



Jabra

SICHERHEITSFUNKTION DER DECT TECHNOLOGIE

Die kabellose Sprach- und Datenkommunikation wächst weltweit. Im Zuge dieser „Wireless“-Revolution wachsen auch die Sorgen um die Sicherheit der kabellosen Kommunikation. Mehr und mehr Fachleute und Laien fragen sich: Ist die kabellose Übertragung stör- und abhörsicher? Können Dritte in eine Wireless-Übertragung eindringen und persönliche oder vertrauliche Informationen abrufen?

A BRAND BY

 GN Netcom

JABRA® IS A REGISTERED TRADEMARK OF GN NETCOM A/S

WWW.JABRA.COM

DIE DECT-TECHNOLOGIE BIETET HOHEN SCHUTZ GEGEN UNBERECHTIGTE ZUGRIFFE

HINTERGRUND

Die kabellose Sprach- und Datenkommunikation wächst weltweit. Die Anzahl von DECT- (Digital Enhanced Cordless Telecommunications) und GSM-Telefonen, Bluetooth®-fähigen Geräten und WLAN-Komponenten ist in den vergangenen Jahren sowohl in den Unternehmen als auch in den privaten Haushalten enorm gestiegen.

Doch im Zuge dieser „Wireless“-Revolution wachsen auch die Sorgen um die Sicherheit der kabellosen Kommunikation. Mehr und mehr Fachleute und Laien fragen sich: Ist die kabellose Übertragung stör- und abhörsicher? Können Dritte in eine Wireless-Übertragung eindringen und persönliche oder vertrauliche Informationen abrufen?

Verlässliche Antworten auf diese und andere sicherheitsrelevante Fragen werden dringend benötigt. Unternehmen wie

Angestellte haben ein Recht darauf, dass ihre Kommunikation vertraulich bleibt und nicht belauscht wird, und dass ihnen durch die Nutzung von kabellosen Kommunikationsgeräten keine persönlichen oder unternehmerischen Risiken entstehen. GN Netcom produziert schnurlose Headsets für die DECT-basierte Telekommunikation. In diesem Dokument untersuchen wir die Sicherheitsmerkmale des DECT-Protokolls, um die tatsächlichen Sicherheitsrisiken dieser Technologie kritisch und objektiv darzustellen.

WAS IST DECT?

DECT ist eine Funktechnologie, die sich ideal für Sprach-, Daten- und Netzwerkanwendungen mit einer Übertragungreichweite von bis zu einigen 100 Metern eignet. Es handelt sich um eine durch und durch digitale Kommunikationstechnologie, die zwei oder mehr Geräte in privaten Haushalten, in Unternehmen oder in öffentlichen Einrichtungen kabellos miteinander verbindet.

ZUSAMMENFASSUNG

Das Risiko des unerlaubten Abhörens von Telefongesprächen über eine DECT-Verbindung ist ausgesprochen gering.

Die Sicherheitsfunktionen der DECT-Technologie garantieren ein hohes Maß an Sicherheit. Der DECT-Standard ist in 110 Ländern als verbindliche Norm geregelt, er wird von Millionen von Menschen genutzt und zählt zu den sichersten Standards für kabellose Anwendungen im dienstlichen Bereich. Unabhängig davon, ob Mitarbeiter schnurlose DECT-Telefone oder -Headsets nutzen, der Schutz vor unberechtigten Zugriffen auf die kabellose Telefonverbindung ist sehr hoch.

Die Sorge, Dritte könnten DECT-Signale abfangen und so Telefongespräche abhören, ist auch deshalb unbegründet, da die nötige Ausrüstung für einen solchen Lauschangriff auf dem Markt nicht erhältlich ist. Selbst wenn es Dritten gelänge, DECT-Funksignale abzufangen, wären enorme Rechenressourcen sowie Transaktionsdaten von mehreren Monaten notwendig, um die Signale zu entschlüsseln.

Sollte jemand direkten Zugriff auf DECT-Geräte erhalten und das Pairing eines schnurlosen DECT-Telefons oder -Headsets mit einer DECT-Basisstation herstellen können, könnte er Gespräche ausschließlich über diese Geräte abhören, nicht aber über andere Geräte im DECT-System.

