhanden waren.

Eine abgeschwächte Simko-Variante wird von der Telekom als Enterprise-Lösung für Firmen vertrieben. Bei diesem Angebot lassen sich grundsätzlich alle Smartphones einsetzen, die ein SD-Kartenslot besitzen. Der Überwachung durch staatliche Behörden können sich diese abgeschwächten Geräte aber nicht entziehen.

[150] Quelle: „SNS Sichere Netzübergreifende Sprachkommunikation", Bundesamt für Sicherheit in der Informationstechnik, 2012

[151] „Terrestrial Trunked Radio" ist eine Bündelfunktechnik, die zur Kommunikation von Polizei, Behörden aber auch Industrie- und Verkehrsbetriebe genutzt wird. BOS steht für Behördenfunknetz. Siehe hierzu auch Kapitel 2.3.3.

4.3.2. GSM/UMTS Gateway für kleine Firmen und den privaten Gebrauch

Eine Gegenmaßnahme, durch die der größte Teil aller Angriffsvektoren eliminiert werden könnte, ist der Einsatz einer GSM/UMTS-Gateway, der Anrufe zwischen Mobilfunknetz und VoIP vermitteln kann. Nur das Audiosignal wird weitergeleitet. Alle Signalisierungen, die im Mobilfunknetz auftreten, enden an der SIM-Karte. Auch der SMS-Empfang und der Versand ist über diese Gateways möglich.

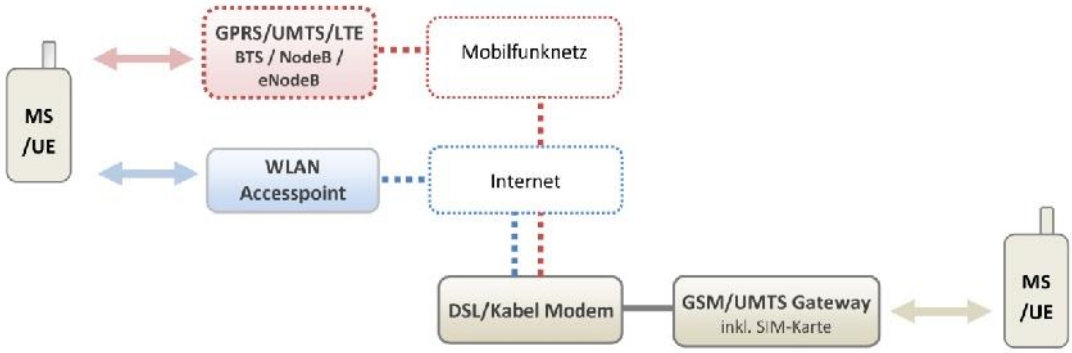


Abbildung 41: GSM/UMTS Gateway

Die SIM-Karte muss dazu im Router betrieben werden, der Anrufe und SMS an einen lokalen VoIP-Client weiterleitet. Ein Smartphone, das über VPN mit dem Home-LAN verbunden ist kann den Anruf auch dann annehmen, wenn er sich in einem fremden Netzwerk befindet. Für eine Datenverbindung über das Mobilfunknetz, ist natürlich eine zusätzliche SIM-Karte nötigt, bei der es sich aber um eine „anonyme“ Prepaid-Karte handeln kann.

4.4. Zusammenfassung

Gegen die Angriffsvektoren, die auf Dienste und Schnittstellen der Mobilfunktelefonie abzielen, werden von keinem Betriebssystem besondere Gegenmaßnahmen ergriffen. Es fehlen zum Beispiel der Cipher-Indikator, Zugang zu den unteren Protokollebenen der GSM/UMTS-Verbindung, SMS-Filter und eine Firewall.
Die Sicherheitsmechanismen wie Sandboxing und der beschränkte Zugriff auf den Baseband-Bereich sind zwar effektive Maßnahmen gegen klassische Angriffe, aber sie verhindern gleichzeitig, dass die oben genannten Funktionen nachgerüstet werden können. Auf der Ebene der APP-Entwicklung sind die meisten Gegenmaßnahmen nicht realisierbar. Dazu müsste tiefer in das System eingegriffen werden, was nur bei der Android Plattform möglich ist.

Würde man die Kommunikation, die zwischen der SIM-Karte und dem Baseband Prozessor stattfindet, abfangen, könnten die fehlenden Informationen gewonnen werden, ohne den Beschränkungen des Betriebssystems ausgeliefert zu sein. Ein weiterer Vorteil ist, dass diese Schnittstelle einen einheitlichen Standard benutzt - somit wäre diese Lösung in jedem Smartphone einsetzbar.

5 Lösungsoptionen

5.1. Konkrete Entwicklung

Alle bisherigen Methoden, die bei den erwähnten Arbeiten und Projekten eingesetzt wurden, um die Daten der unteren Protokollschichten zu analysieren, wurden mit einer eigenen Infrastruktur[152] in einer kontrollierten Umgebung durchgeführt.

Eine benutzerfreundliche Lösung gegen die Angriffsvektoren des Schwierigkeitsgrads 3, die ohne den Eingriff in systeminterne Abläufe auskommt, wie es am Anfang dieser Arbeit gefordert wurde, ist nach heutiger Beurteilung nicht möglich. Somit kommt als Lösung nur ein autonomes Zweitgerät in Betracht, das als Gateway eingesetzt wird, oder im Falle des fB-Detectors alle benötigten Messungen der Funkkanäle durchführen kann. Das hätte auch den Vorteil, dass eine anonyme SIM-Karte benutzt werden könnte.
Das Osmocom Projekt wurde schon an verschiedenen Punkten genannt. Es besteht unter anderem aus der quelloffenen Software „OsmocomBB“ für das GSM-Baseband, die Treiber für das Modem (Calypso DBB, IIota ABB, Rita R/F-Frontend) und eine Implementierung der GSM Protocol Layer 1 bis 3 beinhaltet.

Das quelloffene Smartphone-Betriebssystem „OpenMoko™“ (Open Mobile Kommunikations) benutzt diese OsmocomBB-Modem-Firmware in ihren Geräten, die über ein Calypso-Board verfügen, wie das „Neo 1973“ in der folgenden Abbildung.

Abbildung 42: Neo 1973 mit OpenMoko, Quelle: www.hightech-edge.com

[152] Die Infrastruktur wird oft durch die Osmocom Projekte realisiert, die unter cgit.osmocom.org/cgit aufgelistet sind.

Abbildung 43: G-Mate Dual SIM Adapter, Quelle: www.skyroam.com

Der Bluetooth-Dual-SIM-Adapter „G-Mate“, besitzt ebenfalls alle nötigen Schnittstellen für Telefonie und Datendienste, kostet[153] aber nur einen Bruchteil vom Neo-Smartphone. Der Adapter kann über Bluetooth von einem zweiten Smartphone ferngesteuert werden und so einen Anruf initiieren oder SMS versenden. Mit dem Dual-SIM-Adapter könnten fB-Detector, PDU-Filter oder Layer 2/3 Firewall realisiert werden. Leider gibt es nach Aussage des Herstellers noch kein Development Kit für Entwickler.
In der Standardkonfiguration könnte der Adapter jedoch einen „Roving-Bug“ erfolgreich abwehren, da das Gerät kein integriertes Mikrofon besitzt.

Eine große Auswahl an Lösungsansätzen findet man bei Projekten, die ein „Software Defined Radio“[154] (SDR) zur Realisation benutzen. Dieser Ansatz versucht den Baseband-Bereich durch Software nachzubilden, die auf einem Standard PC läuft, wodurch die Entwicklung vereinfacht und das Ergebnis flexibler einsetzbar wird.
Die kostenlose und quelloffene Software „GNU Radio Development Kit“[155] strukturiert den SDR-Ansatz weiter, indem es einzelne Module bildet, die jeweils für bestimmte Aufgaben zuständig sind. Die Rechenintensive A/D-, D/A-Wandlung kann dadurch auf die dafür spezialisierte Recheneinheit (DSP) auf der Soundkarte verlagert werden.
Die Programmierung erfolgt mit Python und bei zeitkritischen Abläufen mit C++, als Entwicklungsumgebung dient Eclipse.

[153] Das NEO 1973 kostet etwa 600 Euro. Der Preis eines G-Mate beträgt 70 Euro
[154] Das „Software Defined Radio Forum“ besteht aus einem internationalen Zusammenschluss von Industrie, Forschung und Regierungsstellen zur Förderung von SDRs
[155] GNU Radio Development Kit “GNU General Public License (GPL) version 3” gnuradio.org [Stand 10.11.2012]

Bei dem darauf folgenden „Universal Software Radio Peripheral“[156] (USRP) wurde besonders die Hardware im RF-Front End verbessert, um auch breitbandigere Signale in einer besseren Qualität verarbeiten zu können.
Auch wenn zu Beginn dieser Arbeit die Erkennung bzw. Gegenmaßnahmen direkt am Smartphone favorisiert wurde, musste an dieser Stelle auf Lösungswege eingegangen werden, bei denen ein PC oder ein Notebook benötigt wird.

Zudem gibt es bereits Portierungen[157] für Android sowie iOS.

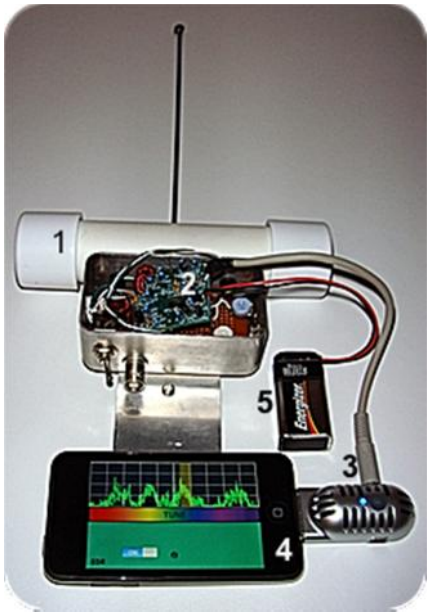


Abbildung 44: iSDR RF-Front End, Quelle: digitalconfections.com

Als Funkempfänger muss ein „Quadrature Sampling Detector (QSD)“ RF-Front End über den Mikrofoneingang mit dem Smartphone verbunden werden.

Außerhalb der Open-Source Gemeinde gibt es eine Vielzahl von kommerziellen Development-Kits, wie unter anderem:

- Texas Instruments „Bluetooth Sensor Tag”, “RF-Fronted”
- Programmable Modems z.B. Sierra Wireless “Airlink Embedded 3G Router”
- Mobile Hotspots z.B. Novatel mit Linux SDK
- Firma Ettus bietet USRP- und RF-Development-Kits
- Arria V FPGA RF Development Kit

[156] Das USRP wurde für das GNU Radio Projekt, von Matt Ettus Entwickelt
[157] iSDR für iOS, itunes.apple.com/us/app/isdr/id480077371?mt=8 [Stand 25.1..2012]

5.1.1. f-BTS-Detector

In diesem Abschnitt werden die zahlreichen Realisationsmöglichkeiten zusammengefasst und in Projektphasen aufbereitet.

