Magdeburger Journal zur Sicherheitsforschung

Gegründet 2011 | ISSN: 2192-4260
Herausgegeben von Stefan Schumacher und Jan W. Meine
Meine Verlag – Wissenschafts-, Sach- und Fachbuchverlag, Magdeburg

Angriffe und Verteidigungsstrategien für vertrauliche Kommunikation über Funkdienste

Michael »MiKa« Kafka **René »Lynx« Pfeiffer**

Dieses Dokument dient als Zusammenfassung mit Angabe weiterer Quellen zum Vortrag »Angriffe und Verteidigungsstrategien für vertrauliche Kommunikation über Funkdienste«, gehalten am 9. IKT Sicherheitsseminar des österreichischen Abwehramtes. Es enthält eine Aufbereitung verschiedener Vorträge der letzten DeepSec-Konferenzen sowie Ergänzungen aus zwischenzeitlich publizierten Forschungsergebnissen.

Zitationsvorschlag: Kafka, M. und Pfeiffer, R. (2012). Angriffe und Verteidigungsstrategien für vertrauliche Kommunikation über Funkdienste. *Magdeburger Journal zur Sicherheitsforschung*, 2, 308–322. Zugriff am 16. Juli 2012, unter http://www.sicherheitsforschung-magdeburg.de/journal_archiv.html

Zusammenfassung

Das zurzeit weltweit verwendete Mobilfunknetz hat große Sicherheitsprobleme und wird für die Übertragung sensibler Informationen nicht mehr ohne zusätzliche Absicherung empfohlen. Gespräche und Daten sowie Textnachrichten lassen sich von Dritten mitschneiden, dekodieren und abhören. Der Aufwand hierfür liegt mittlerweile im leicht finanzierbaren Bereich, wodurch das Bedrohungspotential weiter steigt.

Die Sicherheit der 2G/3G Netzwerke erscheint in historischem Kontext besonders bedrohlich. Ursprünglich wurde die 2G Technologie von staatlichen Kommunikationsfirmen entwickelt, die zwischen Europa/USA und dem Rest der Welt unterschieden haben. Mittlerweile sind die meisten Mobilfunkanbieter private Unternehmen (entweder als solche gegründet oder privatisiert, wobei in einigen Ländern noch staatliche Monopole auf Kommunikationsnetzwerke bestehen), und die Verbreitung der 2G/3G Technologie setzt Vertrauen zwischen nahezu beliebigen Staaten voraus.

Überblick

Die folgenden Ausführungen haben ihren Fokus auf Mobilfunknetzwerke der 2. Generation, abgekürzt 2G Technologie[1]. Einige Konzepte sind jedoch auch Teil von 3G Netzwerken, wobei die Abgrenzung zwischen den Technologien durch den Markt und den Konkurrenzdruck fließend ist. Um die wachsende Zahl der Mobilfunknutzer zu versorgen, wurden technologische Zwischenschritte eingeführt, um die Kapazitäten stetig zu erweitern (2.5G, 2.75G, 3.5G, 3.75G, 3.9G findet man als Abkürzungen in der Literatur, 4G Technologie ist ebenso schon im begrenzten Betrieb). Dieser Umstand erschwert die Einschätzung des Bedrohungspotentials. Darüber hinaus lassen die Spezifikationen den Mobilfunkbetreiber einen Spielraum bei der Konfiguration an ihrer Infrastruktur. Alle diese Punkte müssen bei einer Sicherheitsanalyse bedacht werden.

GSM-Kommunikation

Die GSM-Kommunikation umfasst mehrere Dienste wie Sprachübertragung, Kurznachrichten[2] sowie Datenübertragung. Das Mobilfunknetz, in dem sich die Teilnehmer befinden, stellt diese Dienste über eine Reihe von Technologien mit den damit verbunden Protokollen zur Verfügung.

- GSM
- Enhanced Data Rates for GSM Evolution (EDGE)
- Universal Mobile Telecommunications System (UMTS)

Die Liste ist nicht komplett, da eine stetige Weiterentwicklung erfolgt, um die Datenraten und Anzahl der Gespräche sowie die Sprachqualität zu verbessern. Man spricht daher von Generationen und gibt diese mit Zahlen wie 2G, 3G, 3.5G, 3.75G, 3.9G, etc. an. Abbildung 1 zeigt die wichtigsten Komponenten eines 2G/3G Netzwerks und wie diese verbunden sind.

Die Luftschnittstelle benutzt Funkfrequenzen in den Bereichen 850/900, 1800/1900 und 2100 MHz.[3] Im 3rd Generation Partnership Project[4] sind 14 Frequenzbänder spezifiziert, die jedoch nicht in allen Ländern verwendet wer-

1 (in Folge auch GSM für Global System for Mobile Communications (GSM), ehemals Groupe Spécial Mobile.

2 Short Message Service, SMS

3 In einigen Ländern wurden auch die 400 und 450 MHz Frequenzen verwendet, weil diese noch den 1G Systemen zugeordnet waren.

