

WEBSTANDARD-INTERVIEW

## Mobiltelefone abhören? GSM macht's leicht!

VON ANDREAS PROSCHOFSKY | 20. Dezember 2010, 17:12



Wer lauscht mit? GSM-Netze machen mit grundlegenden Sicherheitslücken das Ausspionieren vergleichsweise einfach.

Image: GSM Roof, a Creative Commons Attribution (2.0) image from txberiu's photostream



### GSM-Hacker Harald Welte im Gespräch über seit Jahren bekannte, schwerwiegende Lücken in allen Netzen

Die meisten haben in mobile Netzwerke ein viel höheres Vertrauen als in das Internet, dies vollkommen zu unrecht - so attestiert es einer, der mit durchaus ausgiebigem Wissen in diesem Bereich aufwarten kann: Harald Welte war unter anderem am Openmoko-Projekt beteiligt, welches sich zum Ziel gesetzt hatte, eine vollständig freie Softwareplattform für Mobiltelefone zu etablieren. Und auch wenn er dieses Unterfangen zwischenzeitlich hinter sich gelassen hat, bleibt Welte doch der Thematik verbunden. Er gehört zu einer Gruppe von Entwicklern, die auf grundlegende Sicherheitsprobleme in Mobilfunknetzen aufmerksam machen will. Dies nicht zuletzt, in dem man Open-Source-Tools schreibt, die die diversen Lücken veranschaulichen. Zusätzlich engagiert sich Welte für die Durchsetzung von freien Softwarelizenzen, mit seiner Plattform [gpl-violations.org](http://gpl-violations.org) konnte er in den vergangenen Jahren bereits einige Erfolge verbuchen.

Im folgenden Interview geht Welte auf die zentralen Problembereiche rund um GSM ein, und veranschaulicht so auch, dass es keine sonderliche Hexerei ist, Telefongespräche - oder auch Datenübertragungen - abzuhören. Das Gespräch führte Andreas Proschofsky am Rande der jährlich in Wien abgehaltenen Sicherheitskonferenz Deepsec, die sich in diesem Jahr einen besonderen Schwerpunkt auf den Punkt mobile Sicherheit gegeben hat.

**derStandard.at:** In den letzten Jahren ist die Mobilfunktechnologie GSM zunehmend in die Kritik gekommen, vor allem die mangelhafte Sicherheit wurde immer wieder beklagt. Können Sie zunächst mal grob umreißen, worum es hier konkret geht?

**Harald Welte:** Wir haben bei GSM eine Technologie die aus den Achtziger-Jahren stammt, basierend auf den damaligen Technologien und geprägt durch die einstige politische Situation. Das heißt, es wurde entwickelt von den damals noch staatsmonopolistischen Telefonunternehmen innerhalb der Europäischen Gemeinschaft, wo sich alle Operator kannten und gegenseitig vertrauten. Das ist ein für heute problematischer Ausgangspunkt. Ein anderer ist, dass die damals höchste für zivile Zwecke zugelassene Verschlüsselung Single-DES mit 56-Bit für Bank-Anwendungen war. Die Design-Prämisse für das GSM-Netz war, dass man schlechter als dies sein müsse, sonst hätte man dies politisch nicht einfach nicht durch bekommen. Und das ist ja auch alles schön und gut, das Problem ist nur, dass mittlerweile 25 Jahre vergangen sind, und das Verschlüsselungsverfahren für Gespräche noch immer das gleich ist, das ist ein grundlegendes Übel.

Gleichzeitig haben wir die Entwicklung des Internets, das von einer Vielzahl von Unternehmen und Organisationen getrieben wurde, und nicht nur von ein paar Monopolbetrieben. Entsprechend hat gerade was die IT-Security betrifft, das Internet die Mobiltelefonie ganz schnell überholt. Zwar ist auch hier das Netz grundsätzlich nicht vertrauenswürdig, aber immerhin wissen die meisten, dass ihre Daten offen einsehbar sind, wenn sie unverschlüsselt surfen. Der Anwender bringt hingegen paradoxerweise dem Telefonnetz ein wesentlich höheres Vertrauen entgegen, was leider gänzlich unbegründet ist.