Die integrierten Sicherheitsroutinen des DECT-Protokolls und der Mangel an geeigneter Ausrüstung für einen Lauschangriff machen es zusammen so schwierig, unberechtigt auf eine DECT-Übertragung zuzugreifen, dass es nach Aussage des führenden dänischen Sicherheitsexperten Torben Rune¹ bislang kein einziges Beispiel für einen solchen Fall gegeben hat. Rune hält andere Möglichkeiten, Zugriff auf vertrauliche Informationen zu erhalten, für wahrscheinlicher als den Lauschangriff auf eine DECT-Übertragung.

Zudem ist die kabellose DECT-Verbindung an sich viel sicherer als das klassische Kupferkabel, da sie grundsätzlich digital und verschlüsselt ist. Je mehr Kupferkabel durch DECT-Verbindungen ersetzt werden, desto höher ist folglich die Sicherheit der Telefonanlage insgesamt. Anders als WLAN- oder Bluetooth®-Geräte bietet das DECT-Protokoll integrierte Sicherheitsroutinen, die sich nicht deaktivieren lassen.

1 Torben Rune, CEO von Netplan A/S (www.netplan.dk).

Die DECT-Technologie bietet eine hohe Sprachqualität und eine große Sicherheit. Die Gefahr von Interferenzen mit anderen Funkanwendungen ist zugleich sehr gering. Seit der Einführung der ersten, durch das ETSI² verabschiedeten Norm im Jahr 1992 bildet DECT in vielen schnurlosen Telefonen und Headsets die Grundlage der Sprachkommunikation.

DECT wandelt analoge Töne (z. B. ein Gespräch) zu einem digitalen Datenstrom, der anschließend von einem DECT-Gerät zum anderen übertragen wird. Erreicht der Datenstrom das Empfangsgerät, wird er wieder in ein analoges Signal gewandelt und an ein schnurloses Telefon oder Headset weitergegeben.

DECT ist eine bewährte Technologie, die noch über viele Jahre eine wichtige Rolle spielen wird. In den vergangenen Jahren ist die Anzahl der Datenanwendungen, die auf Grundlage von DECT entwickelt wurden, leicht gestiegen, doch den Löwenanteil der DECT-Datenübertragung macht nach wie vor die Sprachkommunikation aus.

WIE GROSS IST DAS PROBLEM?

Das DECT-Verfahren ist sowohl in der Theorie als auch in der Praxis ein sehr sicheres Verfahren der kabellosen Datenübertragung. Uns ist seit Einführung des DECT-Verfahrens nicht ein einziges Beispiel bekannt geworden, in dem übermittelte Daten in Gefahr gewesen wären – und wir sind Teil dieses Marktes!

Die hohe Sicherheit der DECT-Datenübertragung ist auch darauf zurückzuführen, dass das DECT-Protokoll vor allem für die Sprachkommunikation über DECT-fähige Telefone und Headsets eingesetzt wurde und eingesetzt wird. Die Sprachübermittlung (d. h. Telefongespräche) wird jedoch weder in den Basisstationen der Jabra Produkte noch in Headsets gespeichert. Die Daten einer DECT-Übertragung existieren also nicht mehr weiter, nachdem ein Gespräch beendet wird. Jeder unerlaubte Zugriff auf die Daten muss in Echtzeit erfolgen – das heißt, noch während das Gespräch stattfindet – damit ein Dritter Zugriff auf irgendwelche Informationen erhalten kann.

Es existiert keinerlei allgemein zugängliche Ausrüstung, mit der sich DECT-Verbindungen überwachen und ihre Datenströme entschlüsseln ließen, um ein Telefongespräch wiederzugeben. DECT ist ein Verfahren zur digitalen – und nicht zur analogen – Datenübertragung, das auf sehr komplexe Verschlüsselungsalgorithmen basiert, die ausschließlich DECT-Herstellern bekannt sind.

Infolgedessen sind bislang weder Instrumente noch Computerprogramme zur Überwachung oder Ausspionierung von DECT-Verbindungen auf den Markt gekommen. Andere Wege, sich Zugang zu vertraulichen Informationen zu verschaffen, dürften daher weit weniger zeitaufwendig und kostspielig sein. Wir tei-

WORUM GEHT ES BEIM THEMA SICHERHEIT?