4 http://en.wikipedia.org/wiki/3GPP

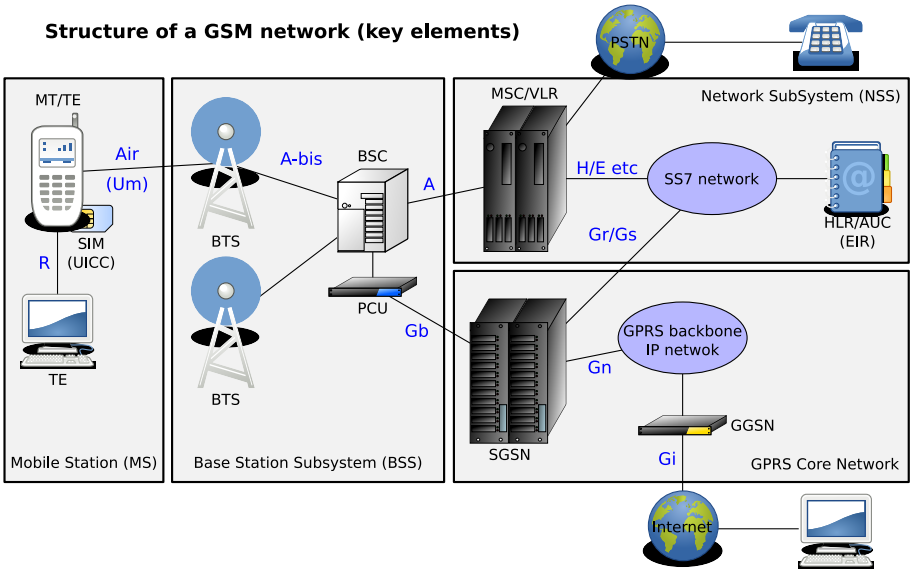


Abbildung 1: Die Mobilfunkinfrastruktur ist hier mit den Schlüsselkomponenten dargestellt. Auf der linken Seite sieht man die mobilen Endgeräte, die über die Luftschnittstelle mit den Basisstationen Kontakt haben. Base Station Controller (BSC) leiten die Verbindung weiter in die interne Infrastruktur, die primär aus SS7 besteht (die Verbindungen ab BTS/BSC können auch schon durch SS7 gehen). (Quelle http://en.wikipedia.org/wiki/GSM)

den. Mit UMTS kommen noch weitere Frequenzbänder hinzu. In Europa wird UMTS neben den bereits erwähnten Frequenzen auf 2100 MHz verwendet.

Verschlüsselung

Verschlüsselung wurde von Anfang an für die Datenübertragungen über die Luftschnittstelle vorgesehen, da bei Funkübertragungen immer passive Attacken durch Abhören möglich sind. Der Verschlüsselungsmodus wird von der Basisstation vorgegeben.

A5 Serie

Die in GSM verwendeten kryptografischen Algorithmen fasst man als A5-Serie zusammen:

- A5/0: Klartext (keine Verschlüsselung).
- A5/1: der gebräuchliche Verschlüsselungsmodus.
- A5/2: eine für den Export geschwächte Variante von A5/1.
- A5/3: ein neuer Algorithmus, der stärker als A5/1 sein soll.
- A5/4: derselbe Algorithmus wie A5/3, nur mit 128-Bit-Schlüsseln statt 64-Bit-Schlüsseln

Darüber hinaus gibt es noch die A3-Hashfunktion[5] und den A8 Schlüsselerzeugungsalgorithmus. A3 und A8 verwenden dieselben Eingabeparameter und werden daher oft als A3/A8 bezeichnet. A3 kann vom Betreiber des Mobilfunknetzwerks selbst gewählt werden.

A5/1 enthält einen Pseudozufallsgenerator aus drei Schieberegistern, der den Datenstrom mit einem Strom aus Zufallszahlen durch eine mathematische Exklusiv-Oder-Verknüpfung (XOR) verändert. Abbildung 2 zeigt den Aufbau des Pseudozufallsgenerators für den Schlüsselstrom. GSM ist impulsbasiert, jeder Sendeimpuls dauert 4,615 Millisekunden und enthält 114 Bit übertragene Information. Mittels A5/1 werden pro Impuls 114 Bit des generierten Schlüsselstroms für die Verschlüsselung der Daten verwendet. Der Schlüsselstrom wird mit einem 64-Bit Schlüssel und einer 22-Bit langen Rahmennummer initialisiert. Nach heutigem Stand der Technik ist die Schlüssellänge von 64 Bit gegenüber Attacken nicht mehr ausreichend. Die US-amerikanische Standardisierungsbehörde NIST[6] hat bereits im Jahre 2003 die Empfehlung ausgegeben, Schlüssel mit Längen von bis zu 80 Bit nach dem Jahre 2015 nicht mehr zu verwenden. Im Jahre 2005 wurde die Verwendung von Schlüsseln der Länge 80 Bit ab 2010 verboten.

A5/2 ist analog zu A5/1 aufgebaut, allerdings wurden absichtlich Schwächen eingebaut, um eine Exportvariante für Länder außerhalb Europas und den USA zu schaffen. A5/2 wurde bereits einige Wochen nach der Publikation im Jahre 1999 gebrochen und ist als unsicher einzustufen. Eine Beispiel-Implementation findet sich mit Quellcode in der Encyclopedia on Cryptography and Information Security[7]. Mitgeschnittene Transmissionen lassen sich nahezu in Echtzeit entschlüsseln. Dieser Umstand hat allerdings nicht dazu geführt, dass A5/2 aus der Infrastruktur entfernt wurde. Harald Welte, ein Sicherheitsforscher und Entwickler, hat die Entfernung von A5/2[8] recherchiert. Die Schwachstelle wurde

5 Eine Hashfunktion ist eine Funktion, die eine Zeichenfolge beliebiger Länge auf eine Zeichenfolge mit fester Länge abbildet. Solche Funktionen werden in der Mathematik oder Kryptografie verwendet.