**derStandard.at:** Selbst können sich die AnwenderInnen aber auch kaum gegen Probleme im Mobilfunknetz wehren, oder?

**Harald Welte:** Ja, das ist das nächste Problem. Wenn ich einen PC ans Internet anschließe, dann kann ich selbst entscheiden, ob ich eine Firewall verwende, welche Software ich einsetze, ob ich die aktuellen Updates einspiele. Das ist mir überlassen - und damit auch einem relativ freien Markt von Sicherheitsanbietern - kommerzielle und nicht kommerzielle. Und auf den Telefonen ist das so, dass das alles sehr viel restriktiver und sehr viel kontrollierter ist. Dass man selber Software auf Telefonen installieren kann, ist ja überhaupt ein Feature, das erst mit iPhone, Android und so richtig populär geworden ist. Und selbst da passiert dies ja nur auf Anwendungsebene. Das heißt: Man kann jetzt zwar selber eine App nachinstallieren, aber das gesamte System darunter kann ich in keinster Weise beeinflussen.

**derStandard.at:** Um das herazustreichen: In einem aktuellen Smartphone gibt es immer zwei parallel installierte Betriebssysteme?

**Harald Welte:** Ja, richtig. Es gibt da zunächst mal den Baseband Processor, der sich um das eigentliche Interface zum GSM oder 3G-Netz kümmert. Und dann gibt es noch den Application-Processor, auf dem dann Windows Mobile, iOS, Android läuft.

Während die meisten NutzerInnen die Application-Seite sehr gut kennen und dort ihre Anwendungen im Blick haben, ist der Baseband-Processor sozusagen die schwarze Box, von der niemand so recht weiß, was sie tut. Für die Gerätehersteller ist das natürlich genau umgekehrt, die vertrauen ihrer eigenen Baseband-Software, und misstrauen all dem neuen Linux und Unix-Zeug, das da so installiert wird. Und das führt dann eben auch dazu, dass der Baseband-Processor den Application Processor kontrollieren kann, der kann diesen also etwa abschalten oder neu starten, umgekehrt geht das aber nicht unbedingt. In manchen Designs kann der Baseband-Processor auch komplett auf den Speicher des Application-Processor zugreifen. Das heißt in dem Moment, wo jemand die Sicherheit der Baseband-Seite kompromittiert, kann er alles am Application Processor sehen. Und gegen dieses Einfallstor kann ich selbst eigentlich überhaupt nichts tun.

**derStandard.at:** In dem Moment bieten mir dann natürlich auch die ganzen Verschlüsselungsprogramme - für SMS, Mail usw. - keine vollständige Sicherheit mehr, da die Texte ja - zumindest theoretisch - direkt am Gerät über einen Einbruch am Baseband-Processor mitgelesen werden könnten.

**Harald Welte:** Genau. Damit ist das hinfällig. Das hängt natürlich von der konkreten Lösung ab, aber gerade bei den integrierten Lösungen von Qualcomm ist das der Fall - und die stecken in einer Vielzahl von Geräten. Ein weiteres Problem ist, dass klassischerweise all die Dinge wie Videokamera, Mikrophon und Lautsprecher direkt am Baseband Processor hängen. Was ja auch klar ist, weil das ist der eigentliche Telefonierteil des Mobiltelefons, während der Application Processor quasi der PDA ist. In dem Moment wo dann aber jemand in den Baseband Processor einbricht, kann er dann auch das Mikrophon aufdrehen und mithören - ohne dass das nach außen irgendwie sichtbar ist.

**derStandard.at:** Sind solche Angriffe auf den Baseband-Processor jetzt rein theoretischer Natur, oder gibt es da auch reale Beispiele?

**Harald Welte:** Es gibt tatsächlich bis jetzt keine offiziell dokumentierten Vorfälle. Aber: Es gibt hier auf

der Konferenz auch einen Vortrag von Ralf Philipp Weinmann von der Universität Luxemburg, der es geschafft hat, in alle gängigen, weitverbreiteten Baseband-Prozessoren einen Exploit reinzubringen. Das ist also keine rein theoretische Möglichkeit.

**derStandard.at:** In den letzten Monaten und Jahren wurde immer wieder vorgezeigt, wie mit einer eigenen Basisstation Telefongespräche abgefangen werden können. Ist dies tatsächlich so einfach?