Die Sicherheitsfunktionen der DECT-Technologie verhindern, dass unbefugte Dritte Zugriff auf den Inhalt des elektronischen Kommunikationsflusses – in diesem Fall der Sprachkommunikation – erhalten. Die Sicherheit³ kabelloser Kommunikationsanwendungen hat zwei wesentliche Aspekte: Authentifizierung und Verschlüsselung.

AUTHENTIFIZIERUNG

Die Initial-Authentifizierung erfolgt über ein Verfahren, bei dem sich Basisstation und Hörer/Headset erstmals über „Pairing“ miteinander verbinden. Dabei rufen beide Geräte ein einzigartiges Datenflussprotokoll „Handshake“ auf, das bestimmte Regeln und Formeln umfasst, tauschen ihre Geräte-Identität aus, und sowohl Basisstation als auch Hörer/Headset führen einen geheimen Authentifizierungsschlüssel aus, der auch bei jedem späteren Vermittlungsaufbau ausgeführt wird. Diese geheime Formel wird nicht über die Funkverbindung übertragen und kann daher nicht durch Dritte abgefangen werden – nicht einmal, wenn diese physisch Zugriff auf die entsprechenden Geräte haben. Ist die Pairing-Funktion erst einmal durchgeführt, werden sich die beiden Geräte aneinander „erinnern“, das heißt, sie können sich zukünftig anhand des beim Pairing ausgetauschten Handshakes gegenseitig authentifizieren.

Ein solches Initial-Pairing kann ausschließlich über eine physische Verbindung der Geräte erfolgen, nicht aber über eine kabellose Funkverbindung. Während des Pairing-Vorgangs tauschen beide Geräte auch einzigartige Verschlüsselungsdaten aus, die ausschließlich für die jeweiligen Geräte gelten. Dieser Vorgang ist eine wesentliche Voraussetzung dafür, dass die Datenübertragung zwischen beiden Geräten verschlüsselt werden kann.

VERSCHLÜSSELUNG

Die Verschlüsselung unter DECT ist ein Verfahren, bei dem der digitale Datenstrom, der zwischen zwei Geräten hin- und herfließt, mittels komplexer Formeln absichtlich durcheinander gebracht (verschlüsselt) wird. In dem sehr unwahrscheinlichen Fall, dass Dritte Zugriff auf den Datenstrom erhalten, finden sie aufgrund der Verschlüsselung nichts weiter als unverständliches, elektronisches Kauderwelsch vor. Erst wenn der Datenstrom den passenden Empfänger erreicht, wird er wieder in sein ursprüngliches Format zurückverwandelt (entschlüsselt).

Die Verwandlung erfolgt auf Grundlage mehrerer Faktoren, die ausschließlich den beiden, durch das „Pairing“ miteinander verbundenen Geräten bekannt sind. Keiner dieser Verschlüsselungsfaktoren wird mit dem Datenstrom übermittelt. Vielmehr sind sie entweder ab Werk in die Geräte integriert oder werden im Rahmen der Initial-Authentifizierung (siehe „Authentifizierung“) vereinbart.

Das bedeutet, dass es für potenzielle Lauscher praktisch unmöglich ist, sinnvolle Informationen aus dem Datenstrom zu gewinnen.

² ETSI: Europäisches Institut für Telekommunikationsnormen (Englisch: European Telecommunications Standards Institute)

³ Es gibt keinen absoluten Sicherheitsstandard, und Sicherheitsmängel können aus den unterschiedlichsten Quellen stammen. Die kabellose Kommunikation ist lediglich eine von vielen Quellen.

len die Ansicht vieler Sicherheitsexperten, dass DECT eine sehr sichere Basis für die Sprachkommunikation bietet. Tatsächlich dürfte DECT überhaupt die sicherste Standardtechnologie sein, die für die Sprachkommunikation in Haus und Wohnung, im Unternehmen und in öffentlichen Einrichtungen zur Verfügung steht.

Darüber hinaus suchen sogenannte Hacker häufig nach Daten, die auf Servern oder auf einzelnen Computerlaufwerken gespeichert und über ein Unternehmens-LAN erreichbar sind, anstatt Telefonsysteme anzuzapfen. Auch dadurch bleiben die DECT-Datenströme der Jabra Produkte außerhalb der Reichweite von Eindringlingen.