6 National Institute of Standards and Technology (NIST)

7 http://cryptodox.com/A5/2

8 http://blog.deepsec.net/?p=173

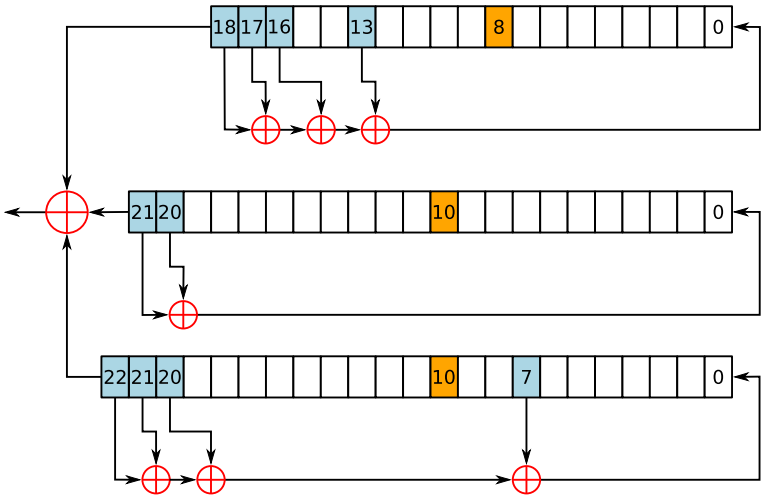


Abbildung 2: A5/1 beruht auf einer Kombination von drei linearen Schieberegistern mit Feedback, die einer unterschiedlichen Taktung unterworfen sind. Die orangen Felder sind die Taktbits, die bestimmen, ob ein Register werden zum Pseudozufallsstrom vermischt. (Quelle http://en.wikipedia.org/wiki/A5/1)

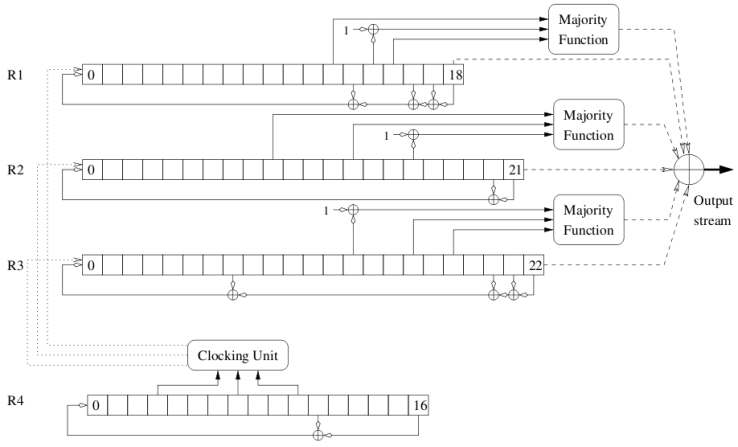


Abbildung 3: A5/2 basiert auf A5/1, enthält allerdings noch zusätzliche Komponenten, die die Sicherheit absichtlich herabsetzen. A5/2 war als Exportvariante für bestimmte Länder gedacht.

von 1999 bis 2007 ignoriert und erst danach wurden Anstrengungen unternommen, um A5/2 aus der Infrastruktur zu entfernen. A5/2 ist derzeit immer noch präsent und wird auch weiterhin verwendet.

A5/3 ist der Nachfolger von A5/1. Der Algorithmus ist auch als *KASUMI* bekannt und basiert auf dem *MISTY1* Algorithmus, der von der Firma Mitsubishi Electric Corporation entwickelt wurde. KASUMI[9] ist im Unterschied zu MISTY1 leichter in Hardware zu implementieren und schneller. Dies wurde durch eine Anpassung des Algorithmus ermöglicht, welche die Stärke der Verschlüsselung prinzipiell geschwächt hat (Dunkelman u. a. 2010). A5/3 wurde für die Verwendung bei UMTS und General Packet Radio Service (GPRS) entwickelt und wird theoretisch in moderneren Netzwerken für Datenübertragungen eingesetzt. Praktisch ist die Unterstützung von A5/3 in Endgeräten sowie mobilen Netzwerken kaum bis gar nicht vorhanden.

GEA-Algorithmen

Für GPRS-Netzwerke, die Teil einer 2G- oder 3G-Infrastruktur sind und Daten transportieren, wurde A5 gegen einen anderen Algorithmus, dem GPRS Encryption Algorithm (GEA), ausgetauscht. Es gibt analog zu A5 GEA/0 (keine Verschlüsselung), GEA/1, GEA/2, GEA/3 und GEA/4 (ähnlich wie A5/4 werden dort 128 Bit Schlüssel verwendet). GEA/0 wird von einigen Werkzeugen bzw. zu Diagnosezwecken benutzt. In den meisten Netzwerken ist GEA/2 und GEA/3 im Einsatz. GEA/4 wird noch nicht eingesetzt (Nohl und Melette 2011).

9 KASUMI ist ein Blockchiffre und kein Stromchiffre.

GSM-Authentisierung und Schlüsselgenerierung

GSM verwendet eine sehr einfache Authentisierung, die nur einseitig erfolgt. Das Mobilfunknetzwerk wird immer als vertrauenswürdig behandelt, nur die Endgeräte müssen sich dem Netz gegenüber authentisieren. Die für Authentisierung und spätere Verschlüsselung notwendigen Zufallszahlen stammen aus dem Mobilfunknetzwerk. Die Authentisierung selbst erfolgt über den A3-Algorithmus[10]. Eingabeparameter sind der geheime Teilnehmerschlüssel K_i (128 Bit) und eine Zufallszahl $RAND$ (128 Bit). Daraus wird eine sogenannte *signed response*[11] $SRES$ (32 Bit) abgeleitet, die in Folge als »Ausweis« im jeweiligen Netzwerk gilt.

