

Der Lauschangriff auf die Telefonkommunikation

Bei Funktechnik besteht grundsätzlich die Gefahr des Mithörens und von Angriffen auf das Netzwerk, auch bei der DECT-Technologie. Doch wie ist es um Störanfälligkeit, Sicherheit und Abhörschutz innerhalb der kabellosen Kommunikation bestellt? Wie leicht können Dritte in eine Mobilfunk- (GSM/UMTS) oder DECT-Verbindung eindringen und persönliche oder vertrauliche Informationen mithören oder gar missbrauchen? Vor dem Hintergrund jüngster Telefonabhörskandale wird deutlich, wie wichtig es ist, dass die Kommunikation per Telefon vertraulich bleiben muss.

Text: **Stephan Böttger**, Revisor und Berater / HSP ADVICE

Weltweit wächst die schnurlose Sprach- und Datenkommunikation auf hohem Niveau. Neben bluetoothfähigen Geräten, WLAN-Komponenten und GSM-Telefonen sind es vor allem Geräte auf Basis der DECT-Technologie (Digital Enhanced Cordless Telecommunications), die private Anwender und Unternehmen aller Größen und Branchen erobert haben. Zum Einsatz kommt DECT insbesondere als reichweitenstarke Schnurlos-Technologie in Telefonen oder bei Headsets. Unschlagbarer Vorteil: Anwendern im Büro eröffnet sich Mobilität auch fernab ihres Arbeitsplatzes. An anderer Stelle wird hierauf nochmals detailliert eingegangen.

Vorsicht, unerwünschte Mithörer: Nicht nur staatliche Stellen können sich unbemerkt in jedes Telefonat einschalten. Wie weitreichend diese Maßnahmen gehen können und welche Gründe gegeben sein müssen, lässt sich unter anderem aus den Vorschriften der §§ 100 ff. StPO und den §§ 23 ff. PolG entnehmen. Die Telekommunikationsüberwachungsverordnung (TKÜV) schreibt in § 8 Abs. 2 Nr. 4 hierfür sogar vor, dass die Tonqualität für die Lauscher „nicht schlechter als die der zu überwachenden Telekommunikation“ sein darf. Für das Jahr 2007 gab die Bundesnetzagentur bekannt, dass 44.278 richterliche Anordnungen zur Überwachung durchgeführt

wurden. Alleine 39.200 davon betrafen Mobilfunknutzer. Die Tendenz ist stark steigend. In Deutschland sind die gewerblichen Betreiber von öffentlichen Telekommunikationseinrichtungen gesetzlich verpflichtet, die Überwachung technisch zu ermöglichen. Das Mithören erfolgt unter anderem durch einen sogenannten IMSI-Catcher (International Mobile Subscriber Identity).

Hierzu muss jedoch erst einmal die Nummer des Verdächtigen bekannt sein. Im Festnetzbereich ist das einfach: Es ist die Rufnummer des Telefonanschlusses in der zu überwachenden Wohnung oder der Firmenräume. Mobiltelefone hingegen lassen sich nicht immer einer Person zuordnen, auch dann nicht, wenn beim Kauf einer Prepaidkarte die Registrierung der Personalausweisedaten obligatorisch ist. Aber keine Handy-Kommunikation ohne sogenannte IMSI. Diese International Mobile Subscriber Identity ist eine von der Rufnummer unabhängige 15-stellige Ziffernfolge, die auf der SIM-Karte des Handys gespeichert ist.

Die IMSI wird für jede SIM-Karte individuell vergeben. Mit dieser Nummer weist sich das Handy gegenüber dem Netz aus. Die Netzbetreiber verknüpfen die IMSI mit der jeweiligen Rufnummer. Vereinfacht ausgedrückt heißt das, wer also die IMSI kennt, kann bei Vorlage einer richterlichen Anordnung beim Netzbetreiber einen Abhör-



trag stellen und in bester Qualität mithören. Und wer sich diese direkte Leitung nicht legen lassen kann, z. B. als privater Verbraucher oder ausländischer Dienst, muss noch lange nicht ins Leere hören: Der IMSI-Catcher fängt nicht nur die Nummer, sondern ermöglicht auch einen diskreten Lauschangriff über das Funknetz.