DIREKT- ODER FERNZUGRIFF

Theoretisch wäre es für jemanden, der direkten Zugriff auf die DECT-Ausrüstung eines Unternehmens hat, einfacher einen Lauschangriff durchzuführen. Das obligatorische Pairing macht ein Abhören jedoch solange unmöglich, solange ein Dritter keinen Zugang zur Basisstation hat.

In dem sehr unwahrscheinlichen Fall, dass jemand in die Räumlichkeiten eines Unternehmens einbricht, sich Zugang zu einer Basisstation verschafft, das Pairing eines schnurlosen Telefons oder Headsets mit dem DECT-System erfolgreich nachbilden kann und das Unternehmen unbemerkt wieder verlässt, wird

dieser Dritte dennoch nicht in der Lage sein, Gespräche über andere Geräte im DECT-System abzuhören. Ein DECT-Telefonsystem bietet also auch dann noch Schutz vor Lauschangriffen, wenn ein Angreifer Zugang zu einem Telefonsystem erhalten hat. Sollte jemand tatsächlich ein schnurloses Telefon auf das Pairing einer Basisstation im DECT-System eingestellt haben, besteht die wohl größte Gefahr in der Nutzung kostenfreier Telefongespräche über das Telefonsystem des Unternehmens.

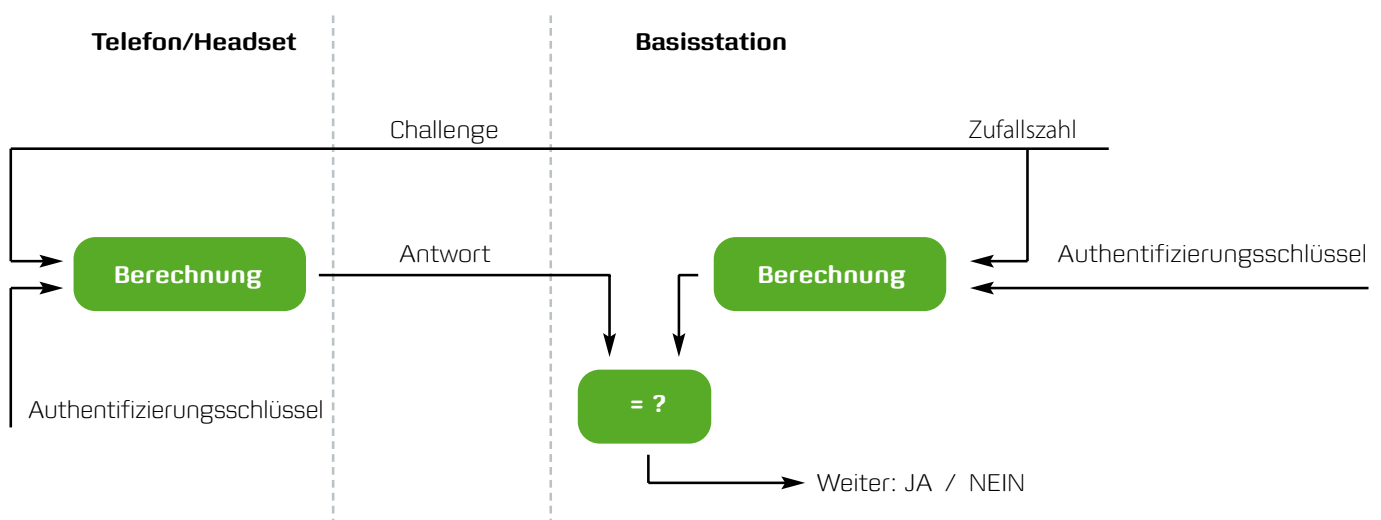
Ein Fernzugriff über kabellose Geräte, die beispielsweise an einen PC angeschlossen sind, ist – wie bereits erwähnt – sehr unwahrscheinlich, da solche Geräte quasi nicht zur Verfügung stehen.

DECT UND DIE SICHERHEITSROUTINEN IM EINZELNEN

Wie bereits beschrieben, gründet die Sicherheit der DECT-Übermittlung auf Authentifizierungs- (Algorithmus) und Verschlüsselungsmechanismen (Keystream-Generator). Im Folgenden erhalten Sie eine detaillierte Beschreibung der DECT-Sicherheitsroutinen.

