Hannes Federrath

# Sicherheit mobiler Kommunikation

Schutz in GSM-Netzen,
Mobilitätsmanagement,
Mehrseitige Sicherheit

# Inhaltsverzeichnis

Vorwort ..... v
Inhaltsverzeichnis ..... xi
Tabellenverzeichnis ..... xvii
Abbildungsverzeichnis ..... xviii

Teil 1 Analyse existierender Mobilfunknetze 1

1 Mobilkommunikation und mehrseitige Sicherheit ..... 1
1.1 Mobilkommunikation ..... 1
1.1.1 Terminal- und Personal Mobility ..... 3
1.1.2 Herausforderungen ..... 3
1.1.3 Beispiele für mobile Netze ..... 4
1.2 Mehrseitige Sicherheit ..... 16
1.2.1 Technische Datenschutzforderungen ..... 18
1.2.2 Anforderungen mehrseitiger Sicherheit ..... 20
1.2.3 Sicherheitsanforderungen in der Literatur ..... 22
1.3 Angreifermodell unter dem Aspekt der Vertraulichkeit der Lokalisierungsinformation ..... 26
1.3.1 Allgemeines zu Angreifermodellen ..... 26
1.3.2 Passiver und aktiver Angreifer ..... 27
1.3.3 Mächtigkeit des Angreifers ..... 28
1.3.3.1 Ausforschungssicherheit der Endgeräte ..... 28
1.3.3.2 Manipulationssicherheit ..... 29
1.3.3.3 Peilbarkeit sendender Funkstationen ..... 29
1.4 Abgeleitete Sicherheitsmaßnahmen ..... 31

2 Mobilkommunikation am Beispiel GSM ..... 35
2.1 Allgemeines ..... 35
2.1.1 Standardisierung von GSM ..... 35

2.1.2 Leistungsmerkmale von GSM ... 36
2.1.3 GSM in Zahlen ... 36
2.2 Struktur von GSM ... 37
2.2.1 Architektur ... 37
2.2.2 Funktechnischer Aufbau ... 39
2.2.3 Mobilfunkgebiete im GSM ... 42
2.2.4 Subscriber Identity Module ... 42
2.3 Datenbanken des GSM ... 43
2.3.1 Home Location Register ... 43
2.3.2 Visitor Location Register ... 44
2.3.3 Equipment Identity Register ... 45
2.3.4 Authentication Centre ... 45
2.4 Sicherheitsrelevante Prozeduren und Funktionen ... 46
2.4.1 Zugangskontrolle ... 46
2.4.2 Authentikation ... 47
2.4.3 Pseudonymisierung durch TMSI ... 49
2.4.4 Generierung des Chiffrierschlüssels Kc ... 53
2.4.5 Verschlüsselung auf der Funkschnittstelle ... 54
2.4.6 Ein Beispiel ... 56

3 Mobilitäts- und Verbindungsmanagement ... 59

3.1 Wozu Location Management? ... 59
3.2 Location Management allgemein ... 61
3.3 Erstellbarkeit von Bewegungsprofilen ... 63
3.4 Location Update Prozeduren ... 64
3.4.1 Einbuchen ... 66
3.4.2 Aufenthaltsaktualisierung ... 66
3.4.2.1 Neues LA, aber altes VLR ... 67
3.4.2.2 Neues VLR ... 68
3.4.3 Periodische Aufenthaltsaktualisierung ... 69
3.5 Rufaufbau (Call Setup) im GSM ... 69
3.5.1 Vermittlung ankommender Rufe ... 70
3.5.2 Vermittlung abgehender Rufe ... 73
3.6 Erstellbarkeit von Bewegungsprofilen im GSM ... 74
3.6.1 Ebene OMC ... 75
3.6.2 Ebene HLR ... 75
3.6.3 Ebene VLR/MSC ... 75

3.6.4 Ebene BSS ... 76
3.6.5 Funktechnische Ebene (BTS) ... 76
3.6.6 Entgeltabrechnung und Bewegungsprofile ... 77
3.6.7 Registrierung der Gerätekennungen (EIR) ... 79
3.7 Bekannte Angriffe auf GSM-Sicherheitsfunktionen ... 80
3.7.1 IMSI-Catcher ... 80
3.7.2 Cloning der SIM-Karte ... 81
3.7.3 Abfangen von Authentication Tripeln ... 82
3.8 Zusammenfassung der Sicherheitsprobleme ... 83

Teil 2 Datenschutzgerechtes Location Management 85

4 Systematik der vorgestellten Verfahren ... 85
4.1 Zusammenhang der Methoden ... 86
4.2 Zusätzliche notwendige Maßnahmen zum Schutz des Aufenthaltsorts ... 89