- Phase 1: Entwicklung einer APP, die Informationen der OpenCellID-Datenbank auf einer Karte darstellen kann. Lokalisierung des eigenen Standortes und Abfragen der Zelleninformation über die vorgegebene „Telephony"-Klassen. Aktualisieren der OpenCellID-Datenbank. Vergleich der ermittelten Werte: RSSI, Cell-ID usw. (Im Zustandsdiagramm mit „Listening", „Save Data" und „Daten vergleich" bezeichnet)
- Phase 2: Optimieren der Informationsgewinnung durch gerätespezifische SDKs und/oder Entwicklung einer autonomen Hardwarelösung, zum Beispiel in Form eines „Bluetooth-Dual-SIM-Adapter" wie oben beschrieben. Datenbank erweitern mit Informationen über Score Werte der Basisstationen.
- Phase 3: Serverseitige Organisation der Clients, die sich in der Region aufhalten, um eine Ortung der „Fake-Basestation" durchzuführen. Warnung vor einer fB, die sich in Empfangsreichweite befindet.

Android OS bietet die meisten Vorteile, um mit einer Softwareentwicklung zu beginnen. Das System ist relativ offen, es existiert eine ausführliche Dokumentation und viele Entwickler-Community, die ebenfalls an Anwendungen für das Mobilfunknetz arbeiten. Die entsprechende APP für iOS sowie eventuell auch für BlackBerry OS und WP8 OS könnte zu einem späteren Zeitpunkt als Client, auf dem Niveau der Phase 1, erfolgen.

Bei einer zu starken Reduzierung der Funktionen in Tabelle „fB-Detection" würde die Software wahrscheinlich keinen Nutzen mehr erzielen, weil zu wenig Parameter in die Entscheidung mit einfließen. Besonders in Stadtgebieten kann durch die umliegenden Gebäude die Messung der Signalstärke und des Abstandes zur Basisstation verfälscht werden.

5.1.2. PDU-Filter

Die vom MS eintreffenden Nachrichten werden vom SIM-Toolkit, das sich auf der Karte befindet, entgegengenommen und in der „Java Virtual Machine“ ausgeführt. Dieser Lösungsansatz wurde in Kapitel 4 untersucht.

Die SIM-Karte ist ein zentraler Angriffspunkt, über den kostenbehaftete Dienste ausgeführt werden können. Die Kommunikation zwischen Baseband-Prozessor und SIM-Karte kann vom Applikations-Prozessor sehr schlecht kontrolliert oder unterbunden werden, so dass eine andere Instanz an dieser Stelle den Datenverkehr mitlesen müsste. Die so genannte Turbo-SIM wird zusammen mit einer Micro-SIM inklusive Adapter in den dafür vorgesehen Kartenschlitten gesteckt.

Abbildung 45: Turbo-SIM der Firma Bladox, Quelle: Eigene Herstellung

Danach können zusätzliche SIM-Toolkit (STK) Anwendungen[158] auf den Turbo-SIM installiert werden. Für den Microcontroller (Typ: ATMEL ATmega128L[159]), der sich auf der zweiten SIM befindet, gibt es eine umfassende Dokumentation und Quellcode, der genutzt werden kann. Ab Werk befinden sich bereits Anwendungen auf der Turbo-SIM, um SMS zu verschlüsseln und Daten sicher speichern zu können. Über diesen Umweg müsste auch der aktuell verwendete Algorithmus („Administrative Cipher Bit“[160]) zu ermitteln sein.

[158] Diese Anwendungen sind bei iOS unter „Einstellungen“>„Telefon“>„SIM-Anwendungen“ und bei Android OS über die STK-APP zugänglich. VORSCHLAG: Keine „“ sondern stattdessen kursiv,: *Einstellungen > Telefon >SIM-Anwendungen*. Bessere Lesbarkeit
[159] Datenblatt unter: www.atmel.com/images/2467s.pdf [24.10.2012]
[160] ETSI Standard 300 977 GSM 11.11, siehe 10.3.18

Adapter, die über I/O Ports verfügen, haben auch eine etwas größere Bauform. Damit können die Daten über NFC oder WLAN an den AP übertragen und direkt ausgewertet werden.

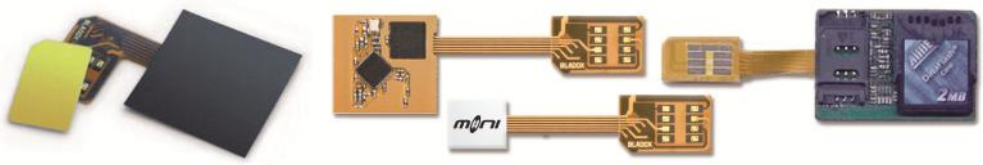


Abbildung 46: NFC und WLAN (Turbo BRA, Turbo Mini), Quelle: Bladox.com

Ein SIM-Tracer, wie er im osmocom Projekt benutzt wird benötigt allerdings einen PC der über die USB Schnittstelle die auszuwertenden Daten erhält. Im täglichen Gebrauch wäre die Realisation mit einem Proxy-SIM aber praktikabler, da die nötigen Bauteile im Smartphone platziert werden können und ohne einen zusätzlichen Computer auskommen.

Dieser SIM-Tracer wurde genutzt, um die übermittelten Daten zwischen SIM und Baseband Bereich abzufangen.

Abbildung 47: Osmocom SIM Tracer und HTC Wildfire, Quelle: Eigene Produktion

Die Hardware wird mit der USB Schnittstelle eines Linux-Rechners verbunden und die SIM-Karte wird in den dafür vorgesehen Schlitten, auf dem Tracer eingeführt. Die Software „Wireshark“ die zur Netzwerkanalyse genutzt wird, muss mit einer zusätzlichen Osmocom-Library erweitert werden, damit die „getraceten“ Daten ausgewertet werden können.

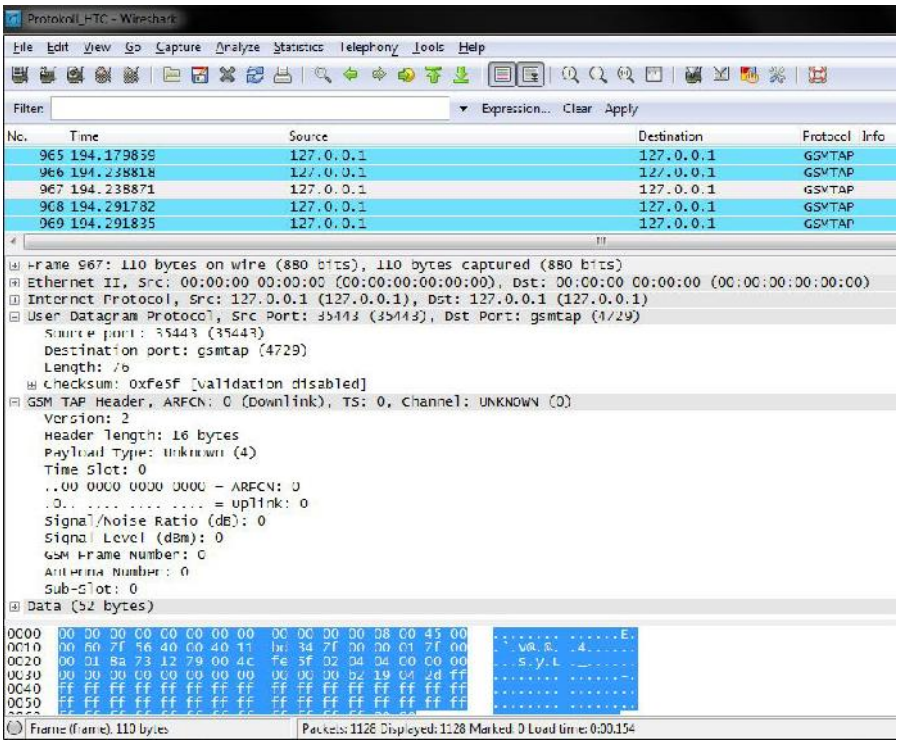


Abbildung 48: Wireshark Ausgabe

Diese Informationen könnten auch mit den zuvor beschriebenen Turbo-Produkte ermittelt werden.

5.1.3. Layer 2/3 Firewall und IDS

Eine Firewall mit IDS, wie sie auf Desktop Computern oder in Routern eingesetzt werden, würde die Rechenleistung merklich beeinträchtigen und die Betriebszeit des Akkus stark verkürzen. Die Umsetzung sollte eher aus wenigen Filterregeln bestehen, die sich aus der Untersuchung vom A07 (Fehlender Cipher Indicator), B07 (Stille-SMS) und B15 (Entladen des Akkus) ableiten lassen.

Zusätzlich sollte das selbstständige Ausführen von Code und Hyperlinks, Versenden von SMS-Nachrichten und Initiieren von Anrufen sowie das Ausführen von USSD-Codes (E11) unterbunden werden. Die Zugriffsberechtigungen der APPs, die neu installiert wurden, sollten zunächst komplett blockiert werden, um beim ersten Programmstart jeder Aktion explizit zustimmen zu können. So wird für jede Applikation ein individuelles Regelwerk erstellt, das unnötige Zugriffe auf Ressourcen vermeidet. Natürlich sind auch an dieser Stelle nur die risikobehafteten Aktionen in Betracht zu ziehen.

5.2. Entwicklungsaufwand und Nutzen

Um letztendlich die Effizienz einer Lösung beurteilen zu können, muss zunächst der Aufwand und der erzielte Nutzen untersucht werden. Da es sich hierbei um Schätzungen handelt, wird ein relativ abstrahierter Wertebereiche vom 1 bis 10 festgelegt, der am Ende einem Trend zugewiesen werden kann. Die Berechnung sollte gut nachvollziehbar sein, ohne wichtige Faktoren auszuschließen.

1. Der Entwicklungsaufwand steht in jedem Fall in direkter Beziehung zu den drei Schwierigkeitsgraden (Sg), die in Kapitel 3.5. definiert wurden. Damit lässt sich über den Sg einen möglichen Wertebereich innerhalb einer Skala festlegen.

- Sg = 1; zwischen 1 - 100 Prozent
- Sg = 2; zwischen 30 - 100 Prozent
- Sg = 3; zwischen 50 - 100 Prozent

Die Aufwendungen (I_a) setzten sich konkret aus der Zeit (t) und dem Kosten (k) zusammen. Beide Elemente werden gleichgewichtet gesehen und besitzen jeweils einen Wert zwischen 1 und 10.

t = Zeit zur Entwicklung (a) und Einführung (b)

- a) Gibt es bereits eine fertige Anwendung? (1 Punkt)
  Nutzbarer Quellcode? (mind. 2 Punkte)
  SDK oder Framework? (mind. 3 Punkte)
  Keine Unterstützung (5 Punkte)
- b) Wie viel Zeit wird für die Einführung benötigt?
  z.B. Dauer des Beta-Tests, Installation und Konfiguration des Systems
  (wenig 1 - viel 5)

$t = (t_a + t_b)$; Wertebereich von t = 1 bis 10 Punkte

k = Die finanziellen Aufwendungen bestehen aus:

- a) Investitionskosten, z.B. Entwicklungskosten, Lizenzen (1=nieder bis 5=hoch)
- b) Betriebs- und Wartungskosten (1=nieder bis 5=hoch)

$k = (k_a + k_b)$; Wertebereich von k = 1 bis 10 Punkte

Aufwand $I_a = (k * t)$; Wertebereich I_a = 1 bis 100 Punkte

2. Der Nutzen könnte theoretisch durch den nicht eingetretenen Schaden beziffert werden, der letztlich auch aus einer finanziellen und einer zeitlichen Komponente besteht. Mit dem Unterschied das es auf der Schadensseite auch zu immateriellen Beeinträchtigungen kommen kann, die noch viel weniger bezifferbar sind.