DECT-AUTHENTIFIZIERUNG

DECT verwendet einen Authentifizierungsalgorithmus, der als DECT Standard Authentication Algorithm (DSAA) bezeichnet wird. Die Spezifikationen dieses Algorithmus werden nicht öf-



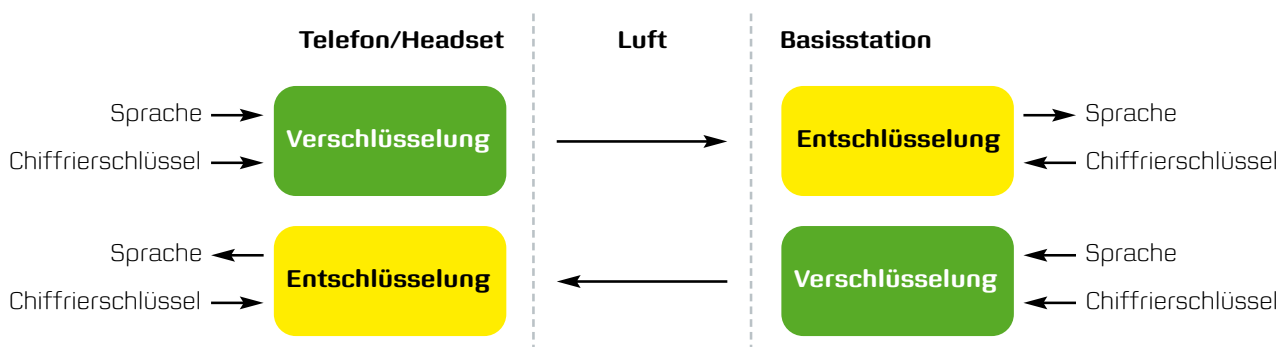
fentlich gemacht, einzig und allein die Hersteller von DECT-Geräten erhalten darauf Zugriff. Die Authentifizierung läuft folgendermaßen ab: Die Basisstation sendet über die Funkverbindung eine zufällige Zahl (die „Challenge“) an das schnurloes Telefon. Dieses führt daraufhin bestimmte Berechnungen durch und schickt der Basisstation eine Antwort, indem es die Zufallszahl nimmt und seinen eigenen Authentifizierungsschlüssel darauf anwendet (der beim Initial-Pairing kommuniziert wurde). Die Basisstation gleicht nun diese Antwort mit der zu erwartenden Antwort ab. Wenn beide übereinstimmen, authentifiziert die Basisstation das schnurlose Telefon.

DECT-VERSCHLÜSSELUNG

DECT verwendet das Verschlüsselungsverfahren DECT Standard Cipher (DSC). DSC ist eine Methode zur Verschlüsselung einer unendlichen Datenfolge unter Zuhilfenahme eines Schlüssels fester Länge (Streamcipher), der einen 35-Bit langen Initialisierungsvektor und einen Chiffrierschlüssel als Eingabewert für die Berechnung des Werteflusses (Keystream) nutzt. Der DSAA (Standardalgorithmus) für die DSC-Spezifikation wird nicht veröffentlicht. Zwei verschiedene Arten von Chiffrierschlüsseln stehen als Eingabe für den Keystream-Generator zur Verfügung:

- Ein abgeleiteter Chiffrierschlüssel – ein Ausgabewert, der aus dem Authentifizierungsprozess zwischen Basisstation und schnurlosem Telefon stammt. Wenn bei jedem neuen Telefongespräch eine Authentifizierung erfolgt, wird bei jedem neuen Gespräch ein anderer Chiffrierschlüssel verwendet.
- Ein statischer Chiffrierschlüssel – ein solcher Schlüssel kann verwendet werden, um eine Verschlüsselung zu erstellen, ohne dass zunächst das Authentifizierungsverfahren durchlaufen wird. Bei DECT wird die Generierung oder Übermittlung eines solchen Chiffrierschlüssels nicht unterstützt.