5 Methoden mit ausschließlichem Vertrauen in die Mobilstation ... 91
5.1 Vermeidung von Lokalisierungsinformation: Broadcast-Signalisierung (A.1) — ein extremer Ansatz ... 91
5.1.1 Implizite Adressierung bei Broadcast ... 92
5.1.2 Technische Rahmenbedingungen ... 98
5.1.3 Konsistenz der Verteilung ... 99
5.1.4 Aufwand ... 101
5.1.5 Auswertung ... 104
5.1.6 Variable implizite Adressierung ... 104
5.2 Methode der Gruppenpseudonyme (A.2) ... 107
5.2.1 Vorbemerkungen ... 108
5.2.2 Einbuchen, Ausbuchen und Aufenthaltsaktualisierung ... 109
5.2.3 Vermittlung eines ankommenden Rufs ... 110
5.2.4 Bewertung der Methode der Gruppenpseudonyme ... 112
5.2.4.1 Bildung der Anonymitätsgruppe ... 112

5.2.4.2 Implizite Adresse auf der Funkschnittstelle ..... 114

6 Methoden mit zusätzlichem Vertrauen in einen eigenen ortsfesten Bereich ..... 117

6.1 Adreßumsetzungsmethode mit Verkleinerung der Broadcast-Gebiete (B.1 und B.2) ..... 117
6.2 Explizite Speicherung der Lokalisierungsinformation in einer Trusted Fixed Station (B.3) ..... 122
6.3 Pseudonymumsetzung in einer vertrauenswürdigen Umgebung mit der Methode der temporären Pseudonyme (B.4) ..... 124
6.3.1 Vorbemerkungen ..... 124
6.3.2 Einbuchen, Ausbuchen und Aktualisieren ..... 125
6.3.3 Vermittlung eines ankommenden Rufs ..... 127
6.4 Sicherheitsbetrachtungen ..... 129
6.4.1 Unberechtigte Abfrage der Trusted Fixed Station ..... 129
6.4.2 Verwendung von Pseudonymen ..... 130
6.4.3 Beobachtbarkeit der Kommunikationsbeziehungen ..... 131

7 Methoden mit zusätzlichem Vertrauen in einen fremden ortsfesten Bereich ..... 133

7.1 Organisatorisches Vertrauen: Vertrauen in eine Trusted Third Party (C.1) ..... 133
7.1.1 Allgemeines ..... 133
7.1.2 Die Methode der verteilten temporären Pseudonyme (DTP-Methode) ..... 134
7.2 Vertrauen in physische Sicherheit: Methode der kooperierenden Chips (C.2) ..... 135
7.2.1 Einbuchen, Aktualisieren, Ausbuchen ..... 137
7.2.2 Vermittlung eines ankommenden Rufs ..... 138
7.2.3 Sicherheitsbetrachtungen ..... 140
7.2.4 Modifikationsmöglichkeiten ..... 142
7.3 Aufwandsbetrachtungen zu den Methoden B.3, B.4, C.2 ..... 144

7.3.1 Skalierbarkeit bzgl. der Teilnehmerzahl bei der Methode der kooperierenden Chips ..... 144
7.3.2 Nachrichtenlängen für die Signalisierung auf der Funkschnittstelle ..... 148
7.4 Mobilkommunikationsmixe: Anonyme Rückadressen zur „Pfadgewinnung“ (C.3) ..... 153
7.4.1 Voraussetzungen, vereinfachende Annahmen und Notationen ..... 154
7.4.2 Schutz der Verkehrsdaten im ISDN: Das Verfahren der ISDN-Mixe ..... 155
7.4.3 Grundverfahren mit HLR, aber ohne VLR ..... 158
7.4.3.1 Aufenthaltsregistrierung und -aktualisierung ..... 159
7.4.3.2 Signalisierung eines ankommenden Rufs ..... 161
7.4.3.3 Signalisierung eines abgehenden Rufs ..... 162
7.4.4 Modifikationsmöglichkeiten ..... 163
7.4.4.1 Trusted Base Transceiver Station ..... 163
7.4.4.2 Generierung von {LAI}-Sets ..... 164
7.4.4.3 Verwendung von Mix-Kanälen ..... 165
7.4.4.4 Trusted Fixed Station ..... 165
7.4.5 Verfahren mit HLR und VLR ..... 166
7.4.5.1 Grundidee des pseudonymen Location Managements ..... 166
7.4.5.2 Pseudonymes Location Management mit Mixen ..... 168
7.4.5.3 Aufenthaltsregistrierung und -aktualisierung ..... 171
7.4.5.4 Geographische Allokation der Mixe und Bildung von Aufenthaltsgebiets-gruppen ..... 174
7.4.5.5 Signalisierung eines ankommenden Rufs ..... 178
7.4.5.6 Signalisierung eines abgehenden Rufs ..... 182
7.4.5.7 Gegenseitige Authentikation zwischen mobilen Teilnehmern und Netz ..... 184
7.4.6 Aufwandsbetrachtungen ..... 188