Eine Bewertung des Nutzens, kann also nur anhand der Verbesserung des Sicherheitsniveaus erfolgen. Bei dieser Definition kann also auch von der Effektivität einer Lösung gesprochen werden.

Ein Punkt entspricht maximal 10%. Zum Beispiel:

- 1 Punkte = 10% kaum Veränderung
- 5 Punkte = 40% - 60%
- 10 Punkte = maximal 99,9% Verbesserung

Bezeichnung	**Zeit**	**Kosten**	**Aufwand (1-100)**	**Effizienz**
fB-Detector APP	Entwicklung: 3	Investition: 2	12	0% - 30%
	Einführung: 1	Betrieb: 1		
	Gesamt: 4	Gesamt: 3		
fB-Detector Hardware	Entwicklung: 5	Investition: 4	51	30% - 90%
	Einführung: 4	Betrieb: 2		
	Gesamt: 9	Gesamt: 6		

Tabelle 2: fB-Detector, Berechnung Aufwand/Effizient

Der tatsächliche Aufwand der Gegenmaßnahme ist auch von dem Betriebssystem und der verwendeten Hardware abhängig, was in der Abbildung durch die ovale Fläche Ausgedrückt wird.

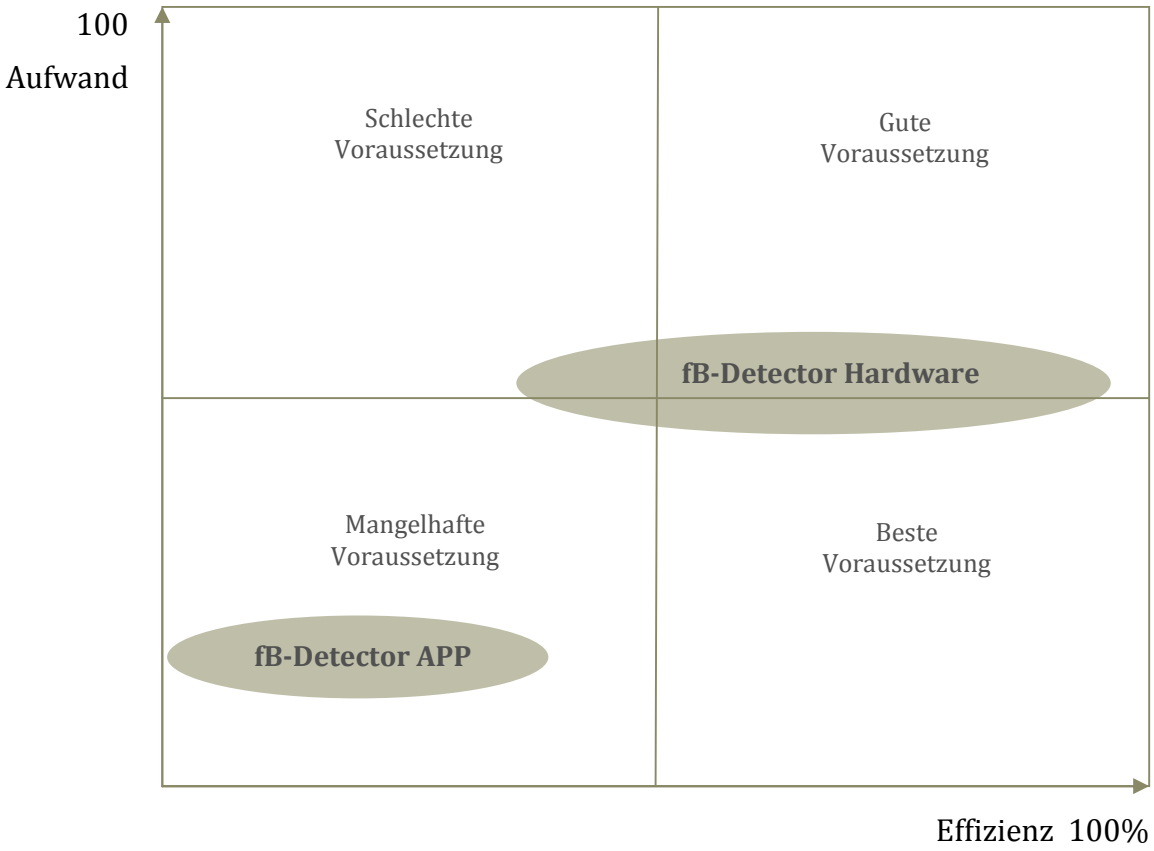


Abbildung 49: Aufwand/Nutzen fB-Detector

Als Ergebnis kann festgehalten werden, dass auf Applikationsebene keine Zuverlässige Erkennung möglich ist. Die Hardwarelösung verfügt dagegen über gute Voraussetzungen, ihr Ziel zu erfüllen, wenn ausreichend große Anstrengungen betrieben werden.

Bezeichnung	Zeit	Kosten	Aufwand (1-100)	Effizienz
PDU-Filter	Entwicklung: 4	Investition: 4	35	50% - 60%
	Einführung: 3	Betrieb: 1		
	Gesamt: 7	Gesamt:5		
Layer 2/3 Firewall	Entwicklung: 5	Investition: 5	70	80% - 95%
	Einführung: 5	Betrieb: 2		
	Gesamt: 10	Gesamt: 7		

Tabelle 3: PDU-Filter und L2/3-Firewall, Berechnung Aufwand/Effizient

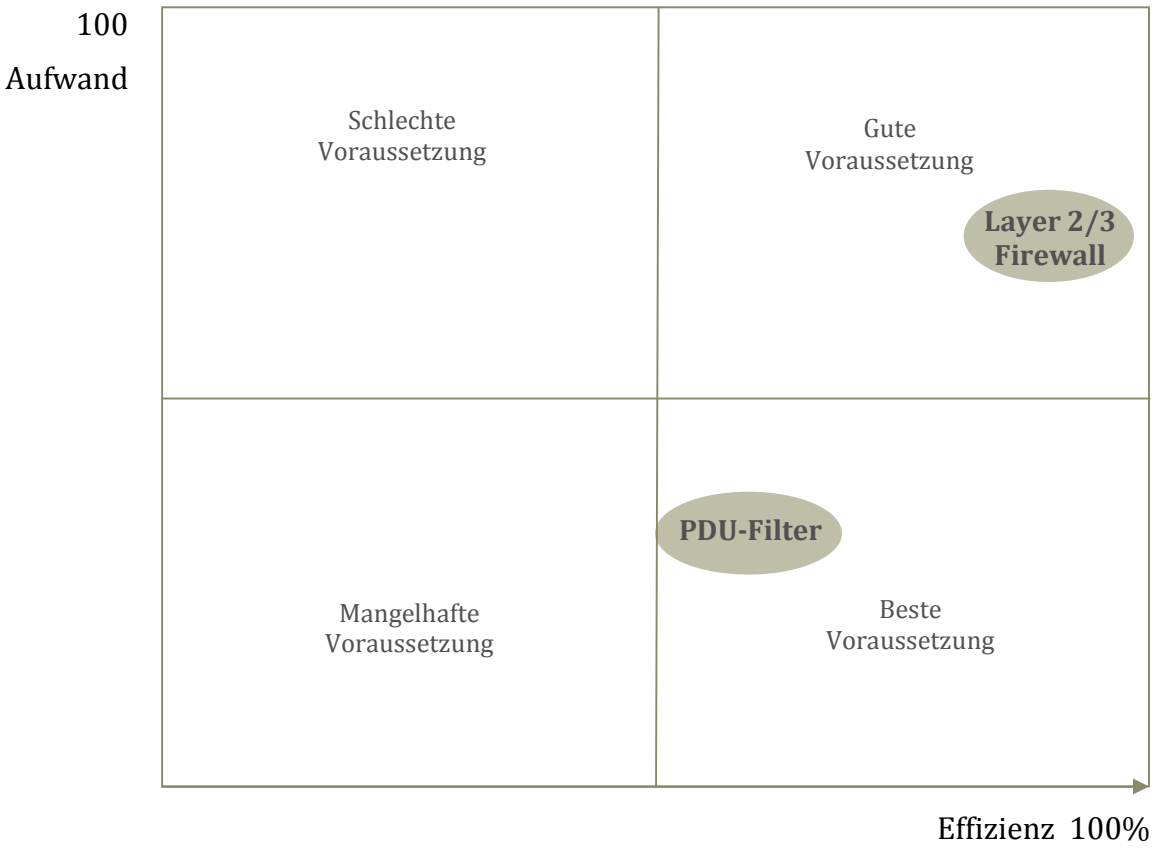


Abbildung 50: Aufwand/Nutzen PDU Filter, L2/3 Firewall

Die Entscheidung, welcher Ansatz verfolgt werden sollte, hängt auch von der Benutzerfreundlichkeit ab. Da eine Layer 2/3 Firewall aus verschiedenen Gründen, besser auf der Basis externer Hardware verwirklicht werden sollte, ist die integrierte Lösung des PDU-Filters vorteilhafter für den täglichen Gebrauch.

5.3. Handlungsvorschläge bei der Nutzung von Smartphones

Im Allgemeinen fehlen im Consumer-Bereich sicherheitsrelevante Vorkehrungen, die im professionellen Bereich zum Standard gehören, was auf zwei Gründe zurückzuführen ist. Der Preis sowie die Bedienerfreundlichkeit sind zentrale Verkaufsargumente, die von Privatkunden eher wahrgenommen werden als Sicherheitsfunktionen, die kaum jemand nachvollziehen kann. Aus Sicht der Hersteller gibt es auch keinen Grund die Kunden über eventuelle Sicherheitsprobleme aufzuklären, solange niemand gewillt ist dafür auch mehr Geld auszugeben. Daher wären geschlossene Systeme, wie sie von Apple und Microsoft angeboten werden, für die meisten Nutzer die bessere Wahl.

Für diese Systeme gibt es dann aber auch nur eine sehr kleine Auswahl an APPs, die gegen Bedrohungen wie Viren, Trojaner oder bösartige APPs vorgehen können.

Die meisten Angriffe finden seit längerer Zeit explizit gegen Android-Smartphones statt, die teilweise sogar auf bestimmte Fehler einzelner Modelle spezialisiert sind. Der Grund ist neben der hohen Verbreitung auch die Fragmentierung der Soft- und Hardware, die in der folgenden Tabelle verdeutlicht werden soll.