**Harald Welte:** Ja. Bei GSM und Edge - also alles kleiner 3G - gibt es keine "Mutual Authentication", das heißt, das Telefon hat keine Möglichkeit zu wissen, ob es mit einem echten oder einem falschen Netz verbunden ist. Ich kann hier also einfach eine eigene Mobilfunkzelle hinstellen, sagen ich bin "A1" oder "T-Mobile Austria" und die Telefone in der Umgebung werden diese benutzen, wenn es das für sie stärkste Signal hat. Dadurch, dass es dagegen keinerlei Absicherung gibt, ist natürlich allen möglichen Dingen Tür und Tor geöffnet.

Das ist dann eben wieder so eine fundamentale Geschichte, die aus der Historie der Netze bedingt ist. Damals konnte man sich einfach nicht vorstellen, dass irgendwer jenseits einiger weniger Monopolbetriebe jemals ein Netz betreiben wird. Oder auch dass sich jemand Privater jemals eine eigene Mobilfunkzelle basteln kann - und heute ist das ziemlich einfach möglich. Und dann hat man es auch verpasst, die Systeme im Laufe der Zeit zu reformieren und entsprechende Systeme einzubauen. Es ist ja nicht so, dass heute noch wo Basisstationen stehen, die 20 Jahre alt sind, die Hersteller machen ja ohnehin alle paar Jahre ein Upgrade ihres Equipments. Man hätte sich also schon vor Jahren um die bekannten Probleme kümmern können - aber es gibt halt kein Interesse daran.

Um ein Beispiel zu bringen: Der Nachfolger der jetzt verwendeten Verschlüsselungsalgorithmus bei GSM wurde bereits 2002 spezifiziert, 2010 hat ihn noch kein einziger Operator im Einsatz. Und auch wenn diese neue Lösung noch genug Probleme hat, so wäre sie doch ein Fortschritt, acht Jahre lang ist aber aber mal nichts passiert.

**derStandard.at:** Wenn ich das richtig in Erinnerung habe, ist selbst die sehr schwache heute eingesetzte Verschlüsselung nicht wirklich verpflichtend, oder?

**Harald Welte:** Ja. Im GSM-Netz ist es so, dass alle Sicherheitsfeatures optional sind. Das heißt das Netzwerk entscheidet, mach ich Authentifizierung oder nicht, verwende ich Verschlüsselung oder nicht, welchen Algorithmus verwende ich. Und der Anwender hat nicht nur keine Einfluss darauf, er wird auch gar nicht informiert. Softwareseitig wäre es natürlich super-einfach da eine Anzeige zu machen, was jetzt gerade für eine Verschlüsselung verwendet wird - wie es ja etwa bei Browsern gängig ist. Das gibt es hier nicht. Nur bei ein paar alten Mobiltelefonen gab es diese Möglichkeit, aber das bringt auch nichts, da der Netzbetreiber die Anzeige dieser Informationen wieder durch eine Konfiguration der SIM-Karte unterdrücken kann.

**derStandard.at:** Und machen das die Netzbetreiber auch?

**Harald Welte:** Ja. Bei allen SIM-Karten die ich mir bisher angesehen habe, war das so konfiguriert. Aber wie gesagt, unterstützen das aktuelle Mobiltelefone ohnehin nicht mehr.

**derStandard.at:** Aber warum verbergen die Betreiber diese Information?

**Harald Welte:** Weil sie die Anwender nicht aufregen möchten. Es gibt da eine gute Dokumentation dazu: Es gab ja bis vor einigen Jahren mit dem A5/2 noch einen schlechteren Verschlüsselungsstandard, der wurde 2006 verboten. Und wenn man sich da die Unterlagen der Standardisierungsgremien anschaut, dann waren insbesondere amerikanische Operator extrem aufgeregt und nervös darüber, dass ihre Kunden bemerken könnten, dass da schlechte Verschlüsselung zum Einsatz kommt - also entsprechende Informationen unter keinen Umständen den Kunden gezeigt werden.

Und dann gibt es natürlich ein Problem mit der Motivation: Der Netzbetreiber hat keinerlei Motivation

dem Anwender Privatsphäre oder Vertraulichkeit der Information zu bieten - das gibt es einfach nicht. Davon hat er kein Geschäft, der Operator verdient kein Geld durch zusätzliche Sicherheit - also warum sollte er das tun?