Über die Basisstation mit dem jeweils stärksten Signal (und dem dahinter liegendem Netz) erfolgt der Verbindungsaufbau und das Telefonat. Ein eingeschaltetes Mobiltelefon versucht immer in Kontakt zur signalstärksten Basisstation seines Netzes zu bleiben. Der sich bewegendende Benutzer bekommt davon in aller Regel gar nichts mit. Wer nun mit einem Radio (Scanner) dem Funkverkehr zwischen Handy und Basisstation zuhört, wird selbst dann nichts verstehen, wenn er diesen digitalen Datenstrom demodulieren¹ kann. Er ist so verschlüsselt, dass er sich nur mit erheblichem Aufwand – und vor

1 Demodulation ist die Wiedergewinnung der Information, die zuvor durch Modulation auf einen Träger aufmoduliert wurde. Bei der Demodulation werden der oder die informationstragenden Parameter (z. B. Frequenz, Phase, Amplitude, Tastverhältnis) des modulierten Trägers ausgewertet und zur weiteren Verarbeitung wiederum einer technischen Größe aufgeprägt (z. B. eine der Information proportionalen elektrischen Spannung oder einem binären Zahlenwert in der Digitaltechnik). Schaltungen zur Demodulation werden Demodulator genannt.

allem nicht live – decodieren ließe. Wer in diesen Funkverkehr einbrechen will, muss sich somit als Basisstation verkleiden.

Der IMSI-Catcher hat daher zwei Aufgaben: Gegenüber dem Handy tritt er als Basisstation auf und spiegelt ferner den tatsächlichen Basisstationen der Netzbetreiber ein Handy vor. Ein gewünschtes Handy herauszufiltern ist eine anspruchsvolle Aufgabe. Hierzu ist der Verdächtige zu beobachten und die Sendeleistung des IMSI-Catchers so einzustellen, dass möglichst nur sein Handy anspricht. Ein zu starkes Signal oder eine zu große Menschengruppe mit eingeschaltetem Mobilteil in der Tasche machte die Sache unübersichtlich.

Hat der IMSI-Catcher das betreffende Handy an der Angel, so fragt er einfach nach der IMSI. In Millisekunden ist dieser Vorgang abgeschlossen. Möglich macht dieses Ausspionieren etwas, was das Bundesamt für Sicherheit in der Informationstechnik für „einen Designfehler im GSM-Standard“ hält, auf den sich auf der ganzen Welt mehr als zwei Milliarden Menschen verlassen. Bei GSM muss sich nur das Handy gegenüber der Basisstation ausweisen, nicht jedoch umgekehrt die Basisstation gegenüber dem Handy. Erst beim neuen UMTS-Netz gibt es eine beiderseitige Authentifizierung.

Mit einfachen Mitteln, handelsüblicher Technik und geringem Aufwand wäre es jedem Konkurrenten nun möglich, sich den entscheidenden Wettbewerbsvorteil zu „erlauschen“. Es versteht sich von selbst, dass solche Handlungen nicht zulässig und strafbewehrt sind.

UMTS

Ein Trick ermöglicht auch bei UMTS das Anzapfen.

Nach dem Nummernempfang schaltet der Lauscher den IMSI-Catcher wieder ab und zapft diesen Anschluss nun direkt beim Netzbetreiber an. Der unbefugte Mithörer hingegen sendet dem Handy noch einen weiteren Befehl: „Verschlüsselung abschalten!“ Die ohnehin lediglich auf dem Funkwege verwendete Verschlüsselung abschalten zu können, war eine Forderung mehrerer Staaten an den internationalen Mobilfunkstandard GSM. Angerufen werden kann der so Abgehörte in diesem Zustand nicht, denn sein Handy ist ja nur über den IMSI-Catcher mit dem Netzbetreiber verbunden. Der wiederum sieht nur die SIM-Karte des Catchers, nicht aber die des eigentlichen Handys, das währenddessen unauffindbar bleibt. Das alles geht weitgehend spurlos vor sich. Da IMSI-Catcher im UMTS-Netz nicht ohne Weiteres Nummern fangen und mitlauschen können, hilft ein Trick. Ein Störsender verdirbt den UMTS-Empfang, woraufhin das Handy automatisch in das GSM-Netz wechselt.

Gibt es Schutzmechanismen? Geht man nach dem Hersteller No.1 Business Communication ist es jetzt für jedermann möglich, Handygespräche absolut abhör- und manipulationssicher zu führen.