A3 ist sowohl im Authentication Center (AuC) des Heimatnetzes (beim Stammmobilfunkbetreiber) als auch auf der SIM-Karte implementiert. Der Algorithmus ist nicht in GSM standardisiert und kann vom Netzbetreiber gewählt werden. COMP128 ist eine verbreitete Implementierung. Abbildung 4 zeigt schematisch wie K_i und $RAND$ zu $SRES$ kombiniert werden.

Die für Anrufe und Datentransmissionen verwendeten Sitzungsschlüssel werden mit Hilfe des A8 Algorithmus erzeugt, der ebenfalls in Abbildung 4 beschrieben wird. Der Sitzungsschlüssel K_s wird pro Anruf jeweils neu erzeugt und ist 64 Bit lang. A8 ist wie A3 eine Vorgabe, die im Rahmen der Spezifikation von jedem Mobilfunkbetreiber selbst implementiert werden kann.

10 http://de.wikipedia.org/wiki/A3_(Algorithmus)

11 übersetzt *unterschriebene Antwort*

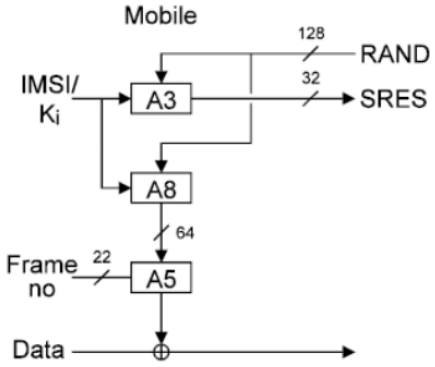


Abbildung 4: COMP128 berechnet aus dem geheimen Teilnehmerschlüssel K_i und einem vom Netzwerk gelieferten Zufallswert $RAND$ die *signed response* $SRES$, welche als Authentisierungstoken verwendet wird. Man sieht in der Abbildung auch den zweiten Schritt, der zur Schlüsselgenerierung für die spätere Verschlüsselung eingesetzt wird. Die Schlüsselgenerierung ist im Standard als A8 bezeichnet.

Angriffe auf die Verschlüsselung

Wie schon erwähnt, bietet A5/0 keine Verschlüsselung an. Da das Netzwerk den mobilen Endgeräten bedingungslos Befehle geben kann, ist es möglich A5/0 einzuschalten und damit verschlüsselte Kommunikation auf Klartext zu zwingen. Das Knacken einer Verschlüsselung erübrigt sich dann.

In bestimmten Ländern[12] wird dies per Default gemacht, um Zugriff auf die Kommunikation zu erlangen[13]. Die meisten Mobiltelefone zeigen nicht an, ob eine GSM-Verschlüsselung gerade aktiv oder inaktiv ist. Am Endgerät gibt es keinen Hinweis ohne Nachrüstung spezieller Software.

A5/2 kann man als gebrochen ansehen. Er wurde im selben Monat der Veröffentlichung im Jahre 1999 schon geknackt (Goldberg u. a. 1999). Der Aufwand für das Entschlüsseln ist sehr gering, da der Algorithmus explizit schwach entworfen wurde.

A5/1 wurde in der Vergangenheit mehrfach attackiert. Bereits 1997 haben sich Kryptografen damit beschäftigt (Golic 1997). Es gibt in Folge publizierte, ausführlichere Kryptanalysen aus den Jahren 2003 und 2006 von Barkan et al. Im Jahre 2007 gab es von den Universitäten Bochum und Kiel ein Projekt zum Angriff mit Hilfe von Field-Programmable Gate Array (FPGA) Chips, die sehr schnell Berechnungen durchführen können. 2008 startete The Hacker's Choice[14] ein Projekt zur Entschlüsselung von A5/1-verschlüsselten Daten mit Hilfe von vorberechneten Tabellen. Das Knacken von verschlüsseltem Text sollte damit binnen weniger Minuten möglich sein. Die Tabellen wurden allerdings nie publiziert. 2009 wurde

12 http://cryptome.org/gsm-spy.htm

13 Die Aussage stammt von David Burgess, der auf der DeepSec 2009 den GSM Security Workshop geleitet hat. Siehe Aufzeichnung der Pressekonferenz der DeepSec 2009 (kann auf Anfrage zur Verfügung gestellt werden).

14 http://freeworld.thc.org

das A5/1 Decryption-Projekt [15] auf der BlackHat- und der DeepSec-Konferenz vorgestellt. Der Ansatz verfolgt wiederum den Einsatz von vorberechneten Tabellen, den sogenannten *Rainbow Tables*, um das Knacken der Verschlüsselung zu beschleunigen. Mit diesen Projekten kann man A5/1 als unsicher einstufen, da handelsüblichen Computern genug Speicherplatz und Rechenleistung zur Verfügung steht, um die Verschlüsselung zu gefährden. Arbeitsgruppen von Sicherheitsforschern und Krypto-Enthusiasten haben bereits die für das Entschlüsseln notwendigen Rainbow Tables ausgerechnet und verfügbar gemacht[16].

A5/3 gilt nach derzeitigem Stand noch als sicher genug. Es wurden zwar schon Kryptoanalysen in den Jahren 2001, 2003, 2005 und 2010 publiziert, jedoch ist der Aufwand verglichen mit A5/1 noch höher. Dunkelman u. a. (2010) ist als Demonstration einer Time-Attacke gegen A5/3 gedacht und sollte zeigen, dass die Veränderungen von MISTY1 zu KASUMI die Sicherheit nicht nachhaltig erhöhen.