<table>
<tr><th>Kernel</th><th>Plattform</th><th>Herstellung</th><th>Vertrieb</th></tr>
<tr><td>Open Mobile Alliance
Linux Systemkern
GPL2 Lizenz</td><td>Google
Dalvik VM, Google-APPs
Apache-Lizenz
Außer die vorinstallierten Google APPS</td><td>Hardwarehersteller
Firmware / Treiber
Geschlossener Bereich</td><td>Provider
Vorinstallation von APPS (Auch von Drittanbietern)</td></tr>
<tr><td colspan="2">Windows Phone OS
komplette Eigenentwicklung – kein offener Quellcode</td><td>Hardwarehersteller
Firmware / Treiber</td><td>Provider</td></tr>
<tr><td colspan="3">Apple iOS
komplette Eigenentwicklung – kein offener Quellcode</td><td>Provider</td></tr>
<tr><td colspan="3">RIM BlackBerry OS
komplette Eigenentwicklung – kein offener Quellcode</td><td>Provider, IT-Firmen</td></tr>
</table>

Abbildung 51: Fragmentierung der Betriebssysteme

Android kann aber trotzdem - oder gerade wegen der Offenheit eine gute Lösung für den privaten und auch für den geschäftlichen Einsatz darstellen. Es setzt jedoch voraus, dass der Nutzer ein gewisses Maß an Fachwissen besitzt und sich selbstständig um sicherheitsrelevante Fragen kümmert. In sicherheitskritischen Umgebungen, besonders bei behördlicher Nutzung, wird dieses System oft bevorzugt. Das ist sicherlich in erster Linie den Lizenzbedingungen geschuldet aber auch zum Teil dem einsehbaren Programmcode und einem Misstrauen gegenüber geschlossenen proprietären Systemen.

Einrichtungen wie das Fraunhofer Institut[161], das BSI und die NSA favorisieren das Android-System als Basis bei eigenen Softwareentwicklungen. Rhode & Schwarz bietet ein „topSec Mobile Crypto Headset", das sich per Bluetooth mit einem Android-Smartphone verbindet lässt. Das dazugehörige APP leitet dann einen verschlüsselten Datenstrom an das Netzwerk weiter. Das Prinzip ähnelt der Hardware-Lösung für den fB-Detection und der Layer2/3 Firewall, nur das bei R&S eine sichere VoIP-Sprachkommunikation das Ziel war.

Damit bleibt festzustellen, dass ein externes Zusatzgerätgerät, das mit dem Smartphone interagieren kann, durchaus eine praktikable Lösung bei Sicherheitsproblemen bietet.

iOS eignet sich für den Enterprise-Bereich und bietet auch für Privatanwender ein robustes und sicheres Betriebssystem.

Windows Phone ist noch in einer relativ frühen Entwicklungsphase und kann erst mit der Version 8 im Unternehmensumfeld eingesetzt werden.

Für RIM wird sich bei der kommenden BlackBerry Version 10 entscheiden, ob es weiterhin seinen Marktanteil halten kann. Das Sicherheitskonzept das innerhalb einer eigenen BES Infrastruktur eingebettet ist, bietet das höchste Sicherheitsniveau, setzt aber auch einen größeren Betriebsaufwand voraus.

Android eignet sich sehr gut für den semi-professionellen Einsatz, wie auch im topSec-Bereich. Für die meisten Unternehmen ist Android aber nicht besonders interessant, da Google ein sehr zentralistisches Konzept der Datenhaltung verfolgt.

[161] Sven Bugiely, Lucas Daviy, Alexandra Dmitrienkoz, Stephan Heuserz, Ahmad-Reza Sadeghiy,z, Bhargava Shastry, "Practical and Lightweight Domain Isolation on Android", Fraunhofer SIT und TU Darmstadt,, http://www.trust.informatik.tu-darmstadt.de/fileadmin/user_upload/Group_TRUST/PubsPDF/spsm18-bugiel.pdf [Stand 28.11.2012]

Außerdem ist Google sehr weit vom Endkundengeschäft entfernt. Niederlassungen von Microsoft und Apple gibt es in vielen Ländern, die mit den bestehenden Vertriebswegen ihrer Hard- und Software bessere Voraussetzungen für Firmenkunden haben.

MDM und PKI sollten auf jeden Fall zum Standard gehören, um Infrastrukturen bei Firmen, Behörden und allgemein in sicherheitsrelevanten Bereichen zu sichern.

Die Virtualisierung von Diensten wird auch im Mobilfunk immer häufiger eingesetzt werden. Mit Remote Controlled Application Systems (ReCAppS[162]) oder Remote Controlled Browser Systems (ReCoBS[163]), die auf einem entfernten Server laufen und die Produktivumgebung nicht gefährden. Unter anderem wird mit dieser Technik schon heute die Nutzung von Flash-Webseiten mit einem iPhone oder iPad ermöglicht.

Die allgemein bekannten Schwächen und Gefahren, die von 2G-Netzen und dem SMS-Nachrichtensystem ausgehen, werden uns die nächsten Jahre - und in manchen Regionen der Welt – sogar Jahrzehnte erhalten bleiben. Solange Smartphone mit GSM/EDGE-Empfänger ausgestattet werden ändert sich für den Nutzer eigentlich nichts, selbst wenn die 2G-Netze schon lange abgeschaltet sind.

Glücklicherweise besteht die Hoffnung, dass in wenigen Jahren die am Anfang des Kapitels erwähnten RF-Frontend von der Herstellerindustrie als Standard in Mobilfunkgeräten verwendet werden. Dadurch können die Empfangskanäle und Sendefrequenzen auch nach der Auslieferung per Softwareupdate auf die jeweiligen nationalen Gegebenheiten angepasst werden. Damit ist es theoretisch möglich, das komplette GSM-Frequenzband direkt am RF-Frontend zu deaktivieren.

Die Entwicklung in der Mobilfunk- sowie auch in der Festnetztechnik geht eindeutig in Richtung VoIP mit einem „All-IP Network“ als Übertragungsmedium. Bei LTE werden alle Komponenten vollständig auf IP-Vermittlungstechnik basieren. Das Zugangsnetz sowie das Kernnetz wird immer mehr mit günstigeren Standardkomponenten betrieben werden. Sowohl VoIP als auch die „End-to-End“-Verschlüsselung wird ebenfalls standardmäßig unterstützt werden.

---

[162] itWatch GmbH, “ReCAppS”, 06-2006, www.itwatch.de/download/ReCAppSFSde.pdf [Stand 28.11.2012]

[163] BSI, „ReCoBS- Grudlagen und Anforderungen”, 06-2006, [Stand 28.11.2012]

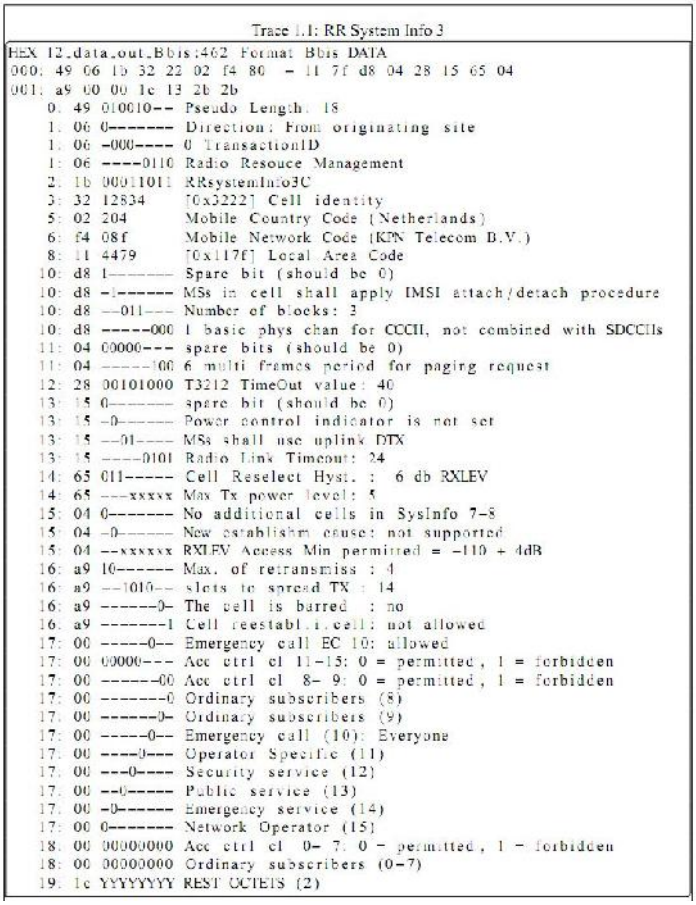
Der SMS-Dienst wird für die Nutzer immer uninteressanter, da mit dem Smartphone auch iMessage oder WhatsApp kostenlos genutzt werden kann. Interessant ist der Dienst dennoch, da er unabhängig vom Internet funktioniert und eine Möglichkeit bietet eine zusätzliche Identifikation durchzuführen. Zum Beispiel bei Bestellvorgängen in einem Onlineshop oder bei der Registrierung in einem Sozialen Netzwerk. Hierzu muss diese Technik aber sichere Methoden nutzen, um einen Mehrwert bieten zu können.

Die Konzentration auf das Internet und VoIP auf Anwendungsebene bringt wieder andere Sicherheitsprobleme mit sich.

Mit der Reduzierung von alternativen Kommunikationskanälen steigt die Abhängigkeit von der Funktionstüchtigkeit dieses Dienstes.

Ein weiterer Effekt lässt sich anhand der entstehenden Monokultur ableiten, in der die Spezialisierung der Schädlinge vorangetrieben wird und die Immunisierung gegenüber Abwehrmechanismen auftreten kann.

VI. Anhang



```
Trace 1.1: RR System Info 3
HEX 12_data_out_Bbis:462 Format Bbis DATA
000: 49 06 1b 32 22 02 f4 80  - 11 7f d8 04 28 15 65 04
001: a9 00 00 1c 13 2b 2b
    0: 49 010010-- Pseudo Length: 18
    1: 06 0------- Direction: From originating site
    1: 06 -000---- 0 TransactionID
    1: 06 ----0110 Radio Resouce Management
    2: 1b 00011011 RRsystemInfo3C
    3: 32 12834    [0x3222] Cell identity
    5: 02 204      Mobile Country Code (Netherlands)
    6: f4 08f      Mobile Network Code (KPN Telecom B.V.)
    8: 11 4479     [0x117f] Local Area Code
   10: d8 1------- Spare bit (should be 0)
   10: d8 -1------ MSs in cell shall apply IMSI attach/detach procedure
   10: d8 --011--- Number of blocks: 3
   10: d8 -----000 1 basic phys chan for CCCH, not combined with SDCCHs
   11: 04 00000--- spare bits (should be 0)
   11: 04 -----100 6 multi frames period for paging request
   12: 28 00101000 T3212 TimeOut value: 40
   13: 15 0------- spare bit (should be 0)
   13: 15 -0------ Power control indicator is not set
   13: 15 --01---- MSs shall use uplink DTX
   13: 15 ----0101 Radio Link Timeout: 24
   14: 65 011----- Cell Reselect Hyst. :  6 db RXLEV
   14: 65 ---xxxxx Max Tx power level: 5
   15: 04 0------- No additional cells in SysInfo 7-8
   15: 04 -0------ New establishm cause: not supported
   15: 04 --xxxxxx RXLEV Access Min permitted = -110 + 4dB
   16: a9 10------ Max. of retransmiss : 4
   16: a9 --1010-- slots to spread TX : 14
   16: a9 ------0- The cell is barred  : no
   16: a9 -------1 Cell reestabl.i.cell: not allowed
   17: 00 -----0-- Emergency call EC 10: allowed
   17: 00 00000--- Acc ctrl cl 11-15: 0 = permitted, 1 = forbidden
   17: 00 ------00 Acc ctrl cl  8- 9: 0 = permitted, 1 = forbidden
   17: 00 --------0 Ordinary subscribers (8)
   17: 00 ------0- Ordinary subscribers (9)
   17: 00 -----0-- Emergency call (10): Everyone
   17: 00 ----0--- Operator Specific (11)
   17: 00 ---0---- Security service (12)
   17: 00 --0----- Public service (13)
   17: 00 -0------ Emergency service (14)
   17: 00 0------- Network Operator (15)
   18: 00 00000000 Acc ctrl cl  0- 7: 0 - permitted, 1 - forbidden
   18: 00 00000000 Ordinary subscribers (0-7)
   19: 1c YYYYYYYY REST OCTETS (2)
```

