

## Serie: Der kleine Lauschangriff (4)

# Angriff auf ISDN, Fax und GSM

Telefonverbindungen sind und bleiben neuralgische Punkte des persönlichen Nachrichtenaustausches. Wegen ihrer Bedeutsamkeit einerseits und der bisweilen leichten Abhörmöglichkeiten werden sie auch weiterhin im Focus von Geheimdiensten und neugierigen Nachbarn stehen. Dieter Görrisch hat sich in der vierten Folge seiner Serie den Abgehörgefahren beim „Telekommunizieren“ gewidmet.

Bedingt durch die vielen Kommunikationsdienste, die heute der Markt bietet, sind natürlich auch die technischen Anforderungen an potentielle Lauscher gestiegen. Diese müssen sich heute gleich mit mehreren Kommunikationsverfahren sowie unterschiedlichen Übertragungsprotokollen auseinandersetzen und aufwendiges Gerät einsetzen, wenn sie etwas mithören möchten.

**Analoge Telefonleitungen:** Hier genügt ein parallelgeschaltetes Telefon, um den beiden Leitungsadern eine Information zu entlocken. Aufwendigere Geräte protokollieren natürlich auch gewählte Nummern mit oder können geführte Gespräche automatisch aufnehmen.

Immerhin rüstet die Telekom ihre Hausverteiler seit einiger Zeit mit Stahlgehäusen und Schlössern aus, um wenigstens allzu neugierige Nachbarn abzuschrecken.

Wesentlich schwieriger dürfte es wohl sein, analoge FAX-Übertragungen (nach Gruppe 3, 9600 Baud) mitzuschreiben, denn das bloße Parallelschalten eines weiteren Faxgerätes an die abzuhörende Leitung nützt hier wenig! Dafür gibt es aber kommerzielle Software, wie beispielsweise FaxProbe 3.0 der US-Firma Gentech, die auf jedem PC lauffähig ist (siehe auch unter <http://www.gentech.com>). Wird die Leitung angezapft und der Rechner mit beiden Telefonadern über eine Schnittstelle verbunden, erscheint der gefaxte Text samt Begleitinformationen wie Datum, Uhrzeit oder Bitfehlerrate am Computerbildschirm. Auch im Zusammenhang mit Abhöraktionen von Fernmeldesatelliten wie etwa Inmarsat, über die massenweise analoger Faxverkehr abgewickelt wird, werden derartige FAX-Dekoderprogramme für Lauscher immer bedeutsamer.

**ISDN-Telefonleitungen:** Im Gegensatz zu analoger Übertragung wird bei ISDN-Leitungen ein digitaler Datenstrom auf den Leitungen übertragen. Die Digitalisierung der



ISDN-Prüfapparat der Firma Festo mit Mithöreinrichtung. Foto: Festo

Sprache findet nämlich schon in den Endgeräten statt. Zudem ist zwischen dem Leitungsabschluß der Telekom (dem NTBA) und den Haustelefonen eine vieradrige Busleitung eingesetzt. Das verleitet so manchen Zeitgenossen zu der Annahme, man könne solche Leitungen nicht mehr abhören.

Doch weit gefehlt, es gibt bereits die ersten ISDN-Prüftelefone (ursprünglich zu Meß- und Servicezwecken gedacht) mit einer Mithöreinrichtung. So muß lediglich noch der gewünschte Übertragungskanal (es gibt im ISDN ja bekanntlich zwei Sprachübertragungskanäle pro Leitung) im Menü des Gerätes eingestellt werden, und schon hört man ev. stattfindende Gespräche auf der Leitung mit. Es dürfte wohl nur noch eine Frage der Zeit sein, bis entsprechende Computerprogramme auf dem Markt sind, die ISDN-Karten bestückten PCs ebenfalls zu derartigen Funktionalitäten verhelfen.

**GSM-Funktelefone:** Über die Schwierigkeiten, die beim Abhören von zellular arbeitenden Funktelefonen nach GSM-Standard auftreten, ist bereits vielerorts berichtet worden (RADIO-SCANNER 2/97). Grund für diese „Abhörprobleme“ an der Luftschnittstelle dürfte in erster Linie das aufwendige Verschlüsselungsverfahren sein, dem die di-

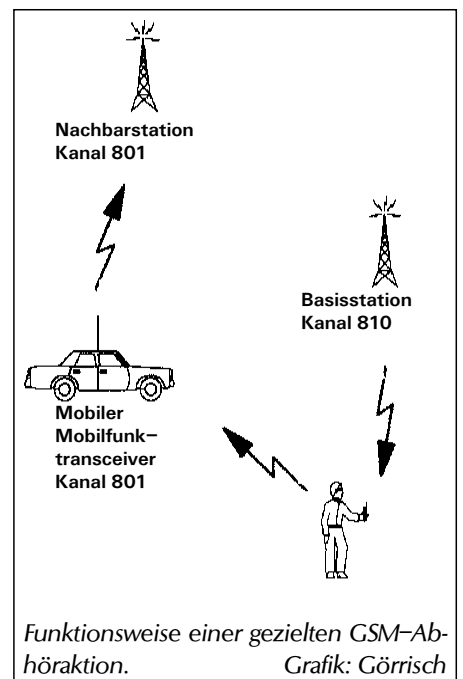
gitalisierten Sprachsignale vor ihrer Aussendung unterzogen werden.