GSM-Authentisierung

Angriffe auf COMP128 wurden in Südmeyer (2006); Wray (2003) beschrieben. Man kann die Authentisierung mit wenig Aufwand ausnutzen, um auf den geheimen Teilnehmerschlüssel K_i zu schließen. Mathematischer Hintergrund ist das sogenannte Geburtstagsparadoxon, welches kryptografisch einem Angriff auf Werte von Hashfunktionen entspricht. Das ursprüngliche Bedrohungsszenario in der Publikation von 1998 drehte sich um das Klonen von GSM-Authentisierungsinformationen, um Anrufe mit der Identität eines anderen Teilnehmers zu tätigen (der Angriff geht von physischer Nähe zum GSM-Endgerät bzw. der SIM-Karte aus). Eine Designschwachstelle im COMP128 Algorithmus Version 1 begünstigt beide Attacken. COMP128 Version 2 und Version 3 stärken die Authentisierung.

Nach wie vor bleibt allerdings das Problem, dass die Authentisierung nur einseitig ist. Ein Angriff durch falsche Basisstationen bleibt dadurch möglich. In 3G Netzwerken ist zwar die Authentisierung in beide Richtungen vorgesehen, aber wir bezweifeln, dass dies so bei allen Mobilfunkbetreibern konfiguriert ist.[17]

Passive Attacken

Das Abgreifen von Daten an der Luftschnittstelle ist möglich und kann schon mit geringem bis moderaten Aufwand betrieben werden. Bestimmte Betriebsmodi wie Frequency Hopping oder OFDM[18] lassen sich mit aktuellen Mitteln noch nicht erfassen. Das Universal Software Radio Peripheral (USRP) ist eine mögliche Hardwareplattform für passive Attacken. Es handelt sich dabei um ein per USB ansteuerbares Peripheriegerät, welches softwaregesteuerte Funkgeräte mit Computern verbindet. Die Abbildung 5 zeigt ein solches Gerät. Man sieht die Stecker für die Empfangsbauteile, die in verschiedenen Frequenzspektren verfügbar sind. Man erhält damit Zugang zu den Daten auf der Luft-

15 http://opensource.srlabs.de/projects/a51-decrypt

16 http://web.luchs.at/t.php?c=y36LsboC1beHaDw

17 An dieser Stelle sei angemerkt, dass österreichische Mobilfunkbetreiber in bestimmten Ländern einen schlechten Ruf in punkto Netzsicherheit haben und österreichische SIM-Karten auf schwarzen Listen geführt werden. Auf Bedarf können wir eine Verbindung zur Quelle herstellen.

18 Orthogonal Frequency-Division Multiplexing (OFDM), eine störungsunempfindliche Modulationsart für Signaltransmissionen.

schnittstelle und kann diese mit geeigneter Software auswerten.

Eine weitere Möglichkeit sind Mobiltelefone mit dem Calypso Digital Base Band Chipsatz (beispielsweise Motorola C123/C115/C140, Sony Ericsson J100i). Die technischen Spezifikationen des Chips[19] wurden publiziert[20] und erlauben damit Softwareentwicklern den direkten Zugriff auf das Base Band Interface. Damit lässt sich die OsmocomBB[21] Software betreiben, welche ebenfalls den Zugriff auf die Luftschnittstelle ermöglicht.

Gekoppelt mit den bereits diskutierten Schwächen von A5 lassen sich mit den passiven Attacken Gespräche und Datentransmissionen abhören. Die Entwickler von OsmocomBB haben diese Attacke bereits mit einem Handy durchgeführt und die neue Version ihres Tools auf der DeepSec 2010 vorgestellt.

Aktive Attacken

Aktive Attacken erfordern aktive Komponenten, die auch auf den vom Mobilfunk verwendeten Frequenzen senden. Der Betrieb solcher Anlagen ist nicht erlaubt, allerdings steht die Hardware dazu zum Verkauf und kann teilweise selbst mit erschwinglichen Mitteln gebaut werden. Das OpenBTS-Projekt[22] kombiniert die bereits vorgestellte Universal Software Radio Peripheral (USRP) Hardware zusammen mit einer Asterisk-Telefonanlage[23]zu einer GSM-Basisstation. Mit OpenBTS wurden bereits Feldversuche am Burning Man Festival 2009 und 2010 sowie auf der Pazifikinsel Niue (in Kooperation mit dem dortigen Mobilfunkbetreiber) durchgeführt.

Mehrere BTS lassen sich mit einem Base Station Controller zusammenfassen. Für dessen Betrieb gibt es auch ein Softwareprojekt namens OpenBSC[24]. Es ist hierbei anzumerken, dass die aufgeführten Softwareprojekte als primäres Ziel haben die beteiligten Protokolle zu untersuchen und Sicherheitsmechanismen, die im GSM-Standard vorgesehen sind, zu überprüfen. Dadurch konnten Sicherheitsforscher schon sehr viel profitieren.

Aktive Attacken täuschen ein Mobilfunknetzwerk vor und locken Endgeräte an. Wenn man ein stärkeres Signal erzeugen kann, lassen sich so Endgeräte aus dem eigentlich Netz abziehen und in das eigene Netz umbuchen. Man kann dann

- Man-in-the-Middle (Mittelsmannattacken) durchführen sowie
- die International Mobile Subscriber Identity (IMSI) ermitteln (sog. IMSI Catcher).

