Karsten Nohl, Erik Tews

Kann man mit DECT noch vertraulich telefonieren?

Nachdem Sicherheitslücken im veralteten DECT-Standards bereits auf dem CCC-Kongress im Dezember 2008 erkennbar wurden, präsentierten die Autoren dieses Jahr eine Kryptoanalyse der DECT Verschlüsselung. Der Beitrag illustriert die derzeitige durch DECT verschuldete Bedrohungslage und gibt Handlungsempfehlungen zum sicheren Telefonieren.[1]

Einleitung

Schnurlose Telefone gehören seit vielen Jahren in jeden Privathaushalt und erfreuen sich auch im Businessumfeld zunehmender Beliebtheit. Aktuelle Geräte ab 20-30 Euro ermöglichen drahtloses Telefonieren im gesamten Haus in ausgezeichneter Sprachqualität und halten im Standby-Betrieb mehr als eine Woche. Seit Auslaufen der CT1+ und CT2 Zulassungen am 31.12.2008 ist Digital Enhanced Cordless Telecommunications (kurz: DECT) der Universalstandard der für schnurlose Telefone in Deutschland.

Karsten Nohl

Chief Scientist der Security Research Labs, Berlin
Schwerpunkte: Risiko-Management, Hardwareanalyse
E-Mail: nohl@srlabs.de

Erik Tews

Wissenschaftlicher Mitarbeiter an der Technischen Universität Darmstadt, Fachbereich Informatik, Fachgebiet Kryptographie und Computeralgebra Schwerpunkte: Angewandte Kryptoanalyse und Drahtlosnetzwerke
E-Mail: e_tews@cdc.informatik.tu-darmstadt.de

1 Eine aktuelle Übersicht der Erkenntnisse rund um die Sicherheit des DECT-Standards findet sich unter https://detected.org.

Andere Verfahren wie WLAN-Telefonie konnten am Erfolg von DECT bisher nicht rütteln. Insgesamt waren Ende des Jahres 2009 in Deutschland etwa 34 Milllionen Basisstationen aktiv [1]; weltweit wurden bisher mehr als 800 Millionen DECT Geräte verkauft.

DECT wird primär für Telefonie eingesetzt, ist aber auch in anderen Industrieprodukten zu finden, wie z. B. drahtlosen EC-Kartenterminals, Babyphones, Gegensprechanlagen oder auch Verkehrsleitsystemen. Beispielsweise werden in einigen ICE-Zügen der deutschen Bahn die Passagierdurchsagen über DECT zwischen den Wagen verteilt.

Der erste DECT Standard wurde 1992 von ETSI verabschiedet und ist bis heute nur um Funktionen erweitert, aber nie grunderneuert worden. Vor allem die Sicherheitsmerkmale sind in Telefonen heute die gleichen wir vor 18 Jahren. Aufgrund der sensiblen Natur der übertragenen Daten verfügt DECT über ein Authentifizierungsverfahren, das einseitige aber auch wechselseitige Authentifizierung zwischen Telefon und Basis ermöglicht – ein Merkmal, das in GSM-Netzen nicht vorhanden ist, wodurch sogenannte IMSI-Catcher möglich sind [2].

Zudem bietet DECT ein Verschlüsselungsverfahren mit 64 bit Schlüssellänge, das die Vertraulichkeit der Verbindung sichern soll. Wie damals üblich wurde bei den kryptographischen Funktionen nicht auf öffentliche, bewährte Standards zurückgegriffen, sondern es wurden Verfahren speziell für DECT neu entwickelt. Diese Verfahren sind angreifbar. In manchen DECT-Systemen sind die Verfahren sogar erst gar nicht implementiert.