7.4.6.1 Nachrichtenlängen auf der Funkschnittstelle ..... 188
7.4.6.2 Kanalkapazität des Paging Channel ..... 196
7.4.6.3 Minimale Dauer eines Systemtaktes bei Call Setup ..... 198
7.4.6.4 Minimale Dauer eines Systemtaktes bei Location Update ..... 200
7.4.6.5 Verbindungsaufbauzeit ..... 204
7.4.7 Konzeptionelle Einbindung der Mobilkommunikationsmixe in UMTS ..... 206
7.4.7.1 Verallgemeinerung auf mehrstufige Speicherung ..... 207
7.4.7.2 Nachrichtenaufbau im allgemeinen Fall ..... 208
7.4.8 Sicherheitsbetrachtungen ..... 214
7.4.8.1 Anonymität und Unbeobachtbarkeit durch Mixe ..... 214
7.4.8.2 Bedeutung der Komponenten aus Sicherheitssicht ..... 215
7.4.8.3 Schubgrößen und Dummy Traffic ..... 216
7.4.8.4 Schutz über Netzgrenzen hinweg ..... 218
7.4.8.5 Zusammenfassung ..... 220

8 Schlußbemerkungen ..... 223

Anhang 227

I Exkurs: Das Mix-Netz ..... 227
II Vergleichende Übersicht der vorgestellten Verfahren ..... 235
III Literaturverzeichnis ..... 241
IV Abkürzungs- und Symbolverzeichnis ..... 253
V Index ..... 259

# Tabellenverzeichnis

Tab.1-1: Die technischen Datenschutzforderungen nach [Pfit_93] ..... 19
Tab.1-2: Aspekte eines Angreifermodells ..... 27
Tab.2-1: Die logischen Kanäle des GSM (nach [FuBr_94]) ..... 41
Tab.2-2: Allokation sicherheitsrelevanter Parameter im GSM ..... 56
Tab.3-1: Sicherheitsprobleme im GSM ..... 84
Tab.4-1: Übersicht der Methoden ..... 87
Tab.7-1: Zustände eines kooperierenden Chips ..... 140
Tab.7-2: Parameter zur Bewertung der kooperierenden Chips ..... 145
Tab.7-3: Nötige Bitrate auf dem Broadcast-Bus ..... 147
Tab.7-4: Mobile Terminated Call Setup: Nachrichtenlängen ..... 149
Tab.7-5: Location Update: Nachrichtenlängen ..... 150
Tab.7-6: Parameterlängen bei den Mobilkommunikationsmixen ..... 190
Tab.7-7: Mobile Terminated Call Setup: Nachrichtenlängen ..... 192
Tab.7-8: Location Update: Nachrichtenlängen ..... 194
Tab.7-9: Vergleich der Nachrichtenlängen für MTC und LUP ..... 196
Tab.7-10: Verfügbare Anzahl an TCHs bei LUP ..... 204
Tab.7-11: Verbindungsaufbauzeit für MTC ..... 205
Tab.7-12: Bedeutung der einzelnen Komponenten ..... 216
Tab.II-1: Systematik der Verfahren nach nötigem Vertrauen ..... 235
Tab.II-2: Systematik nach Signalisieraufwand und Peilbarkeit ..... 236
Tab.II-3: Dynamisierbarkeit der Sicherheitsbereiche ..... 237
Tab.II-4: Systematik nach Unbeobachtbarkeit ..... 238