Das Endgerät muss dazu im 2G Modus sein. Da nahezu alle handelsüblichen Geräte 2G und 3G unterstützen, ist dies keine Einschränkung. Man kann eine solche Attacke sehen, wenn man die Kennungen der zuletzt verwendeten Basisstationen vergleicht, jedoch gibt es kaum Firmware, die das unterstützt. Abgesehen davon ist der Wechsel von Basisstationen und ein 2G Downgrade durch schlechten Empfang ein durchaus öfters vorkommendes Ereignis, d.h. man muss sehr genau wissen ob ein solches Ereignis eine Anomalie darstellt. Angreifer können beispielsweise einen Wechsel auf 2G durch Stören der 3G Frequenzen

19 http://bb.osmocom.org/trac/wiki/Calypso

20 Die technische Dokumentation des Chipsatzes wurde durch Geheimhaltungsabkommen geschützt. Die Dokumentation wurde unabsichtlich publiziert und steht damit Entwicklern zur Verfügung.

21 Open source mobile communications Base-Band

22 http://openbts.sourceforge.net

23 http://www.asterisk.org

24 http://openbsc.osmocom.org/trac/wiki/OpenBSC

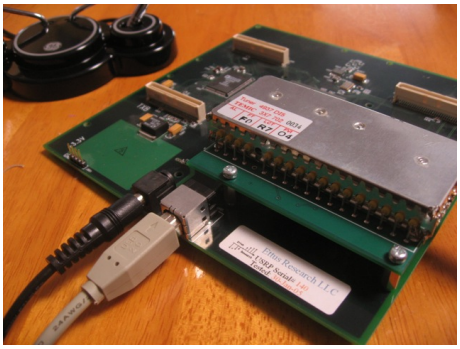


Abbildung 5: Das Bild zeigt ein Universal Software Radio Peripheral mit angeschlossenem USB-Kabel und TVRX Empfänger für die Frequenzen zwischen 50 MHz und 870 MHz.

herbeiführen.

Natürlich ist eine aktive Attacke sehr riskant und kann nicht nebenbei stattfinden. Abhängig vom Szenario besteht durch die Kombination der bereits vorgestellten Schwächen und Werkzeuge ein mittleres Risiko, das nicht unterschätzt werden darf.

Halb-aktive Attacken

Es ist möglich passive Kommunikation mitzuschneiden und anschließend eine Replay Attacke mit geänderter Krypto-Konfiguration durchzuführen. Grob skizziert kann ein solcher Angriff wie folgt ausschauen:

1. `start_cipher( A5/3, RAND )` - Gespräch passiv aufzeichnen
2. BTS simulieren und Endgerät einfangen
3. `start_cipher( A5/1, RAND )` - Downgrade auf A5/1 mit identischem $RAND$ Wert[25]
4. A5/1 brechen
5. mit gefundenem Sitzungsschlüssel die mit A5/3 aufgezeichnete Transmission dekodieren

In diesem Fall verwendet die mit A5/1 und A5/3 durchgeführten Kommunikationen denselben Schlüssel. Es handelt sich daher um eine sogenannte »Downgrade Attacke«, welche in Barkan u. a. (2006) beschrieben wird.

Aktive Signalstörungen

Es gibt Bauanleitungen für Störsender (Jammer), die sich sehr leicht nachbauen lassen. Die Sendeeigenschaften eines solchen Jammers sind ausreichend, um Mobilfunknetze lokal stark zu stören und Dienste nicht verfügbar zu machen. In Abbildung 6 sieht man den WaveBubble[26], dessen Bauanleitung verfügbar ist. Die Sendeleistung liegt zwischen 1 und 0,3 Watt. Die Frequenzabstimmung verläuft automatisch. Gesendet wird auf einstellbaren Frequenzen, d.h es lassen sich GSM, Bluetooth, WLAN und drahtlose Telefone stören.

25 Das Mobilfunknetzwerk gibt die $RAND$ Werte vor.

26 http://www.ladyada.net/make/wavebubble/

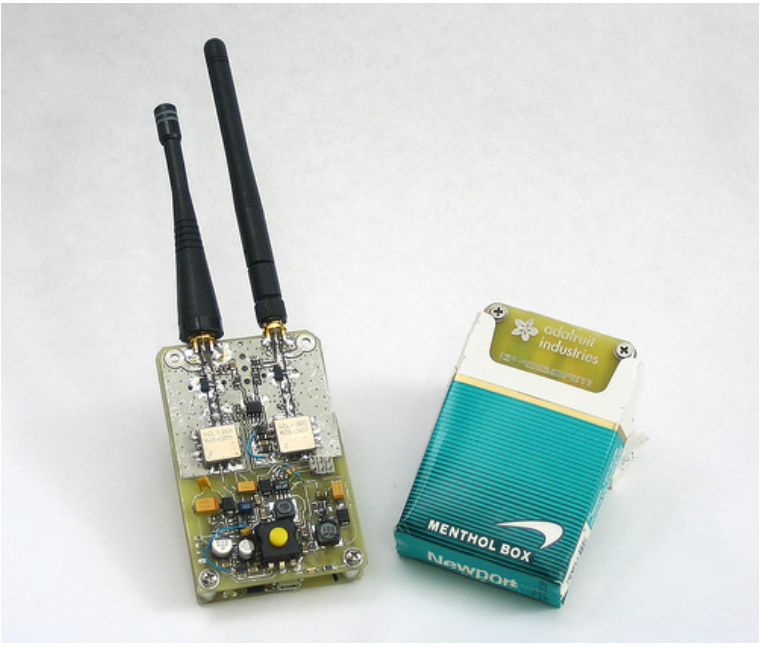


Abbildung 6: Das Bild zeigt den WaveBubble GSM-Jammer, der sich nach Bauanleitung sehr leicht in Betrieb nehmen läßt. Die Bauform ist sehr kompakt, und die Stromversorgung kann man über Akkus oder Batterien betreiben.