Möglich machen soll dies die No.1BC-Card, und das 100 % legal, ohne technische Stolperfallen. Das System basiert auf Voice over IP und verfügt über einen dreiteiligen Schutzmechanismus. Die Mischung aus einer Smart- und einer Flash-Memory-Card kombiniert symmetrische und asymmetrische Verschlüsselungen (Hybrid-Verschlüsselung) mit 512 Bit beziehungsweise 2048 Bit langen Schlüsselpaaren.

Unter Beachtung der geltenden Richtlinien des BSI (Bundesamt für Sicherheit in der Informationstechnik,

BSI-DSZ-CC-0348-2006) erfüllt der integrierte Kryptographie²-Chip die Kriterien der Sicherheitsstufe EAL5+³. Um die Verschlüsselung der No.1BC-Card mit Hilfe einer sogenannten Brute-Force-Attacke⁴, also dem Durchspielen aller möglichen Kombinationen, zu knacken, würde selbst die amerikanische Sicherheitsbehörde NSA Hunderte von Millionen Jahre benötigen, so der österreichische Hersteller.

Alle privaten Informationen wie etwa die persönliche Kontaktliste sind verschlüsselt auf geschützten Datenbank-Servern gespeichert. Ein Zugriff darauf ist nur mit dem privaten Schlüssel der No.1BC-Card möglich. Die Kommunikation erfolgt stets über eine hybrid verschlüsselte Internetverbindung.

Inbetriebnahme und Bedienung. Die Inbetriebnahme und die Bedienung soll vergleichsweise einfach sein. Der Nutzer muss lediglich die No.1BC-Card in den microSD-Schacht seines Smartphones stecken und die zugehörige Applikation installieren. Nach einem Neustart des Telefons ist die Anwendung betriebsbereit. Mittels einer maximal 8-stelligen PIN meldet sich der User am Server an. Vergisst ein User seine PIN, kann nicht einmal der Hersteller diese wieder freischalten.

.....

2 Kryptographie (auch: Kryptografie; griechisch: „verborgen“ und „schreiben“) ist die Wissenschaft der Verschlüsselung von Informationen.

3 Nach den Information Technology Security Evaluation Criteria (ITSEC): Kriterien für die Bewertung der Sicherheit von Informationstechnologie; ist ein europäischer Standard für die Bewertung und Zertifizierung von Software und Computersystemen in Hinblick auf ihre Funktionalität und Vertrauenswürdigkeit bezüglich der Daten- und Computersicherheit.

4 Die Brute-Force-Methode (engl. für „Methode der rohen Gewalt“), auch Exhaustionsmethode (von lat. exhaurire = ausschöpfen), ist eine Lösungsmethode für Probleme aus den Bereichen Informatik, Kryptologie und Spieltheorie, die auf dem Ausprobieren aller (oder zumindest vieler) möglichen Fälle beruht.

In diesem Fall ist eine neue No.1BC-Card erforderlich. Alle bis dahin gespeicherten Kontakte müssen aus Sicherheitsgründen ebenfalls neu angelegt werden. Zu jeder No.1BC-Card gehört eine weltweit einmalige 11-stellige BC-Nummer. Diese dient als Kennung des Benutzers und zur eindeutigen Identifizierung gegenüber Gesprächspartnern. Sichere Anrufe können nur zwischen Nutzern getätigt werden, die ihre BC-Nummern ausgetauscht und in der Applikation als Kontakt hinterlegt haben. Unbekannte Anrufer sind damit ausgeschlossen.

Systemvoraussetzungen und Preis. Um No.1BC nutzen zu können, muss das Smartphone mindestens über einen 520+-MHz-Prozessor und einen freien microSD-Steckplatz verfügen. Des Weiteren ist eine breitbandige Internet-Verbindung erforderlich. Geeignet sind die Mobilfunkstandards HSDPA, UMTS und EDGE. Auch kabellose Netzwerke nach dem Wi-Fi-Standard kommen in Frage. Um die beste Sprachqualität zu erhalten, sollte die Internetverbindung mit der kürzestmöglichen Signallaufzeit ausgewählt werden. Gegenwärtig wird als Betriebssystem das weitverbreitete Windows Mobile 6 von Microsoft unterstützt. Eine Version für Blackberry und Symbian OS soll in Kürze verfügbar sein.

Sicherheit hat ihren Preis. Die No.1BC-Card ist seit April 2009 in Deutschland. Die unverbindliche Preisempfehlung für Deutschland lautet 1.190 Euro inklusive Mehr-

wertsteuer. Im Preis enthalten ist bereits die Nutzungsgebühr in Höhe von 280 Euro zuzüglich Mehrwertsteuer für das erste Jahr. Diese Gebühr wird jährlich fällig.