1 Schwache Verschlüsselung

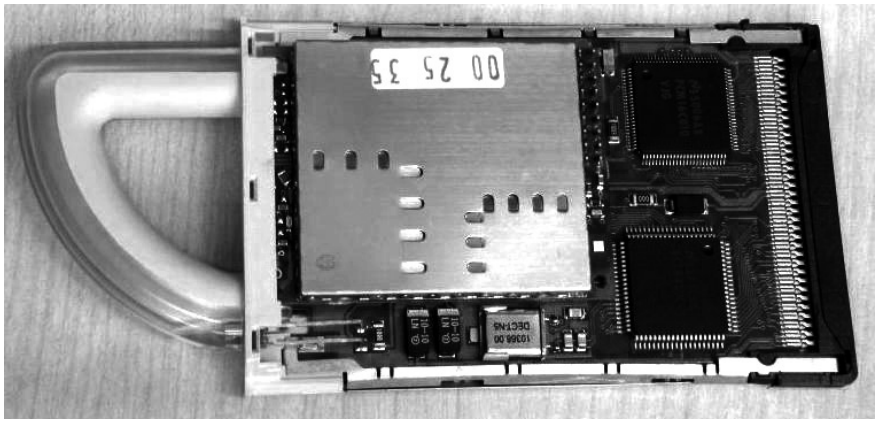
Eine selbstverständliche Sicherheitsanforderung für Telefonieanwendungen ist die Vertraulichkeit der übertragenen Daten. Anrufe zum Anwalt oder Arzt sind zum Beispiel höchst vertraulich, aber auch Gespräche mit Familie und Freunden sollen sich auf die Gesprächspartner beschränken. Selbst die Tatsache, dass eine bestimmte Rufnummer wie etwa die einer Drogen- oder Schuldnerberatung oder eines bestimmten Arztes angerufen wurde, sollte geheim bleiben.

DECT Telefone haben prinzipiell den Anspruch, Sprach- und Verbindungsdaten als vertraulich zu schützen und mittels einer Stromchiffre zu verschlüsseln. Viele DECT-Geräte implementieren diese Verschlüsselung allerdings nicht. Teils werden auch Pakete aus Basisstation und Telefon verkauft, bei denen nur das Telefon, nicht aber die Basisstation eine Verschlüsselung beherrscht. Wieder andere Telefone schalten die Verschlüsselung erst nach dem Gesprächsaufbau ein, also nach dem Senden der Telefonnummer.

In allen diesen Fällen werden Daten unverschlüsselt übertragen und können einfach abgefangen und ausgewertet werden. Seit einiger Zeit stehen Analysewerkzeuge für DECT zum freien Download im Internet [3], wodurch „DECT-Hacking“ ähnlich einfach wird wie es das Knacken von nicht oder schlecht verschlüsselten WLANs schon lange ist.

Auch bei verschlüsselten DECT-Verbindungen ist die Vertraulichkeit keinesfalls garantiert. Die Stromchiffre DSC (DECT Standard Cipher) verwendet einen geheimen Schlüssel von lediglich 64 bit Länge. Solche Schlüssellängen kön-

Abb. 1 | DECT-PCMCIA-Karte (geöffnet)



nen heute nicht mehr als sicher angesehen werden, da eine Suche über alle Schlüssel mit heute verfügbarer Hardware möglich ist. Zusätzlich besitzt die Chiffre kryptographische Schwächen, die es erlauben, den Schlüssel auf einem einfachen PC in wenigen Minuten bis Stunden zu bestimmen. Der aktuelle Stand der Angriffe ermöglicht diese beschleunigten Angriffe allerdings nur gegen lange Gespräche von mehreren Stunden Länge [4].

3 Fehlende Authentizität

Als weiteres kryptographisches Versäumnis verlangen die meisten Telefone keine Authentifizierung der Basisstation, so dass ein aktiver Angreifer sich selbst als Basisstation ausgeben und die Verschlüsselung abschalten kann. Da bei DECT – ähnlich wie in GSM-Netzen, wo ein solcher Angriff als „IMSI-Catcher" bezeichnet wird – die Basisstation über die Sicherheitsstufe des Telefons entscheidet, kann ein aktiver Angreifer über das Emulieren einer Basisstation oft jegliche Sicherheitsvorkehrungen umgehen.

Über das reine Aufzeichnen von Gesprächsinhalten hinaus kann eine emulierte Basisstation auch aktiv in das Geschehen eingreifen und zum Beispiel Gespräche zu anderen Nummern umleiten. Viele Telefone bieten die Möglichkeit, die Nummer des Anrufenden auf dem Display anzuzeigen. Kontrolliert der Angreifer die Basisstation, so kann er ebenfalls diesen Displayinhalt frei wählen. Ein Angreifer könnte dies Ausnutzen, um unter falscher Identität anzurufen.