Abbildung A01: Cell-Broadcast Quelle: GSM-Signals Communikation

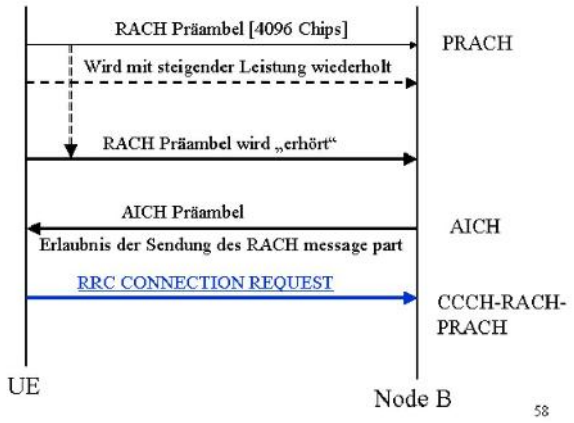


Abbildung A02: UMTS Connection Request Quelle: GSM-Traces, Informatik hu-Berlin 2012

A5-Algorithmen	A5/0	A5/1	A5/2	A5/3 GSM	A5/3 UMTS
		Stream-Cipher		Block-Cipher	
Schlüssellänge K_i	---	128 Bit	128 Bit	128 Bit	128 Bit
Sitzungsschlüssel K_c	---	64 Bit	64 Bit	64 bis 128 Bit	128 Bit

Tabelle T01: A5-Algorithmen

GEA-Algorithmen	GEA/0	GEA/1	GEA/2	GEA/3	GEA/4
		Stream-Cipher		Block-Cipher	
Schlüssellänge K_i	---	128 Bit	128 Bit	128 Bit	128 Bit
Sitzungsschlüssel K_c	---	64 Bit	64 Bit	128 Bit	128 Bit

Tabelle T02: GEA-Algorithmen

ASCII value	Character	Control character	ASCII value	Character	ASCII value	Character	ASCII value	Character
000	(null)	NUL	032	(space)	064	@	096	
001	☺	SOH	033	!	065	A	097	a
002	☻	STX	034	"	066	B	098	b
003	♥	ETX	035	#	067	C	099	c
004	♦	EOT	036	$	068	D	100	d
005	♣	ENQ	037	%	069	E	101	e
006	♠	ACK	038	&	070	F	102	f
007	(beep)	BEL	039	'	071	G	103	g
008	◘	BS	040	(	072	H	104	h
009	(tab)	HT	041	)	073	I	105	i
010	(line feed)	LF	042	*	074	J	106	j
011	(home)	VT	043	+	075	K	107	k
012	(form feed)	FF	044	,	076	L	108	l
013	(carriage return)	CR	045	-	077	M	109	m
014	♫	SO	046	.	078	N	110	n
015	☼	SI	047	/	079	O	111	o
016	►	DLE	048	0	080	P	112	p
017	◄	DC1	049	1	081	Q	113	q
018	↕	DC2	050	2	082	R	114	r
019	‼	DC3	051	3	083	S	115	s
020	¶	DC4	052	4	084	T	116	t
021	§	NAK	053	5	085	U	117	u
022	▬	SYN	054	6	086	V	118	v
023	↨	ETB	055	7	087	W	119	w
024	↑	CAN	056	8	088	X	120	x
025	↓	EM	057	9	089	Y	121	y
026	→	SUB	058	:	090	Z	122	z
027	←	ESC	059	;	091	[	123	{
028	(cursor right)	FS	060	<	092	\	124	|
029	(cursor left)	GS	061	=	093	]	125	}
030	(cursor up)	RS	062	>	094	^	126	~
031	(cursor down)	US	063	?	095	_	127	⌂

Abbildung A03: ASCI-Zeichen 7-Bit 1

PDU-Typen im SM-TL Layer[164]:		
NR	Bit 1 Bit 0	Message Type
1	0 0	SMS-Deliver: conveys a short message from an SMSC to the MS
2	0 0	SMS-Deliver-Report: conveys the cause of a failure to deliver
3	0 1	SMS-Submit: conveys a short message from an MS to the SMSC
4	0 1	SMS-Submit-Report: conveys the cause of a failure to submit
5	1 0	SMS-Status-Report: status report from SMSC to MS
6	1 0	SMS-Command: conveys command from MS to SMSC
7	1 1	Reserviert

Tabelle T03: PDU Typen beim SMS Versand, Quelle: ETSI GSM 3.40

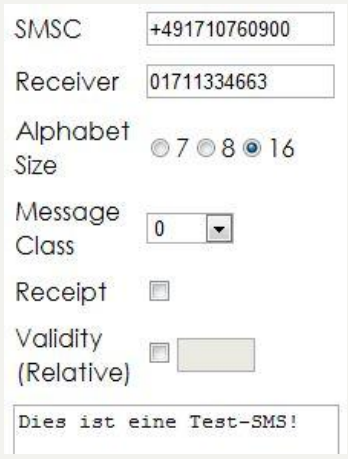
Beispiel einer Flash-SMS im PDU-Mode[165]		
Eingabe:	**Hexadecimal PDU-Message:**	**Ausgabe als PDU-Message:**
	AT+CMGS=59 07919471016790000100 0B8110173 14366F300182E0044006900650073 00200069007300740020006500690 06E006500200054006500730074002D0053004D00530021	SMSC#+491710760900 Receipient:01711334663 Validity: Not Present, TP_PID:00, TP_DCS:18, TP_DCS-popis: Uncompressed Text class:0 Alphabet:UCS2(16)bit Dies ist eine Test-SMS! Length:23

Tabelle T04: Beispiel einer SMS-Nachricht, Quelle: www.rednaxela.net/pdu.php

Class	Bit 1 Bit 0	Steuerungsbefehle für den Empfänger
0	0 0	Wird sofort auf dem Display angezeigt und nicht auf dem ME gespeichert
1	0 1	Wird vom ME interpretiert, zum Beispiel zur OTA-Konfiguration
2	1 0	Wird an die SIM-Karte weitergeleitet
3	1 1	Wird an Peripheriegeräte gesendet
		Bit 2: Wert=“ 0“ für 7bit Kodierung; Wert=“ 1“ für 8bit Kodierung Bit3: Wert= „0“ default

Tabelle T05 Codierungsgruppen des DCS[166] 1, Quelle: ETSI GSM 3.38 Kapitel 4

[164] Quelle: ETSI Standard GSM 3.40, Kapitel 9.2.2.
[165] Quelle: Converter für das PDU Format, Online im Internet: http://rednaxela.net/pdu.php, [01.08.2012]
[166] Quelle: ETSI Standard GSM 3.38, Kapitel 4

Access to this program is restricted to major corporations and governments under NDA (Non-Disclosure Agreement).

Threat Protection Levels

Basic Level	Enhanced Level	Comprehensive Level
• 30 credits(1) • Brief technical description • In-depth technical analysis • Workaround / mitigation(2)	• 40 credits(1) • Brief technical description • In-depth technical analysis • Workaround / mitigation(2) • Proof-of-concept (crash only)	• 50 credits(1) • Brief technical description • In-depth technical analysis • Workaround / mitigation(2) • Proof-of-concept (crash only) • Code execution exploit(2) • Attack Detection guidance(2)

(1) each research report costs 1 or 2 credits depending on the nature of the vulnerability
(2) when available

Pricing and Licensing

VUPEN Threat Protection Program is priced as a prepaid annual subscription based on the chosen level.

Abbildung A04-1: VUPEN 0-Day-Exloits

Access to this program is restricted to Intelligence and Law Enforcement Agencies under NDA (Non-Disclosure Agreement) in countries members or partners of NATO, ANZUS and ASEAN.