**derStandard.at:** Bietet UMTS zumindest für die Datenübertragung eine höhere Sicherheit?

Harald Welte: Prinzipiell schon. Das Problem ist allerdings, dass es bei einem Angriff leicht ist, das 3G-Netz zu stören, wodurch das Mobiltelefon automatisch auf 2G zurückfällt - und die ganze zusätzliche Sicherheit wieder weg ist. Zusätzlich ist 3G ja auch noch immer nicht flächendeckend verfügbar

**derStandard.at:** Sind diese Lücken im GSM-Netz eigentlich rein theoretischer Natur oder werden diese auch aktiv ausgenutzt?

Harald Welte: Aber natürlich sind die real. Kein IMSI-Catcher (der von der Polizei zu größeren Abhöraktionen eingesetzt werden kann, Anm.) würde funktionieren wenn es diese Lücke in der Authentifizierung nicht gäbe. So ein IMSI-Catcher ist ja auch nichts anderes als eine gefälschte Basisstation, die alle Gespräche in der Umgebung auf sich zieht. Es gibt zumindest seit zehn Jahren Techniken, die diese Fehler ganz aktiv ausnutzen.

**derStandard.at:** Machen sich auch nicht-staatliche Organisationen diese Fehler zu nutze?

**Harald Welte:** Ja. Es ist zum Beispiel dokumentiert, dass in Afghanistan auf beiden Seiten IMSI-Catcher verwendet werden.

Darüber hinaus gibt es aber noch eine ganze weitere Klasse von Problemen. So kann jeder einzelne Netzbetreiber weltweit Anfragen an alle anderen Netze stellen. Dafür gibt es eigene Schnittstellen - und das macht ja prinzipiell auch Sinn, weil die Netze miteinander kommunizieren können müssen. Aber diese Schnittstellen wurden halt auch spezifiziert als man sich kaum Gedanken über Sicherheit gemacht hat. So kann also etwa jeder beliebige Betreiber herausfinden, wo sich eine einzelne Person derzeit aufhält. Das ist nicht sehr genau, das Land findet man immer, meistens auch die Stadt, bei größeren Städten auch Teile davon. Hat nun etwa ein Auslandsgeheimdienst irgendwo die Telefonnummer eines Politikers reicht das um über diesen Reiseprofile zu erstellen.

**derStandard.at:** Gibt es aktive Bestrebungen den GSM-Standard zu verbessern?

**Harald Welte:** Wenige. Es gab zwar über die Jahre immer wieder kleinere Verbesserungen an der Spezifikation, das Problem ist, dass man der Kompatibilität wegen viele Lücken drinnen lässt. Es gibt zum Beispiel im GSM-Standard schon seit einigen Jahren eine Spezifikation für die zuvor erwähnte "Mutual Authentication", aber es gibt keine Möglichkeit, dass das Endgerät diese einfordern kann. Die Entscheidung bleibt also beim Netz, was die Sicherheitsverbesserung effektiv zunichte macht. Denn wenn ich eine falsche Basisstation aufstelle, sag ich natürlich, dass ich keine beidseitige Authentifizierung will - und damit gibt sich das Telefon zufrieden, ohne dass der Anwender je davon erfährt.

Es wäre also auch jetzt schon ganz einfach möglich, dass Mobiltelefone zumindest einen gewissen Mindeststandard zur Verschlüsselung verlangen, was ja etwa gerade für Unternehmen durchaus interessant sein sollte, um die Sicherheit der Mitarbeiter zu erhöhen. Aber das geht halt dann wieder nicht, weil die Hersteller der Geräte bzw. der benutzten Chipsets diesen Eingriff nicht erlauben.

**derStandard.at:** Ist das Aufstellen einer gefälschten Basisstation eigentlich die einzige Möglichkeit für Dritte ein Gespräch mitzuhören, oder gibt es hier noch andere Lücken?

**Harald Welte:** Gibt es. Ich kann beispielsweise passiv mithören, indem ich einfach einen Funkempfänger in der Nähe aufstelle und dann die Verschlüsselung knacke. Auf halbwegs gängiger PC-Hardware sollte das in so ca. 35 Sekunden erledigt sein. Das ist auch schon lange bekannt.