Einsatzgebiet solcher Jammer sind Systeme, die per GSM wichtige Nachrichten versenden (beispielsweise Alarmanlagen, die Einbrüche per SMS melden). Durch die kleine Bauform sind sie sehr portabel einsetzbar. Der Stromverbrauch ist gering genug, um einen Batteriebetrieb von 2 bis 4 Stunden zu ermöglichen. Neben WaveBubble gibt es noch weitere Jammer, deren Bauanleitungen verfügbar sind.

Es gibt außerdem noch andere Möglichkeiten aktiv einzugreifen. Auf der DeepSec 2010 hat Sylvain Munaut seine Forschungsergebnisse an der Luftschnittstelle zwischen Mobiltelefon und der nächsten Basisstation vorgestellt. Er zeigte Verfahren auf den untersten Protokollebenen zur Kanalwahl und erläuterte, wie Angreifer Mobilgeräte effektiv von einer Funkzelle abmelden und damit einen Denial-of-Service verursachen. Dies geschieht im Gegensatz zu einem Störsender innerhalb des Protokolls und kann wesentlich gezielter eingesetzt werden.

Angreifer werden solche Systeme meist nur kurzfristig und als begleitende Maßnahme verwenden.

Fazit und Empfehlungen

Vorab möchten wir betonen, dass die Aufklärung über die verwendete Konfiguration eines Mobilfunknetzwerkes allen Maßnahmen und Bedrohungsanalysen vorausgehen muss. Die 2G und 3G Technologien werden stetig erweitert, und die Netze werden periodisch nachgerüstet. Eine Bedrohungsanalyse muß die zur Verfügung stehenden Betriebsmodi kennen und sich auf den kleinsten gemeinsamen Nenner zwischen Endgeräten und Mobilfunknetz einstellen.

Alle Funkdienste im 2G/3G Bereich können mit moderatem Aufwand abgehört oder gestört werden. Damit trifft sie dasselbe Schicksal wie Wireless Fidelity Produkte. Die Gegenmaßahmen sind aus diesem Grunde ähnlich.

Abwehr von Attacken auf A5 und A3/A8

Die dargelegten Attacken auf A5 und A3/A8 lassen sich nicht abwehren. Selbst die Verwendung von KASUMI (A5/3) kann nach derzeitigem Stand der Technik umgangen werden. Speziell bei Verwendung von Mobilfunknetzwerken im Ausland spielt A5/0 und A5/2 auch noch eine Rolle.

A3/A8 sind auf dem Subscriber Identity Module (SIM) gespeichert. Änderungen erfordern daher einen Austausch der SIM Karte. Modernere SIMs, die COMP128 V2 und V3 enthalten, sind besser geschützt aber nicht offengelegt. Eine Kryptoanalyse für COMP128 V2 und V3 liegt nicht vor.[27]

Der einzige Ausweg zur Absicherung von Datentransmissionen ist hier die Verwendung zusätzlicher Verschlüsselung, bevorzugt von Ende zu Ende. Es gibt Mobiltelefone, die diese Funktion unterstützen. Bei Datentransmissionen lässt sich eine geeignete VPN[28] Technologie wie IPsec[29], SSL/TLS VPN[30] oder OpenVPN[31] verwenden.

Abwehr von passiven Attacken

Rein passive Attacken lassen sich nicht detektieren, daher bleibt hier nur die zu-

27 Für COMP128 Version 4 ist der Einsatz des Advanced Encryption Standards (AES) geplant.

28 Virtual Private Network (VPN) - Sammelbegriff für kryptografisch gesicherte Verbindungen zwischen authorisierten Endpunkten

29 http://de.wikipedia.org/wiki/IPsec

30 http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htwebvpn.html

31 http://openvpn.net/

sätzliche kryptografische Absicherung des Gesprächsinhalts bzw. der Daten. Unter Umständen kann man bei Anlagen oder Gebäuden die Standorte für passive Angreifer einschränken oder durch regelmäßige physische Kontrollen die Zeitfenster für solche Angriffe verringern.

Abwehr von aktiven Attacken

Sobald ein Angreifer aktive Attacken verwendet, wird er/sie sichtbar. Gegenmaßnahmen umfassen Detektoren für Mobilfunksignale sowie das Verfolgen/Aufzeichnen von Gerätkennungen (z.B. IDs von Basisstationen). Jammer lassen sich mit Detektoren ebenso lokalisieren.[32] Bei modernen Mobiltelefonen lassen sich unter Umständen Applikationen installieren, die Netzparameter überwachen und Abweichungen anzeigen.[33]

Verbesserungen an Mobilfunknetz und Endgeräten

Die wenigsten Mobilfunkbetreiber betreuen ihr Netzwerk selbst. Meist wird die komplette Netzplanung und -betreuung an eine Drittfirma ausgelagert (nahezu ausschließlich Ericsson, Nokia-Siemens, Alcatel-Lucent oder Huawei).[34] Dieser obliegen dann auch die Wartung und damit die Wartungen der Soft- und Hardware. Upgrades werden daher vom übergeordneten Mobilfunkbetreiber aus Kostengründe nur in Auftrag gegeben, wenn es unbedingt notwendig ist.

Bei den Endgeräten verhält es sich analog. Firmware zu den Endgeräten ist im Paket mit Wartung enthalten. Upgrades sind auf eine bestimmte Anzahl beschränkt. Hat man diese aufgebraucht, so werden weitere Upgrades zusätzlich verrechnet. Es geht hier um große Abnahmemengen. Die österreichischen Mobilfunkbetreiber sind zu klein, um direkt mit den Herstellern verhandeln zu können.[35] Viele Produkte sind daher im Verbund mehrerer Mobilfunkbetreiber auf dem Markt. Eine Chance auf Verbesserungen in Form von verbesserten Design oder Upgrades erscheint sehr gering (mit Ausnahme von Android- oder iOS-basierten Endgeräten, wo das System von Google bzw. Apple zur Verfügung gestellt wird und die Zyklen kürzer sind).