Abbildung A04-2: VUPEN Access

Zugangs-Voraussetzungen, Quelle: „279_VUPEN-Thread-Exploits“ Seite 2 von 3

Abbildung A05-1: Deutsche Firmen für Sicherheitstechnik

Abbildung A05-2: Phone-Monitoring

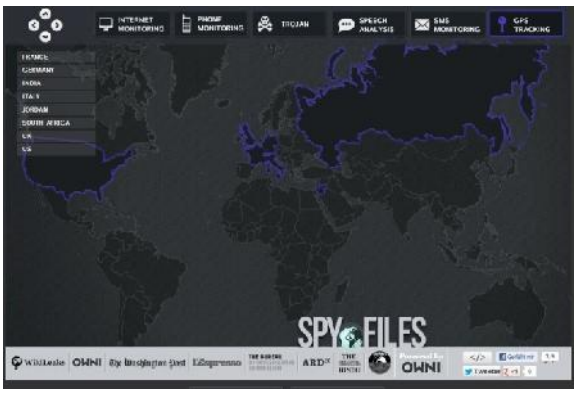


Abbildung A05-3: GPS-Monitoring

Abbildung A05-4: SMS-Monitoring

Quelle: SpyFiles/wikileaks.org

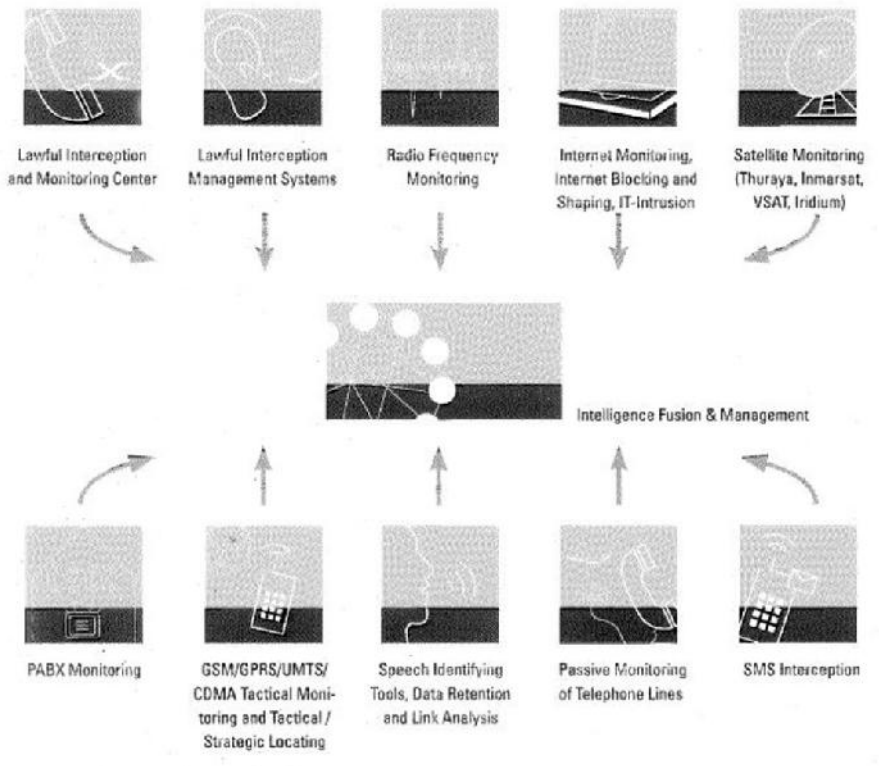


Abbildung A06: Gesamtübersicht LI

Quelle: Firma ELAMAN GmbH[167], Produktkatalog S.5 „188_201106-ISS-ELAMAN3.pdf“

[167] Firma ELAMAN GmbH, Produktkatalog „188_201106-ISS-ELAMAN3.pdf“, Seite 5

	SIM-Karte
Unveränderbare Werte	o SIM-Kartentyp o SIM-Seriennummer o Integrated Circuit Card Identifier (ICCID)(Je 2 digits für Telecom Id, Country Code, Network Code und weitere) o IMSI-Nummer o PIN & PUK o Liste der zusätzlich abonnierten Dienste o Sprache des Benutzers o Ki – Identity Key (Shared Secret)) o A3/A8 Algorithmen
Variable Werte	**Lokalisation der Zelle** o TMSI o LAI o Periodic Location Update - Zeitgeber o Aktualisierungsstatus
	Sicherheit & Verschlüsselung o RAND Zufallszahl 128Bit o SRES (A3 und RAND) 32Bit o Kc Cipheringkey (A8 und RAND) 64Bit o Administrative Data Field
	Verbindungsaufbau o BCCH-Liste (Trägerfrequenzen des Providers, zum Einbuchen oder zur Zellenauswahl beim Handover) o Liste der gesperrten PLMNs o Zeitdauer bis das ME versucht, sich in ein fremdes PLMN einzubuchen, wenn es das eigene nicht findet.

TabelleT06: Daten der SIM-Karte

Tabelle A07: der Angriffsvektoren

Luftschnittstelle (12)		
NR	Schwachstelle	Details
A01	A3/A8 Implementierung	Implementierungsfehler durch den Service Provider.
A02	Fehlendes Authentisieren der BTS gegenüber dem Smartphone	Ermöglicht einen „MITM“ Angriff. - IMSI-Catcher/fake Base Station - Dynamic SIM-Cloning - Semi-Aktive Anlagen
A03	IMSI - Request Location-Update IMEI-Request	Smartphone antwortet mit der unverschlüsselten IMSI. Abmelden eines MS am Netzwerk erzwingen. (IMSI muss dem HLR/VLR bekannt sein)
A04	Jammer	Störfunk > Unterbrechung > Provoziert neuen Verbindungsaufbau. Oder um eine UMTS Verbindung zu unterbinden.
A05	Femto-Zelle	Gehackte NodeB bei Vodafone. Durch Ausnutzen einer Softwarefehlers
A06	Verschlüsselung	Passives Mithören A5/1 /2
A07!	Fehlender Cipher Indicator	Kein Cipher Indicator vorhanden, wenn keine verschl. Verbindung besteht.
A08!	UMTS Integritätsschutz	Kann deaktiviert werden. Unverschlüsselte Übertragung ist auch bei UMTS möglich.
A09!	Hand Over	z.B. bei UMTS zu 2G. Im „Dedicated-Mode“ vom Netzwerk organisiert. Schwer zu manipulieren.
A10!	Fall-Back to GSM	UMTS Verbindung unterbinden - wird auch bei Semi-Aktiven Anlagen genutzt.
A11	GPRS Verschlüsselung	Passives Mithören bei GEA/1, GEA/2, GEA/3
A12	GPRS ohne Verschlüsselung	Provider schaltet Verschlüsselung ab

Legende: A-Funkschnittstelle**, B-**SMS, WAP und MMS**, C-**Providernetzwerk,
D-Lawful Interception**, E-**Schnittstellen des Smartphone
(*) = Kombination aus mehreren AVs, **(!) =** Schwachstelle - kein direkter Angriff möglich

SMS, WAP und MMS (16)		
NR	Schwachstelle	Details
B01	SMS Authentifizierung	Kein Authentifizieren des Senders oder Empfängers.
B02	Unverschlüsselter Versand der SMS	Keine Verschlüsselung der SMS möglich.
B03	SMSC Zustellung	Wird die SMS in das Internet weitergeleitet ist kein Schutz vorgesehen
B04	SMS MO-MT	BTS senden ein Broadcast an alle Empfänger einer Funkzelle. Direkter Versand ebenfalls möglich.
B05	WAP-Push SMS	Ausführbarer Link als SMS
B06!	Flash SMS	Text der Nachricht muss Unicode sein. Die Message Class „0“ steht für höchste Priorität. Das Feld „TP_DCS“ bekommt den Wert „18“
B07	Stille SMS	PDU Message
B08*	SMS Injection	PDU Message + AV-B04
B09*	SMS Botnetz	PDU Message + AV-B04
B10	GSM, USSD und MMI Codes	Änderungen an der Konfiguration oder Anzeigen von Informationen über das Smartphone
B11	MMS Authentifizierung	Kein Authentifizieren des Senders oder Empfängers.
B12	Unverschlüsselter MMS Versand	Verschlüsselung ist nicht vorgesehen
B13	WAP Abfangen des Profils und der IP	Bei WAP 1.0 wird nur bis zum MMS-Proxy MMS Proxy kann auch dazu missbraucht werden um einen e-Mail Push auf den Client zu erreichen
B14	MMS Transport	Kein Screening des Headers oder nach Schadsoftware oder Spam.
B15*	Entladen des Akkus MMS-Push	Smartphone wird zum ununterbrochenen Senden der gleichen Nachricht verleitet und entleert so das Akku.
B16	Synchronisation E-Mail-Konten, Kalender, Kontakte PIM-Daten…	MDM (Mobile Device Management) unverschlüsselte Speicherung in der Cloud

Legende: A-Funkschnittstelle**, B-**SMS, WAP und MMS**, C-**Providernetzwerk,
D-Lawful Interception**, E-**Schnittstellen des Smartphone
(*) = Kombination aus mehreren AVs, **(!) =** Schwachstelle - kein direkter Angriff möglich

Signalisierungen im Mobilfunknetz (3)		
NR	Schwachstelle	Details
C01	GSM Zugangs- und Kern-Netz	Keine Verschlüsselung vorgesehen
C02	UTMS Zugangs- und Kern-Netz	Verschlüsselung nicht zwingend notwendig
C03	Fremder Zugriff	Zugriff durch Drittanbieter auf Komponenten des Kern-Netzes des Providers. Angriffe auf HLR, VLR denkbar.

Signalisierungen aus fremden Netzen (3)		
NR	Schwachstelle	Details
C04	Caller ID-Spoofing	Anzeigen einer falschen Telefonnummer auf dem Display des Angerufenen. Durch ISDN Leistungsmerkmal *„CLIP no screening“*
C05!	Early Media Stream	Telefonieren ohne Verbindungsdaten und Kosten.
C06	SS7 Protokolle	Fehlende Sicherheitsfunktionen im Signalisierungsnetz

Lawful Interception (6)		
NR	Schwachstelle	Details
D01	Unlawful Interception	Missbrauch durch Insider oder Eindringlinge in das LI-System. (Angriff von innen)
D02	Mobile Geräte	Nutzung ohne Genehmigung möglich.
D03	Zero-Day-Exploits	Nutzen von unbekannten Sicherheitslücken
D04	LEA Domain und Schnittstellen	Angriff auf die Schnittstelle bzw. der Domain. Jede Komponente die Vermittlungsaufgaben erfüllt muss eine LI Schnittstelle besitzen. Also auch die BSC und RNC. (Angriff von außen)
D05	Klein Declaration	Auswerten des gesamten Datenverkehrs
D06	Schlüssel-hinterlegung	Fehlende Sicherheitsfunktionen im Signalisierungsnetz

Legende: A-Funkschnittstelle**, B-**SMS, WAP und MMS**, C-**Providernetzwerk,
D-Lawful Interception**, E-**Schnittstellen des Smartphone
(*) = Kombination aus mehreren AVs, **(!) =** Schwachstelle - kein direkter Angriff möglich

Schnittstellen am Smartphone (11)		
NR	Schwachstelle	Details
E01	GSM Injection	Direktes Einwirken auf den Empfänger
E02*	Roving Bug	Freischalten des Mikrofons ohne physikalischen Zugriff auf das Mobiltelefon und Senden der Audiodaten.
E03	SIM Cloning, Differential Power Analysis	Comp-128, Identitätsdiebstahl, Berechnen von Ki
E04	Auslesen der SIM	Kontaktdaten, SMS Nachrichten, Angerufene Nummern
E05	OTA (Over The Air)	Manipulieren der SMS, MMS und Proxy Konfiguration. Installation von Software auf dem Smartphone möglich.
E06	FOTA (Firmware Over The Air)	Manipulierte Firmware einspielen. Betriebssystem Updates.
E07	Bluetooth Verbindungs-Verschlüsselung	Abhören bei Verwendung eines Head Set etc. Standardeinstellungen: Verschlüsselung ist ausgeschaltet
E08	Bluetooth Interface	Auslesen Datenspeicher: Telefonbuch, SMS, E-Mail, Speicherkarte. Konfigurationsänderungen: Anrufe tätigen, Rufannahme, Weiterleitung, Lautlosschalten, zur Telefonkonferenz einladen
E09	WLAN Cross-Service-Attacks	Automatisches Verbinden und aktiviertes Interface.
E10	NFC Daten unverschl. / Kein Passwortschutz	Auslesen oder Speichern von Daten durch Unbefugte.
E11	QR Codes	Ausführen der Daten als Hyperlink, Aufbau eines Telefonats oder ausführen von Java-Skript möglich.

Standortbestimmung und Ortung (5)		
NR	Schwachstelle	Details
F01!	Ortung	Peilung über Providernetz. Keine Authentifizierung nötig. Ortungsinformationen werden unverschlüsselt übertragen.
F02	Lokalisieren über WLAN/Skyhook	Prüfung vom MS ausgehend. Scannen der WLAN Accesspoints im Umfeld.
F03	Ortung über eindeutige IDs	Prüfung von außen auf MS (lokal). Erkennen eindeutiger IDs wie IMSI, IMEI, MAC-Adresse, BD ADDR, RFID-Tag
F04	Pagin Channel (PCCH)	Abhören des PCCH in der vermuteten Region (Lokal). Verbindungsaufbau über Stille-SMS oder Stiller-Anruf der vor dem Klingeln abgebrochen wird. SS7 Lokalisierung im Kern-Netz
F05	APPS und Location Based Services	Prüfung von außen auf ME (International) mit Skype, Facebook oder Twitter-Accounts.