DECT

Da DECT ein digitales, funkbasiertes Verfahren ist, besteht grundsätzlich die Gefahr eines unberechtigten Zugriffs Dritter. Fremde DECT-fähige Geräte – so die Theorie – könnten sich aktiv in eine laufende Verbindung einschalten und das Gespräch mithören. Damit das nicht passiert, bestehen kryptographische Authentisierungs- und Verschlüsselungsalgorithmen sowie die Tatsache, dass der Zugriff auf die Daten in Echtzeit – also während des laufenden Gesprächs – erfolgen muss. Grund: Die Telefonate können weder in den Basis- oder Mobilstationen der Telefone noch in Headsets gespeichert werden.

Mit Hilfe einer modifizierten Com-On-Air-Karte können DECT-Telefonate ganz einfach abgehört werden. Auch die Verschlüsselung bietet keinen Schutz vertraulicher Gespräche.

Hacker erörterten auf dem 25. Chaos Communication Congress (25C3) in Berlin, dass sich die schnurlose Kommunikation auf Basis von DECT (Digital Enhanced Cordless Telecommunications) ganz leicht abhören lässt. Benötigt wird dafür eine für die Internet-Telefonie gedachte

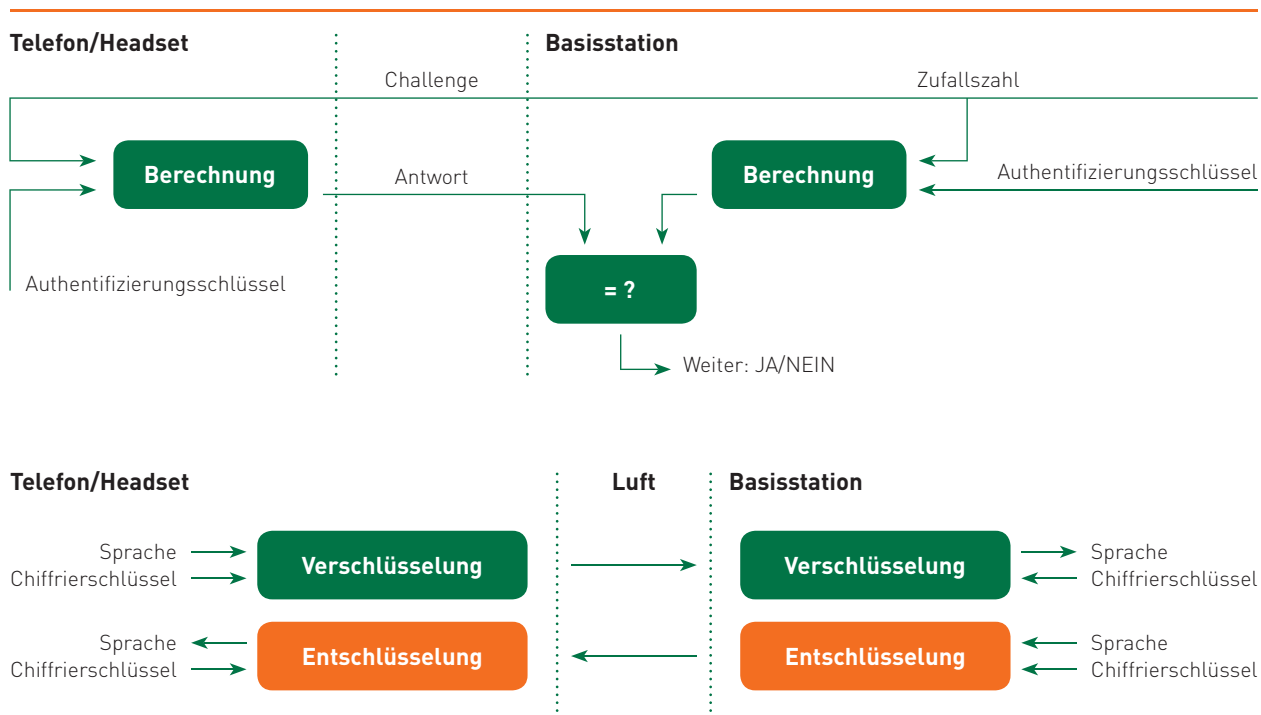


Abb.: DECT-Verschlüsselungsprinzip

Laptop-Karte für 23,00 Euro (Com-On-Air) sowie ein Linux-Rechner mit einem von den Hackern entwickelten Treiber, welcher mittlerweile in einschlägigen Foren kostenlos zum Download angeboten wird.