Sicherheitsforschung

Die folgenden Punkte wurden aus den Vorträgen über GSM/3G entnommen, die während der DeepSec 2010 Konferenz gehalten wurden.

Sowohl von GSM/3G als auch von TCP/IP stehen die Spezifikationen öffentlich zur Verfügung.[36] Die Implementationen des Internet Protokolls sind aber im Gegensatz zu denen von GSM/3G viel besser analysiert und getestet. Die Gründe sind vielschichtig:

- Die GSM-Industrie ist ein geschlossener Kreis.
- Es gibt nur etwa 4 Implementationen des Protokolls, von allen ist der Quellcode nicht verfügbar.

32 Wie gut die Lokalisierung funktioniert, hängt natürlich stark von der Topologie vor Ort ab.

33 Gerüchten zufolge gibt es eine Applikation für das Nokia N900, welches die Präsenz von IMSI Catchern entdecken und melden kann. Bitte nehmen Sie mit uns Kontakt auf, wenn Sie in diesem Bereich Nachforschungen anstellen wollen.

34 Einzige Ausnahmen sind kleinere Hersteller für Femto-/Nano-/Pikozellen oder Meßstationen.

35 Wurde in der Pressekonferenz der DeepSec 2010 von Harald Welte diskutiert.

36 Im Falle von GSM/3G sind das mehr als 1000 PDF Dokumenten, von denen einige mehr als 1000 Seiten haben.

- Hersteller von GSM-Chips publizieren keine Dokumentation der Hardware.
- Nur wenige Hersteller produzieren die Chips für den GSM/3.5G Baseband-Bereich, die dazugehörige Software (Kern und Protokollimplementation) werden dazugekauft.
- Nur sehr wenige Endgerätehersteller sind in der Lage bei den Herstellern der Chips direkt zu kaufen. Zugang zur Hardwaredokumentation ist strikt limitiert, die Firmware ist unzugänglich.

Zusammengefasst heißt das:

- Es gibt kaum Experten außerhalb der GSM/3G Industrie, die ausreichende Kenntnis zur Sicherheitsanalyse haben.
- Es gibt keine unabhängige Forschung im Bereich Protokollsicherheit.
- Es gibt keine Implementierungen in Open Source / Freier Software Lizenz (was für unabhängige Forschung ein Grundbaustein ist).

Die GSM/3G Industrie erschwert eine ausführliche und wissenschaftliche Sicherheitsanalyse aller Komponenten bewusst. Umgekehrt ist es Sicherheitsforschern aus dem bisherigen Kenntnisstand klar, dass die bestehenden Implementationen nur schwache Sicherheitsmaßnahmen enthalten. Mit diesem Modell lassen sich die bisherigen Schwächen erklären, und es ist zu vermuten, dass noch mehr Angriffspunkte gefunden werden, da sich nun vermehrt Sicherheitsforscher mit GSM/3G befassen.

Über die Autoren

René Pfeiffer ...

Michael Kafka ...

Die DeepSec GmbH veranstaltet seit 2007 jährlich im November die »DeepSec In-Depth Security Conference« in Wien. Die DeepSec bringt als neutrale Plattform die Sicherheitsexperten aus allen Bereichen zum Gedanken- und Erfahrungsaustausch zusammen. Dort erhalten IT- und Security-Unternehmen, Anwender, Behördenvertreter, Forscher und die Hacker-Community in über 30 Vorträgen und Workshops die Chance, sich über die aktuellen und zukünftigen Sicherheitsthemen auszutauschen. Die Konferenz will aber auch dem verbreiteten Vorurteil entgegen wirken, dass Hacker zwangsläufig Kriminelle sind.

Literaturverzeichnis

Barkan, E., Bihan, E. & Keller, N. (2006). Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication. Haifa: Israel Institute of Technology. Zugriff am 12. Januar 2012, unter http://cryptome.org/gsm-crack-bbk.pdf

Dunkelman, O., Keller, N. & Shamir, A. (2010). A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony. Cryptology ePrint Archive, Report 2010/013. Zugriff am 12. Januar 2012, unter http://eprint.iacr.org

Goldberg, I., Wagner, D. & Green, L. (1999). The (Real-Time) Cryptanalysis of A5/2. Rump session of Crypto'99.

Golic, J. D. (1997). Cryptanalysis of Alleged A5 Stream Cipher. Zugriff am 12. Januar 2012, unter http://cryptome.org/jya/a5-hack.htm

Kafka, M. & Pfeiffer, R. (2012). Angriffe und Verteidigungsstrategien für vertrauliche Kommunikation über Funkdienste. *Magdeburger Journal zur Sicherheitsforschung*, 2, 308–322.

Zugriff am 16. Juli 2012, unter http://www.sicherheitsforschung-magdeburg.de/journal_archiv.html

Nohl, K. & Melette, L. (2011). GPRS Intercept: Wardriving phone networks. CCC. Zugriff am 12. Januar 2012, unter http://events.ccc.de/camp/2011/Fahrplan/events/4504.en.html

Südmeyer, P. (2006). A performance oriented implementation of COMP128. Bochum: Ruhr-Universität Bochum. Zugriff am 12. Januar 2012, unter http://www.suedmeyer.net/inhalte/pdf/comp128_thesis.pdf

Wray, S. (2003). COMP128: A Birthday Surprise. Zugriff am 12. Januar 2012, unter http://www.stuartwray.net/comp128-a-birthday-surprise-rev.pdf

16. Dezember 2012