Tabelle A08: Funktionen des fB-Detectors

ID	Funktion	Details	Sonstiges
Physikalische Erkennung			
FB01	Signale & Informationen	Signale (ACFN, Signal to Noise, Bitfehlerhäufigkeit) Analysieren. Informationen im BCCH (LAC/LAI, Cell-ID, RSSI und BSIC/BCC) Auslesen und zusammen mit Standortdaten Abspeichern. Datenerfassung an mehreren geografischen Positionen und erstellen eines „Fingerprint“ von jeder Basisstation. Erkennen von Ereignissen die Teil eines Angriffs sein können. (zb FB02/03/04) oder CC-Tabelle	
	Quelle: Tabelle „Catcher-Catcher Projekt“		
	RED **je 50 Punkte**	o No encryption (after using encryption with the same operator before) o LAC is changing more than 1x o You are paged, but do not enter any transaction o Being assigned a traffic channel but not entering call control state/receiving a text message for 2 seconds **BLACK** …10 seconds	
	YELLOW **je 25 Punkte**	o Cipher mode complete message is sent more than twice. **RED** …more than four times o IMEI not requested in Cipher Mode Complete message o Cell is not advertising any neighbor cells o Cell reselection offset > 80db o The LAC of a base station changes 1x o The LAC differs from all neighboring cells o The network queries the phones IMEI during location update o The "IMSI attach procedure" flag is set o Receive a silent text message o You do not receive a call setup message while already being on a traffic channel for 2 seconds **RED** …10 seconds o Your phone sends at the highest possible power	

FB02	„Forced-Connection„	Die BTS mit dem schwächsten Signal wird imitiert / Anstieg der Signalstärke (RSS) um ein vielfaches.	Ereignis 1 50 Punkte
FB03	Tabellen der Nachbarzellen vergleichen	Die Tabelle (Neighbouring BTS)der umliegenden Stationen müssen auf die angegebene Signalstärke der aktuell verbundenen BTS, verglichen werden. Ist die aktuelle BTS auch in den Nachbarzellen als stärkste BTS geführt?	Ereignis 1 50 Punkte
FB04	Abweisung durch die BTS (fB)	Versucht das „falsche“ MS über den PRACH eine Verbindung aufzubauen und bekommt nach mehrmaliger Anfrage keine Antwort (Aloha beachten)	Auf dem Display Anzeigen
Geografische Erkennung			
FB05	Abstands-messung	Senden eines „Hello Packet-delay“ an die BTS. Auf gleiche Broadcasts achten die zeitverzögert eintreffen.	Bewertung kann erst später erfolgen.
FB06	E-OTD Lokalisierung	Testen des Mobilfunknetzes mittels Funktionen zur Ortung (LBS). z.B. eine BTS die nicht antwortet oder 2 Antworten einer BTS die sich zeitlich überschneiden.	Bewertung kann erst später erfolgen. Nutzen noch nicht bewiesen.
Informelle Erkennung			
FB07	Datenbestand, Server/Client	o Community teilt Datenstamm o Gleichzeitige Messung	fB Warnung auf dem Display Anzeigen
Erkennung spezieller Abhörtechniken			
FB08	Dyn. SIM-Cloning „Evidence in network“	o Ungewöhnliche “location update queries“ (IMSI) o Verzögerung und zählen der missglückten Versuche	Ereignis 1 50 Punkte
FB09	Semi-Aktive Erkennung	o Fall-Back to GSM Polling (durch Polling) o Hand-Over zu 2G (durch Polling) o UMTS-Jammer (Siehe FB11) o Paging Request	Die genaue Bewertung (Anzahl der Punkte) kann erst nach Tests erfolgen.

Weitere Merkmale			
FB10	Location-Fingerprint des IMSI/TMSI Verhältnis.	Protokollieren der gesendeten IMSIs / TMSIs und statistische Auswertung folgender Prozeduren: IMSI-Request, Location Update, IMEI-Request	Die genaue Bewertung kann erst nach Tests erfolgen.
FB11	Jammer / für UMTS Frequenz	plötzliche Frequenzstörungen bzw. der Verringerung des Signal-Rauschabstands erkannt werden. Eventuell wird nur das zwischen 1900 – 2200 MHz liegende UMTS Frequenzband gestört.	Störungen auf dem Display Anzeigen
FB12	Femtozellen Anzeigen	Datenbank wie unter FB07 beschrieben	Warnung auf dem Display Anzeigen
FB13	Cipher Indicator Anzeigen	Wie im GSM Standard beschrieben oder mittels Protokollierung der Schicht 3 im Protokollstack möglich.	Cipher Indicator auf dem Display Anzeigen
FB14	IMSI/IMEI Request	Anzahl der Anfragen/Zeit > Statistik Option: IMEI nie Senden oder IMEI ändern	

Tabelle 7: fB-Detector

VII. Glossar

ARM - Advanced RISC Machines

Lizenzgeber ist die Firma „ARM Limited“, die das Chip-Design an verschiedene Hersteller verkauft. Zum Beispiel: Apple, IBM, Infinion, Freescale, Intel, Atmel, Toshiba, Renesas, NXP, Nvida und Texas Instruments.

ROM-Kitchen

Ein Softwarepaket aus einzelnen Tools und einer Hauptanwendung, zur Generierung einer „Custom-Rom“, einer angepassten Distribution für ein bestimmtes Smartphone Modell. Bei Android und sogar Windows Phone können so die einzelnen Bestanteile des Betriebssystems, selbst zusammengestellt und erweitert werden.

Obfuscator

Der Begriff Obfuscator beschreibt die „Verschleierung“ des Quellcodes um Reverse Engineering zu erschweren. Der Deobfuscator ermöglicht die Rückführung in eine für Menschen verständliche Darstellungsform.

SDR - Software Defined Radio Forum

Das Forum besteht aus einem internationalen Zusammenschluss von Industrie, Forschung und Regierungsstellen zur Förderung von SDRs.

USRP - Universal Software Radio Peripheral

Diese Hardware wurde innerhalb des GNU Radio Projekts, von Matt Ettus Entwickelt. Die Firma Ettus bietet eine große Anzahl von Komponenten für die Softwareentwicklung in dem Bereich Mobilfunk benutzt wird.

VIII. Literaturverzeichnis

3GPP 3G TS 23.140 // 3rd Generation Partnership Project; Technical Specification Terminals; Multimedia Messaging Service (MMS); Functional description; Stage 2. - 2000-03.

3GPP Circuit Switched (CS) fallback in Evolved Packet System (EPS): Stage 2 // Technische Spezifikation TS 23.272. - 2012.

3GPP Technical Specification // TS 22.001. - 2011-03.

3GPP Technical Spezifikation // TS 23.041 Technical realization of Cell Broadcast Service- Release9. - 2010.

3GPP Technische Spezifikation TS 25.401 // UTRAN overall description.

3GPP TS 04.31 // Technical Specification Group GSM/EDGE Radio Access Network: Location Services (LCS); Serving Mobile Location Centre (SMLC), Radio Resource LCS Protocol (RRLP)". - 2007-06.

3GPP TS 22.090 // 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects; Unstructured Supplementary Service Data (USSD); Stage 1 (Release 10). - 2011-03.

3GPP TS 22.140 // 3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; Multimedia Messaging Service (MMS); Stage1; (Release 10). - 2011-03.

Agency National Security Mobility Capability Pkg (Version 1.1U). - [s.l.] : NSA, 02-2012.

Alex Biryukov Adi Shamir und David Wagner Real time cryptanalysis of A5/1 on a PC und Advances in Cryptology, proceedings of Fast Software Encryption [Book] / ed. Software FSE '00 Proceedings of the 7th International Workshop on Fast. - [s.l.] : Springer-Verlag, 2000. - pp. 1-18.

Andrew M. White Austin R. Matthews, Kevin Z. Snow, Fabian Monrose Phonotactic Reconstruction of Encrypted VoIP Conversations: // Hookt on fon-iks. - Universtity of North Carolina at Chapel Hill : SP '11 Proceedings of the 2011 IEEE Symposium on Security and Privacy, 2011.

Android Developer Guides [Online]. - 10 22, 2012. - http://www.developer.android.com/about/dashboards/index.html.

ATMEL 8-bit Microcontroller with 128kBytes In-System Programmable Flash // ATmega128, ATmega128L. - [s.l.] : ATMEL.

BBC-News // United Arab Emirates will not ban Blackberries. - 2010-10.

BlackBerry BlackBerry Java application development [Online] // Developers. - 11 04, 2012. - http://www.blackberry.com/developers/docs/7.1.0api/.

Cellcrypt Secure Mobile Voice [Online]. - 10 22, 2012. - http://www.cellcrypt.com/government/cellcrypt-mobile-baseline.

Collin Mulliner Charlie Miller // Injecting SMS Messages into Smart Phones for Security Analysis. - TU-Berlin : [s.n.], 2009.

Collin Mulliner Giovanni Vigna, David Dagon, and Wenke Lee // Using Labeling to Prevent Cross-Service Attacks Against Smart Phones. - Heidelberg : Springer-Verlag Berlin, 2006. - Vols. pp. 91–108.

Cross Tom Exploiting Lawful Interception to Wiretap the Internet // X-Force Research. - Blackhat DC : IBM Corporation, 2010.

Denis Foo Kune John Koelndorfer, Nicholas Hopper, Yongdae Kim // Location Leaks on the GSM Air Interface. - University of Minnesota : [s.n.], 2012-02.

Developer Android (telephony) [Online]. - 10 11, 2012. - http://developer.android.com/reference/android/telephony/.

Dietrich Dipl.-Ing. Peter Teufel und Dipl.-Ing. Kurt Zentrum für sichere Informationstechnologie AU // Sicherheitsanalyse BlackBerry OS5. - 2010.

Dr. Stephan Rupp Franz-Josef Banet Schritt für Schritt // Die Entwicklung von GSM zu UMTS. - Stuttgart : Alcatel, 2001.

Eikenberg Roland Britische Vodafone Kunden mit Femto-Zelle abhörbar [Article] // C't. - 2011. - 14.07..

ELAMAN GmbH Newsletter Q1 // Governmental Security Solutions. - 2011-01.

ELAMAN GmbH Produktkatalog // Governmental Security Solutions. - 2011.

Engel Tobias // Locating Mobile Phones using SS7. - 25th CCC Berlin : [s.n.], 2008.

Engeneers Institute of Electrical and Electronic IEEE 802.11-2007 [Pdf] // Local and Metropolitan Area Networks - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications / ed. IEEE. - 2007. - ISBN: 9780738156552.

ETSI TS 102 312 // Near Field Communication Interface and Protocol-2 (NFCIP-2). - 2004-02 : [s.n.].

ETSI 300 625 // Digital cellular telecommunications system (Phase 2); Unstructured Supplementary Service Data (USSD) – Stage 1 (GSM 02.90 version 4.1.1). - 10-1997.

ETSI ES 201 671 // Telecommunications security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic. - 1997-07.

ETSI ETS 300 977 10.3.18 // GSM 11.11. - 1998.