Die fehlende Authentizität der Verbindung kann auch in die andere Richtung zum Problem werden. Dann nämlich, wenn ein Betrüger sich gegenüber einer Basisstation als ein angemeldetes Telefon ausgibt und zum Beispiel teure Sonderrufnummern anruft. Ebenso könnte ein Angreifer unter falscher Identität Gespräche führen. In Fällen, in denen die Telefonnummer als Zugangsberechtigung benutzt wird, z. B. bei internen Support-Hotlines, die Windows-Passwörter zurücksetzen, kann dies zum Sicherheitsproblem werden.

Selbst bei DECT-Geräten, die eine Authentifizierung verlangen, ist diese oft schwach umgesetzt. Der DECT Standard Authentication Algorithm (DSAA) verwendet zwar geheime Session-Schlüssel von einer Länge von 128 bit [5]. Diese Schlüssel werden aber beim Initial-Pairing von Telefon und Basisstation nur aus der PIN (fast immer: 0000) und einer 64 bit langen Zufallszahl generiert. Basisstationen verwenden für diesen Schritt oft erschreckend schlechte Zufallszahlengeneratoren, welche z. B. nur 2^{22} mögliche Zahlen generieren können, also weniger als ein Billionstel der möglichen Zufallszahlen. Bei bekannter PIN (0000) sind damit nur 2^{22} verschiedene Schlüssel möglich, die ein Angreifen in weniger als einer Sekunde durchprobieren kann. Hat er den korrekten Schlüssel gefunden, kann er sich selbst bei aktiver Authentifizierung immer als Telefon oder Basisstation ausgeben und die oben genannten Angriffe durchführen.

4 Angriffe einfach durchführbar

Alle hier erwähnten Angriffe sind inzwischen ohne größeren Aufwand umzusetzen. An Hardware wird nur ein PC oder

Laptop mit einer DECT PCI- oder PCMCIA-Karte benötigt. Als Betriebssystem bietet sich Linux an. Das Repository unter http://deDECTed.org/ bietet Tools zum passiven Mitschneiden von DECT-Gesprächen. Zudem ist ein DECT Kernel Stack verfügbar, der die Emulation von DECT-Basisstationen-Handsets unter Linux ermöglicht [3].

Kryptographische Angriffe auf anfällige Zufahlszahlengeneratoren oder DSC können bereits auf einem aktuellen PC oder Notebook ausgeführt werden. Hochleistungsrechner oder Spezialhardware wie Grafikkarten oder FPGAs bieten zusätzliche Geschwindigkeitsvorteile. Open Source Implementierungen der in DECT verwendeten kryptographischen Verfahren sind auf http://deDECTed.org/ zu finden.

5 Gegenmaßnamen

Viele der angesprochenen Probleme liegen nicht im DECT-Standard selber, sondern in der unvollständigen Implementierung und Erzwingung aller Sicherheitsfeatures begründet. Dabei muss oft eine Abwägung zwischen Kompatibilität und Sicherheit erfolgen. Würde ein Telefon z. B. immer die Verschlüsselung von Gesprächen erzwingen, wäre es nicht in der Lage, mit Basisstationen zusammen zu arbeiten, die eine Verschlüsselung nicht unterstützen. Nur selten sind Anwender in der Lage, die Sicherheitseinstellungen ihres Telefons einzusehen oder zu verändern.

Viele dieser Probleme können durch Änderungen in der Firmware der Basisstationen oder Telefone behoben werden. Leider sehen nur wenige Telefone oder Basisstationen die Möglichkeit vor, dass ein Anwender dort die Firmware austauschen kann. Es gibt allerdings auch Telefone auf dem Consumer-Markt wo dies mit wenigen Tastendrücken möglich ist, und die vom Hersteller auch aktiv mit Firmwareupdates versorgt werden.

Strukturelle Schwachstellen wie z. B. die Schlüssellänge und die Angreifbarkeit von DSC werden erst mit einer neuen Version von DECT behoben sein. An dieser wird zur Zeit aktiv entwickelt, so dass bald mit besseren Verschlüsslungs- und Authentifizierungsverfahren für DECT zu rechnen ist. Da DSC meist in Hardware und nicht in der Firmware implementiert ist, werden wohl nur die wenigsten Telefone durch ein Firmware-Update auf die neuen Algorithmen umrüstbar sein. Alte Hardware muss daher vollständig gegen neue getauscht werden.