Mithören kann ich weiters an der Verbindung zwischen der Basisstation und den nächsthöheren

Netzwerkelementen. Diese sind ja auch oft über Mikrowellen-Richtfunkstrecken realisiert, spezifiziert war das aber mal für Kabel, also wird hier in aller Regel nicht verschlüsselt. Da hab ich dann nicht nur ein Gespräch sondern gleich hunderte bis tausende Gespräche, die völlig unverschlüsselt quer durch die Stadt gehen. Da ist zwar der technische Anspruch für das Abhören etwas höher, weil diese Mikrowellentechnik mit "Hausmitteln" etwas schwerer beherrschbar ist, aber da gibt es auch Leute, die sich aktuell damit beschäftigen und da kann man sicher sein, dass da in den nächsten Jahren noch etwas kommen wird.

Eine weitere Abhörmöglichkeit sind die "Lawful Interception"-Schnittstellen, über die normalerweise die Polizei bei Gesprächen mitlauschen kann - im jeweiligen rechtlichen Rahmen. Es gibt aber auch belegbare Beweise, dass diese Schnittstellen schon von Dritten zum Abhören benutzt wurden.

**derStandard.at:** Zum Beispiel?

**Harald Welte:** Es gab den Fall Vodafone Griechenland im Jahr 2004, wo diese Schnittstellen von der organisierten Kriminalität benutzt wurden, um Spitzenpolitiker abzuhören - über mehrere Monate hinweg.

**derStandard.at:** Wenn ich das mal so zusammenfasse, gibt es also mittlerweile eine Fülle von Möglichkeiten Telefongespräche abzuhören - und das dazu noch ohne sonderlich großen finanziellen Aufwand.

**Harald Welte:** Ja. Das mangelnde Wissen ist eigentlich das Hauptproblem, warum so wenig öffentliches Bewusstsein über diese Lücken da ist. Es gibt halt fünf Hersteller auf der Netzwerkseite, fünf Hersteller auf der Telefonseite, die die entsprechenden Implementierungen machen, und wenn man jetzt nicht gerade für eine dieser Firmen arbeitet, dann weiß man nichts davon. Und auf Universitäten wird das ja auch nicht gelehrt.

Das ist auch alles nicht neu, es gibt Hersteller die entsprechende Geräte zum Abhören seit vielen Jahren anbieten, das beginnt so bei 200.000 Dollar und geht dann in die Millionen hinauf. Neu ist nur dass wir das jetzt in Open Source machen, um die Leute auf diese Problematik aufmerksam zu machen.

Übrigens find ich das Abhören von Gesprächen gar nicht so das spannende Thema, viel interessanter sind eigentlich all die sensiblen Daten die über GSM-Netze verschickt werden: Das geht von Schlüsselsystemen über Zugkommunikation bis zum Telefonbanking - alles über ein sehr schlecht geschütztes System und damit leicht für Dritte abzufangen.

**derStandard.at:** Inwiefern ist Open Source hilfreich, um auf diese Probleme aufmerksam zu machen?

**Harald Welte:** Open Source ist insofern nützlich, als dass die Ergebnisse der angewandten Sicherheitsforschung in diesem Bereich für jedermann nachvollziehbar sind. Es gibt ja Leute, die schon seit Jahren auf diese Probleme hinweisen, aber das will halt keiner hören, da wird dann immer an der realen Umsetzbarkeit gezweifelt. Also arbeiten jetzt Leute wie ich in den letzten zwei, drei Jahren an dem Thema, um klar nachvollziehbar zu zeigen, dass die Probleme nicht nur auf dem Papier existieren, sondern dass man die Lücken auch tatsächlich ausnutzen kann.

**derStandard.at:** Wir danken für das Gespräch.

(Andreas Proschofsky, derStandard.at, 20.12.10)

Der WebStandard auf Facebook

#### Links

Blog von Harald Welte

Openmoko

gpl-violations.org

Deepsec

---

© derStandard.at GmbH 2010 -

Alle Rechte vorbehalten. Nutzung ausschließlich für den privaten Eigenbedarf.  
Eine Weiterverwendung und Reproduktion über den persönlichen Gebrauch hinaus ist nicht gestattet.