Bisher galt DECT als sicher. Für die Authentisierung der Basis und der zugehörigen Endgeräte sowie für die mögliche Verschlüsselung der Datenübertragung nutzt DECT standardisierte Kryptoverfahren. Außerdem sind die Verschlüsselungsalgorithmen in den Geräten fest verankert und nur den Herstellern bekannt. Mit der Com-On-Air-Karte wurde jedoch eine einfache und günstige Möglichkeit gefunden, den Datenverkehr zu empfangen. Nach einer Modifizierung der Karte konnte diese als Tool zum Mithören/Aufzeichnen von DECT-Telefonaten genutzt werden.

Wird der Datenverkehr im DECT-Netz verschlüsselt, funktioniert das einfache Mithören nicht. Jedoch verbinden sich alle getesteten Endgeräte auch dann mit einer Basisstation, wenn diese keine Verschlüsselung unterstützt. Mit Hilfe eines modifizierten Treibers und eines Skripts lässt sich der Sniffer⁵ als Basisstation ausgeben: Dadurch können Gespräche abgefangen und etwa über einen Asterisk-Server⁶ (VoIP) umgeleitet werden.

Aber auch beim Verschlüsselungssystem selbst wurden Schwachstellen entdeckt. So gelang es den Hackern, ein Reverse Engineering⁷ des zentralen DECT Standard Authentication Algorithm (DSAA) durchzuführen. Es gibt auch erste Ansatzpunkte beim DECT Standard Cipher⁸ (DSC). Die Experten nutzen ein Patent, das Alcatel in Spanien und in den USA beantragt hat, um mögliche Schwachstellen zu finden. Darüber hinaus kündigten die Autoren des WLAN-Sniffers Kismet⁹ an, in naher Zukunft

auch DECT zu unterstützen. Die Com-On-Air-Karte wird aber auch dann benötigt, da WLAN-Hardware nicht mit DECT kompatibel ist.

Interessant ist auch, dass seit Bekanntwerden dieser Informationen, die Com-On-Air-Karte des mittlerweile insolventen Herstellers bei eBay um bis zu 1.100 % im Preis gestiegen ist.

Fazit

Mit einfachen Mitteln, handelsüblicher Technik und geringem Aufwand wäre es jedem Konkurrenten nun möglich, sich den entscheidenden Wettbewerbsvorteil zu „erlauschen“. Es versteht sich von selbst, dass solche Handlungen nicht zulässig und strafbewehrt sind.

5 Ein Sniffer (engl. „to sniff“ für riechen, schnüffeln) ist eine Software, die den Datenverkehr eines Netzwerks empfangen, aufzeichnen, darstellen und ggf. auswerten kann. Es handelt sich also um ein Werkzeug der Netzwerkanalyse.

6 Asterisk ist eine freie Software, die alle Funktionalitäten einer herkömmlichen Telefonanlage abdeckt. Asterisk unterstützt Voice Over IP (VoIP) mit unterschiedlichen Protokollen und kann mittels relativ günstiger Hardware mit Anschlüssen wie POTS (analoger Telefonanschluss), ISDN-Basisanschluss (BRI) oder -Primärmultiplexanschluss (PRI, E1 oder T1) verbunden werden.

7 Reverse Engineering (engl., bedeutet: umgekehrt entwickeln, rekonstruieren, Kürzel: RE) bezeichnet den Vorgang, aus einem bestehenden, fertigen System oder einem meistens industriell gefertigten Produkt durch Untersuchung der Strukturen, Zustände und Verhaltensweisen, die Konstruktionselemente zu extrahieren.

8 Der DECT Standard Cipher ist der Verschlüsselungsstandard, der beim mobilen Telefonieren mit DECT auf der Funkstrecke zum Einsatz kommt. Die Spezifikation des DECT Standard Cipher wurde bisher nicht veröffentlicht und ist nur unter bestimmten Voraussetzungen vom Europäischen Institut für Telekommunikationsnormen (ETSI) erhältlich.

9 Kismet ist ein freier passiver WLAN-Sniffer zum Aufspüren von Funknetzwerken.



Herr **Stephan Böttger** ist Revisor und Berater bei der HSP ADVICE Unternehmensberatung GmbH & Co. KG.