**Dennoch scheint nun eine technische Lösung gefunden worden zu sein, die zumindest das gezielte Abhören von GSM-Mobitelefonen ermöglicht.**

Um das Prinzip zu verstehen, zunächst ein kurzer Ausflug in das GSM-Verfahren: Großflächige Bereiche werden immer von mehreren sog. Basisstationen versorgt. Um eine Größenordnung zu nennen, soll eine Stadt mittlerer Größe beispielsweise mit 10 Basisstationen versorgt werden, die jeweils einen eigenen Frequenzkanal verwenden. Telefoniert man nun im Netz, sucht sich das Handy zunächst die gerade am besten empfangbare Funkzelle des Netzes aus und nimmt Kontakt mit der dazugehörigen Basisstation auf (im Beispiel Kanal 810). Ändert man seinen Standort während des Gesprächs nicht, wickelt man meist das ganze Gespräch auf dieser Frequenz (und dem zugewiesenen Zeitschlitz ab).

Um alle Möglichkeiten abzusichern, überträgt die Basisstation dem Handy aber auch eine Frequenztabelle mit Alternativfrequenzen benachbarter Basisstationen, die es ständig abscannt und auf die es bei Bedarf wechseln kann. Dies ist bei Störungen der Arbeitsfrequenz oder aber auch bei Ortswechsel des Handys erforderlich.

Beim angesprochenen Abhörverfahren wird nun ein tragbarer Mobilfunktransceiver in unmittelbare Nähe des abzuhörenden Handys gebracht und ein starkes Funksignal erzeugt, dessen Frequenz einer solchen Alternativfrequenz entspricht. Das Handy erkennt den besseren Träger, meldet dies



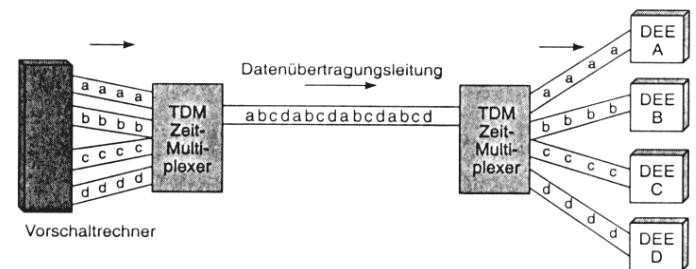
dem Funknetz. Sofort wird ein sog. Handover (Kanal- und Zeitschlitzwechsel) auf die neue (Transceiver-) Frequenz ausgelöst.

**Somit ist das Gespräch auf den Mobilfunktransceiver umgeleitet, der es seinerseits wie ein zweites Handy zur Nachbar-Basisstation weiterleitet. Sowohl der Telefonkunde, als auch das Funksystem bekommen von dieser Manipulation nichts mit.**

Lediglich ein erfahrener Spezialist könnte mit einem sog. Monitor-Handy, das sind Handys die auch Betriebsdaten (wie Arbeitskanal, Zeitschlitz, Timing-Advance dgl.) am Display anzeigen, die Manipulation erkennen. Ist der gesamte Datenstrom des Handys erst mal umgeleitet, können die erforderlichen Manipulationen in der Signalisierung vorgenommen werden.

Der Trick besteht nun darin, dem Handy durch den eingeschleiften Transceiver jenes GSM-Steuerkommando zuzuführen, welches die Verschlüsselung der Daten wieder abschaltet. Der dann unverschlüsselte digitale Datenstrom wird in einem D/A-Wandler wieder zurückverwandelt. Was sich hier so fürchterlich kompliziert anhört, erledigt ein mikroprozessorgesteuertes Gerät in wenigen Augenblicken.

Dieter Görrisch



*Beim Zeitmultiplex wird die verfügbare Bandbreite nach dem TDMA-Verfahren in Zeitschlitze aufgeteilt.*

Quelle: Lipinski (Hg.): Lexikon der Datenkommunikation, DATACOM Buchverlag

## GSM-Glossar:

**GSM-Arbeitskanal:** Vollduplex-Frequenzkanäle, die von Mobilfunksystemen verwendet werden, Modulationsart ist GMSK, von gewöhnlichen Scannern nicht dekodierbar!

**Zeitschlitz:** Da bei GSM jeder Arbeitskanal von mehreren Geräten gleichzeitig genutzt werden kann, ist er in einzelne Zeitsegmente unterteilt, sog. Zeitschlitze. Um eine Verbindung herzustellen, ist also nicht nur die Angabe der Frequenz notwendig, sondern auch noch des gerade verwendeten Zeitschlitzes.

**Handover:** Bezeichnung für die Weiterreichung einer Verbindung zu einer Nachbarschaftszelle. Das Funksystem wertet die Messungen des Handys ständig aus und leitet bei Bedarf einen Handover ein.

**Timing Advance:** Da jedes Handy einen Zeitschlitz zugewiesen bekommt, muß es seine Datenpakete mit hoher zeitlicher Genauigkeit absetzen. Weil die Entfernung zur Basisstation auf die Übertragungszeit Einfluß nimmt, wird dies elektronisch korrigiert. Eine Regelschleife sorgt dafür, daß das Datenpaket vom Handy um so früher abgesendet wird, je weiter die Basisstation entfernt ist.

Dieser Korrekturwert wird „Timing Advance“ genannt und von Monitorhandys direkt angezeigt. Die Entfernung zur Basisstation kann damit auf etwa 100 m genau ermittelt werden. Eingriffe in den Übertragungsweg (z.B. Betrieb über Mobilfunkrepeater) machen sich durch die Laufzeitvergrößerung durch eine schlagartige Änderung dieses Wertes bemerkbar.

**ISDN:** Telefonverfahren, das voll digital arbeitet. Eine ISDN-Busleitung besteht aus vier Adern, dem sog. S0-Bus, der zwei Gespräche (B1/B2-Kanäle) gleichzeitig übertragen kann. Zudem findet noch ein Signalisierungskanal (sog. D-Kanal) Platz, auf dem das gesprächs begleitende Protokoll ausgetauscht wird.