# Abbildungsverzeichnis

Abb.1-1: Prinzipschaltbild eines GPS-Empfängers für C/A-Code.....11
Abb.1-2: Architekturkonzept von UMTS (vgl. [Mitt_94]).....16
Abb.2-1: Architekturschema des GSM (vgl. [Keda_91]).....38
Abb.2-2: Aufteilung der Bandbreite in Radiokanäle.....39
Abb.2-3: Authentikationsprozedur.....48
Abb.2-4: Neuvergabe einer TMSI bei bekannter alter TMSI.....50
Abb.2-5: Neuvergabe einer TMSI bei unbekannter alter TMSI.....51
Abb.2-6: Generierung von Kc.....53
Abb.2-7: Verschlüsselung auf der Funkschnittstelle.....54
Abb.2-8: Sprachkodierung, Verschlüsselung und Kanalkodierung.....55
Abb.2-9: Zusammenspiel der Sicherheitsfunktionen.....57
Abb.3-1: Verbindungsaufbau bei zentraler Speicherung.....61
Abb.3-2: Verbindungsaufbau bei zweistufiger Speicherung.....62
Abb.3-3: Verallgemeinerte mehrstufige Speicherung.....63
Abb.3-4: Grafische Darstellung verschiedener LUP-Situationen.....65
Abb.3-5: LUP: Neues LA, aber altes VLR (TMSI bekannt).....67
Abb.3-6: LUP: Neues VLR (altes VLR erreichbar).....68
Abb.3-7: Protokoll des Mobile Terminated Call Setup im GSM.....71
Abb.3-8: Datenbankabfragen bei einem MTC im GSM.....72
Abb.3-9: Protokoll des Mobile Originated Call Setup im GSM.....73
Abb.3-10: Bewegungsprofile auf den administrativen Ebenen.....74
Abb.5-1: Offene implizite Adressierung.....93
Abb.5-2: Verdeckte implizite Adressierung.....96
Abb.5-3: Verteilung über einen geostationären Satelliten.....98
Abb.5-4: Konsistenz der Verteilung von Signalisiernachrichten.....100
Abb.5-5: Mittlere Systemzeit bei Broadcast.....103
Abb.5-6: Notwendige Bitrate bei Broadcast.....103
Abb.5-7: Paging-Prozedur mit Zellseparation.....105
Abb.5-8: Beispiel einer Zellseparation.....106
Abb.5-9: Zellseparation mit Verkleinerung der Segmente.....107
Abb.5-10: MTC bei den Gruppenpseudonymen.....111

Abb.6-1: Funk-Mixe (in Anlehnung an [Pfit_93]) ..... 119
Abb.6-2: MTC beim Verfahren der Funk-Mixe ..... 121
Abb.6-3: MTC bei expliziter Speicherung ..... 122
Abb.6-4: MTC bei der TP-Methode ..... 128
Abb.6-5: MTC bei der vereinfachten TP-Methode ..... 129
Abb.7-1: Kooperierende Chips (Architektur) ..... 136
Abb.7-2: MTC bei den kooperierenden Chips ..... 139
Abb.7-3: Mittlere LUP-Rate in Stoßzeiten (nach [FuBr_94]) ..... 145
Abb.7-4: Ersetzen der Registerfunktionen durch C-NW ..... 146
Abb.7-5: Nötige Bitrate auf dem Broadcast-Bus ..... 148
Abb.7-6: Vergleich der Nachrichtenlängen für MTC und LUP ..... 152
Abb.7-7: MTC bei zentraler Speicherung ohne Schutz ..... 158
Abb.7-8: Aufenthaltsregistrierung ..... 160
Abb.7-9: MTC bei zentraler und verdeckter Speicherung ..... 161
Abb.7-10: MOC mit Schutz des Senders (Mobilstation) ..... 162
Abb.7-11: MTC bei gestufter und pseudonymer Speicherung ..... 167
Abb.7-12: Location Registration und Update ..... 173
Abb.7-13: LUP bei den Mobilkommunikationsmixen: Neues VLR ..... 174
Abb.7-14: Bildung der Anonymitätsgruppen bei den ISDN-Mixen ..... 176
Abb.7-15: Geographische Allokation der Mixe ..... 177
Abb.7-16: MTC Mobilkommunikationsmixe (konkretisiert) ..... 179
Abb.7-17: MTC Mobilkommunikationsmixe (Protokoll) ..... 181
Abb.7-18: MOC Mobilkommunikationsmixe ..... 182
Abb.7-19: MOC Mobilkommunikationsmixe (Protokoll) ..... 183
Abb.7-20: Gegenseitige Authentikation ..... 186
Abb.7-21: MTC, MOC und LUP auf einen Blick ..... 191
Abb.7-22: Anzahl simultan verfügbarer Verkehrskanäle ..... 203
Abb.7-23: Verbindungsaufbauzeiten ..... 206
Abb.7-24: Architekturkonzept der Mobilkommunikationsmixe ..... 207
Abb.7-25: Erweitertes Architekturkonzept von UMTS ..... 208
Abb.7-26: Allgemeine Darstellung der Verkettung beim MTC ..... 209
Abb.7-27: Senderanonymitätsschema beim LUP ..... 211
Abb.7-28: Senderanonymitätsschema beim MOC ..... 213
Abb.8-1: Schalten von anonymen Kanälen ..... 225
Abb.I-1: Umkodieren gemixter Nachrichten [Pfit_93] ..... 228
Abb.I-2: Systematik der Mixe ..... 231
Abb.II-1: Vergleich der Verfahren ..... 239