ETSI GSM 04.11 . - 1996.

ETSI Technical Report // Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN);. - 2006-02.

ETSI Technical Standard // GSM 03.40. - 1996.

ETSI Technical Standard // TS 24.011 V11. - 2002-03.

ETSI Technical Standard // Mobile Equipment (SIM-ME) Interface Release 1999. - 1999.

ETSI TR 180 005 // Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN);. - 2010-10.

ETSI TS 100 906 GSM 02.07 // Digital cellular telecommunications system (Phase 2+); Mobile Stations (MS) features (GSM 02.07, version 6.2.0, Release 1997). - 2000-04.

ETSI TS 100 977 // Specification oft he Subscriber Identity Module – Mobile Equipment (SIM-ME) Interface. - 2007-06.

ETSI TS 101 671 // Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffiv. - 2010-08.

ETSI TS 101 671 // Lawful Interception (LI) Hadover interface for the lawful interception of telecommunications traffic. - 2011-11.

ETSI TS 102 190 // Near Field Communication (NFC) IP-1; Interface and Protocol (NFCIP-1). - 2003-03.

ETSI TS 102 671 // Smart Cards: Machine to Machine UICC; Physical and logical characteristics (Release 9). - 2010-04.

ETSI TS 122 030 // Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Man-Machine Interface (MMI) of the User Equipment (UE); . - 2011-05.

ETSI TS 133 106 // Universal Mobile Telecommunications System (UMTS); LTE; Lawful interception requirements. - 05-2011.

ETSI TS 143 033 // Digital cellular telecommunications system (Phase 2+); Lawful Interception; Stage 2 . - 2004-12.

ETSI TS GSM 03.03 // Digital cellulat telecommunications system (Phase 2+); Numbering, addressing, and identification. - 1996.

G. Camarillo E. Schulzrinne Early Media and Ringtone Generation in the Session Initiation Protocol (SIP). - 2004.

Ghanem [et al.] Legal Intercept [Patent] : 20110153809 : U.S. Class 709/224; 709/228 / ed. Office US Patent & Trademark. - USA, 12 29, 2009.

Globalplatform Globalplatform [Online] // Spezifikationen für die Industrie . - 2012. - 09 19, 2012. - http://www.globalplatform.org.

Goolge Seek-for Android [Online]. - 10 10, 2012. - http://code.google.com/p/seek-for-android.

Grugq Attacking GSM Base Station Systems and Mobile Phone Base Bands // Base Jumping:. - Black Hat Abu Dhabi : [s.n.], 2011.

Guardian The UAE BlackBerry ban set to spread throughout Gulf states. - 2010-09.

He Guoyou Overview of UMTS // Tech-Paper. - Helsinki University of Technology : [s.n.], 2003.

Hewett By Lee Dryburgh und Jeff Signaling System No. 7 (SS7/C7): Protocol, Architecture, and Services [Book]. - [s.l.] : Cisco Press, 2004. - ISBN-10: 1-58705-040-4.

Heyde Klaus v. d. Sicherheit im Mobilkommunikationsnetz der 3. Generation (UMTS) [Book]. - 2002. - p. 8.

Informationstechni BSI Bundesamt für Sicherheit in der ReCoBS Grudlagen und Anforderungen. - 06-2012.

Informationstechnik BSI Bundesamt für Sicherheit in der SNS Sichere Netzübergreifende Sprachkommunikation. - 2012.

Informationstechnik Bundesamt für Sicherheit in der BSI // Gefährdungskatalog. - 2005. - Vols. Abschnitt G5 Vorsätzliche Handlungen, G5.96 Manipulation von Mobilfunktelefonen.

Informationstechnik Bundesamt für Sicherheit in der IT-Grundschutz-Katalog // 12. Ergänzungslieferung - September 2011. - 2011.

itWatch GmbH ReCAppS. - 06-2006.

Jens Heider Rachid EL Khayari Geht Ihr Smartphone fremf? [Article] // DuD Datenschutz und Datensicherheit . - 2012-03. - Seite 155-160.

Karsten Nohl Attacking Phone Privacy // BlackHat USA. - 2010.

Karsten Nohl Chris Paget GSM-SRSLY? // Präsentationsfolien 26C3. - 26th CCC Berlin : [s.n.], 2009.

Karsten Nohl Luca Melette GRPS Intercept // SRLabs Camp. - Chaos Computer Camp : [s.n.], 2011.

Karsten Nohl Sylvain Munaut GSM Sniffing // Präsentationsfolien 27C3. - 27th CCC Berlin : [s.n.], 2010.

Kit GNU Radio Development GNU General Public License (GPL) version 3 [Online]. - 11 10, 2012. - http://www.gnuradio.org.

Klein Mark Declaration of Mark Klein. - 2006.

Kostrewa Adam Development of a man in the middle attack on the GSM Um-Interface // Master Thesis. - Technische Universität Berlin : [s.n.], 2011.

Kubovy Harald BlackBerry Unlocker [Online] // MFI Multiloade . - 11 04, 2012. - http://www.gsmfreeboard.com .

McCullagh Declan FBI Taps Cell Phone Mic as Eavesdropping Tool [Journal]. - [s.l.] : ZDNET , 2006-12.

Menn Joseph Reuters [Online] // Key Internet operator VeriSign hit by hackers. - 02 02, 2012. - 11 24, 2012. - http://www.reuters.com/article/2012/02/02/us-hacking-verisign-idUSTRE8110Z820120202.

Metz Rachel An Apple Vorbei [Article] // C't. - [s.l.] : Heise, 11-2012.

Microsoft Entwicklungsumgebung für WP8 [Online]. - 2011. - 11 20, 2012. - http://www.microsoft.com/visualstudio/deu/products/visual-studio-express-for-windows-phone.

Microsoft Visual Studio Express [Online] // Entwicklungsumgebung für WP7. - 2012. - 11 23, 2012. - http://microsoft/germany/express.

Microsoft Webcast Windows Phone 7 Grundlagen [Online]. - 11 23, 2012. - http://www.microsoft.com/germany/msdn Stand .

OMA Open Mobile Aliance OMA/WAP Forum [Online]. - 09 19, 2012. - http://www.WAPforum.org.

OMA Open Mobile Aliance Standart TS STI V1.0 // OMA Transcoding Interface. - 2007 : [s.n.].

Oreskovic Alexei Reuters [Online] // Google to Iran: Change your password. - 11 09, 2011 . - 11 24, 2012. - http://www.reuters.com/article/2011/09/09/us-google-security-idUSTRE7885U320110909.

Orr Dunkelman Nathan Keller und Adi Shamir A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony // Cryptology ePrint Archive. - 2010.

Project Osmocom - Open Source Mobile Communication [Online] // Open Source Software projects in the area of mobile communications. - 09 17, 2012. - http://openbsc.osmocom.org/trac/wiki/OsmocomOverview.

Radmilo Racic Denys Ma, Hao Chen Exploiting MMS Vulnerabilities to Stealthily Exhaust Mobile Phone's Battery. - 2006.

Rednaxela Rednaxela [Online] // Converter für das PDU Format. - 09 19, 2012. - http://rednaxela.net/pdu.php.

Reserch in Motion Developer BlackBerry [Online]. - 11 04, 2012. - http://www.developer.blackberry.com/develop/ .

Ries Uli IMSI-Catcher für 1500 Euro im Eigenbau [Article] // C't. - 2010. - 01.08..

Rohde & Schwarz GmbH & Co TSMX-PPS, TSMQ, TSMU, TSML und die Software ROME S4 // Produktkatalog. - 2007.

security VUPEN Threat Protection Program // Zero-Day Exploits for Law Enforcement Agencies. - 2011.

Seek for Android [Online]. - 10 11, 2012. - http://code.google.com/p/seek-for-android.

SIPGate sipgate One [Online]. - 11 01, 2012. - http://www.sipgate.de/one.

Skyhook [Online] // location positioning. - 09 19, 2012. - http://www.skyhookwireless.com/.

Solomo besser mobil [Online]. - 11 1, 2012. - http://www.solomo.de.

Source Android "Tech Info" [Online]. - 10 22, 2012. - http://www.source.android.com/tech/security/index.html.

Spectrum IEEE Athens Affair [Journal]. - [s.l.] : IEEE Spectrum Article , July 2007.

Strobel Daehyun IMSI Catcher // Seminararbeit der Ruhr-Universität Bochum 2007. - 2007.

Sven Bugiely Lucas Daviy, Alexandra Dmitrienkoz, Stephan Heuserz // Practical and Lightweight Domain Isolation on Android. - TU Darmstadt, Fraunhofer SIT : [s.n.].

Teufl Dipl.-Ing. Peter Sicherheitsanalyse BlackBerry OS5. - Wien : Zentrum für sichere Informationtechnologie - Austria, 04-2010.

Tsukasa Oi Fourteenforty Windows Phone 7 Internals and Exploitability. - [s.l.] : Research Institute Inc. (FFRI), 2011.

Ulrike Meyer (University of Technology Darmstadt), Susanne Wetzel (Stevens Institute of Technology, USA) // A Man-in-the-Middle Attack on UMTS. - 2004.

Ulrike Meyer Susanne Wetzel ON THE IMPACT OF GSM ENCRYPTION AND MITM ATTACKS ON THE SECURITY OF INTEROPERATING GSM/UMTS Networks. - 2004.

Union) ITU (International Telecommunication Specifications of Signalling System No.7 // Q.700 bis Q.795. - 1993.

Union) ITU (International Telecommunication Telecommunication Standardization Sector // ITU-T E.800. - 2008.

VUPEN Security Vunerability Research & Solution [Online]. - 09 19, 2012. - http://www.vupen.com.

Weidman Georgia Transparent Botnet Control for Smartphones over SMS. - Shmoocon : [s.n.], 2011.

Weinmann Ralf-Philipp // Baseband Atacks: Remote Exploitation of Memory Corruptions in Cellular Protocol Stacks. - University of Luxembourg : [s.n.], 2012.

Weinmann Ralf-Philipp // All Your Baseband Are Belong To Us. - Universty of Luxembourg : [s.n.], 2010.

whatever mobile GmbH Whatevermobile [Online] // Lösungen zur mobilen Kommunikation von höchster Qualität.. - 09 19, 2012. - http://www.whatevermobile.com/de/.

WhisperSys Whispersystems (Beta) [Online] // mobile security for android. - 11 19, 2012. - http://www.whispersys.com/.

Wikileaks Spy-Files - Dokumente [Online]. - 09 19, 2012. - http://wikileaks.org/the-spyfiles.html.

Wikileaks Spy-Files - Kartenansicht [Online]. - 09 19, 2012. - http://spyfiles.org/.

Xinyuan Farley Ryan und Wang // Roving bugnet: Distributed surveillance threat and mitigation. - George Mason University, USA : Department of Computer Science, 2009.

Eidesstattliche Erklärung

Marcus Prem, 871713

Hiermit erkläre ich, dass ich diese Arbeit selbständig abgefasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

Die Arbeit wurde bisher keiner anderen Prüfungsbehörde vorgelegt und auch noch nicht veröffentlicht.

Ort, Abgabedatum Unterschrift (Vor- und Zuname)