6 Angriffe über DECT hinaus

Alle hier gezeigten Schwachstellen von DECT sollen nicht davon ablenken, dass es noch viele weitere Möglichkeiten gibt, Telefongespräche abzuhören. Telefonanschlüsse im Keller von Mehrfamilienhäusern sind oft nur gering gesichert und können mit einfachsten Mitteln wie einem analogen Telefon angezapft werden. Wird anstelle eines alten analogen Telefonanschlusses VoIP verwendet, können Telefongespräche mit den gleichen Mitteln wie auch andere Datenübertragungen im Internet abgehört werden. Auch gibt es auf der Seite des Telekommunikationsanbieters meist Abhörschnittstellen für staatliche Stellen.

Die Weiterentwicklung der Telefonie bietet sogleich aber auch die Chance, sicheres Telefonieren massentauglich zu machen. Mobiltelefone, die Ende zu Ende Verschlüsselung anboten, mussten meist eine Modemverbindung (CSD) zur Gegenstelle aufbauen. CSD-Verbindungen arbeiten leider nur mit einer Geschwindigkeit von 9600 bit/s, was für eine gute Sprachqualität nicht ausreicht. Spezialhardware zur Verschlüsselung von analogen Telefongesprächen ist ebenfalls auf dem Markt erhältlich, hier wird meist auch eine Modemverbindung zur Gegenseite aufgebaut.

Moderne Smartphones verfügen über eine schnelle Internetverbindung (UMTS/HSPA) und ausreichend Rechenleistung, um Schlüssel auszutauschen und ein Telefongespräch in Echtzeit zu verschlüsseln. Auch Festnetztelefone werden vermehrt über Datennetze angebunden. In den gängigen VoIP Protokollen wie SIP/RTP sind bereits Krypto-Erweiterungen vorgesehen, so dass Gesprächsinhalte verschlüsselt übertragen werden können.

Dem gleichen Trend folgend können auch neue DECT-Basisstationen direkt über Datennetze anstelle eines analogen Telefonkabels angeschlossen werden.Die kommende Generation von DECT-Geräten in Kombination mit verschlüsselter Internettelefonie wird also ein wesentlich höheres Schutzniveau bieten als aktuelle Telefone und analoge Telefonanschlüsse.

Conclusio

Moderne Technik verlangt von uns, ihr unsere privaten Daten anzuvertrauen. Im Falle von DECT-Telefonen, die auf alter Sicherheitstechnik basieren und selbst diese nicht zwingend verlangen, ist dieses Vertrauen nicht gerechtfertigt. Mit kürzlich veröffentlichen Tools ist das Mitlauschen von Nachbars Telefongesprächen in die Reichweite von "Skript-Kiddies" gerückt.

Sensible Gespräche im Sinne des Datenschutzes sollten nicht über DECT geführt werden, sofern die Sicherheitsmaßnahmen der verwendeten Telefone und Basisstationen nicht zweifelsfrei nachgewiesen sind. Ein solcher Nachweis wird erst durch die geplante Zertifizierung von DECT-Telefonen praktisch umsetzbar, und sollte auch dann möglichst nur solche Telefone umfassen, die nach dem bald verfügbaren DECT2-Standard verschlüsseln. Bis dahin gehört DECT (wie bereits GSM) zu den datenschutzrechtlich kritischen Technologien.

Referenzen

[1] Alexandra Mengele: Security of Digital Enhanced Cordless Telecommunication (DECT) devices for residential use, Diplomarbeit.

[2] Fox, Dirk: Der IMSI-Catcher. Datenschutz und Datensicherheit (DuD), 4/2002, S. 212-215.

[3] Patrick McHardy, http://dect.osmocom.org/

[4] Karsten Nohl, Erik Tews, und Ralf-Philipp Weinmann. Cryptanalysis of the DECT Standard Cipher. Fast Software Encryption, Seoul, Korea, Februar 2010.

[5] Stefan Lucks, Andreas Schuler, Erik Tews, Ralf-Philipp Weinmann, Matthias Wenzel: Attacks on the DECT authentication mechanisms, CT-RSA 2009.