Der Initialisierungsvektor wird anhand der Frame-Nummer des zu verschlüsselnden Frames erstellt. Mit jedem neuen Frame, der gesendet wird, erhöht sich der Initialisierungsvektor entsprechend. Schließlich berechnet das DSC-Verfahren anhand des Initialisierungsvektors und des Chiffrierschlüssels einen Keystream. Der Keystream wird dann über eine XOR-Verknüpfung des zu sendenden Datenfelds chiffriert. Je nach Art des gesendeten Datenfelds werden einige Teile des Keystreams im XOR-Verknüpfungsprozess aussortiert. Die Entschlüsselung des Datenfeldes erfolgt auf dem gleichen Wege wie die Verschlüsselung.



RISIKEN & SCHUTZMASSNAHMEN

RISIKO	RISIKOBESCHREIBUNG	SCHUTZFUNKTION	AUSMASS DER GEFÄHRDUNG
Lauschangriff	Ein Dritter verschafft sich Zugang zu einer DECT-Übertragung und hört das Gespräch ab.	Sprachdaten werden zu einem digitalen Datenstrom konvertiert, der mithilfe einer 64-Bit-Verschlüsselung verschlüsselt wird.	Geringes Risiko: Geräte, die eine digitale Funkverbindung überwachen können, sind schwierig zu beschaffen. Und es ist sehr aufwendig, eine Software zu entwickeln, die Datenströme entschlüsseln kann. Eine Kombination aus beidem ist noch unwahrscheinlicher.
Viren	Ein Virus wird per Funk an das DECT-System geschickt.	Das DECT-Verfahren ermöglicht keinerlei Ausführung von Befehlsketten, Programmen oder Makros.	Kein Risiko: Es ist unmöglich, in die Prozessroutinen der DECT-Komponenten einzugreifen, da das DECT-Verfahren keine fremden Codes, Makros usw. ausführen kann.
Zugriff über Fremdgeräte	Jemand verschafft sich Zugriff zu PC-kompatibler Funkausrüstung, um damit auf ein DECT-System zuzugreifen und die Authentifizierungs- und Verschlüsselungs-Codes zu knacken.	DECT verfügt über integrierte Authentifizierungs- und Verschlüsselungsmechanismen, die einen unerlaubten Zugriff auf das Netzwerk durch Dritte unmöglich machen.	Geringes Risiko: Denn das DECT-Verfahren verfügt über integrierte Sicherheitsmechanismen. Zudem ist die nötige Ausrüstung quasi nicht erhältlich.
Stellvertreter-Angriff	Bei einem Stellvertreter-Angriff (Piggy-in-the-middle attack) gibt sich ein Gerät als Basisstation oder schnurloses Telefon aus und schaltet sich zwischen die anzugreifenden Geräte. Die Authentifizierung zwischen den angegriffenen Geräten erfolgt wie gewohnt, außer dass der gesamte Datenverkehr über den Angreifer geführt wird. Auf diese Art und Weise erhält der Angreifer die für den Verbindungsaufbau erforderlichen Informationen.	Die beste Möglichkeit, sich vor dieser Art von Angriffen zu schützen, bietet eine Verschlüsselung, die durch einen Dritten nicht deaktiviert oder aktiviert werden kann.	Geringes Risiko: Dies ist ein theoretisches Risiko. Ein entsprechender Angriff ist bislang nicht bekannt geworden.
Kostenlose Anrufe	Ein Dritter bildet das Pairing zwischen schnurlosem Telefon und DECT-Basisstation nach und kann so kostenlos telefonieren.	Pairing-Routinen bieten ein hohes Maß an Sicherheit.	Geringes Risiko: Es ist sehr unwahrscheinlich, dass ein Dritter unbemerkt in die Räumlichkeiten eines Unternehmens eindringt, Zugriff auf das DECT-System erhält und das Pairing eines schnurlosen Telefons nachbilden kann. Zudem müsste er anschließend in der Nähe bleiben, um kostenlos telefonieren zu können.
VoIP	Jemand erhält über ein DECT-Gerät, das VoIP unterstützt, Zugriff auf ein LAN.	Die DECT-Funkverbindung ist sehr sicher (siehe oben), gleich welches Netzwerk genutzt wird.	Geringes Risiko: DECT bietet unabhängig davon, welche Art von Netzwerkprotokoll im Netzwerk genutzt wird, ein hohes Maß an Sicherheit.