Phreaking im 21. Jahrhundert



Ein Guide von

7SAC7

Stand: 794-18.10.06

Phreaking im 21. Jahrhundert
Ein Guide von 7SAC7

© by 7SAC7, Deutschland 2006

Dieses Dokument besitzt eine GNU-Lizenz. Der Gebrauch und die unentgeltliche Weitergabe zu privaten Zwecken sind der Allgemeinheit erlaubt. Die Veränderung des Wortlautes hingegen ist dem Autor vorbehalten. Ergänzungen und Veränderungen durch Dritte müssen bei der Weitergabe entsprechend gekennzeichnet werden.

Warnhinweis!

Diese Publikation dient einzig und allein Anschauungs- und Schulungszwecken. Die hier beschrieben Vorgehensweisen sind gesetzeswidrig im Sinne des Strafgesetzbuches (StGB) und des Fernmeldegesetzes. Die Umsetzung der beschrieben Sachverhalte kann zu zivil- und strafrechtlichen Verfolgung und Ahnung führen.
Es wird hiermit darauf hingewiesen, dass der Autor keines Falls zum Ausprobieren und Durchführen anstiftet. Die vernünftige Umgang mit dem erworbenen Wissen obliegt einzig und allein dem Leser. Alle Angaben sind ohne Gewähr.

Der Autor

Inhaltsverzeichnis

Vorwort
- Das Hacker-Manifest

Mitgehört und aufgeschaltet
- Angriffspunkte
  - Gebäude
  - ÜVt
  - HVt
  - KVz
  - EVz
- Angriffsarten
- Werkzeuge
- Adernfarben
- Analoge Anschlüsse
- Erweiterung der TAE2Go
- ISDN-/DSL-Anschlüsse
  - Uk_0
  - S_0
  - Leistungsmerkmale
  - DSL

Exkurs: Die Starterbox

PUMA und anderes Viehzeug
- SEPT
- ERNA und andere Schlampen

Virtuelle Anrufbeantworter

DTMF und andere Flötentöne
- DTMF
  - Anrufbeantworter
  - Tastensperren
- Blueboxing

DECT, GAP und die große Freiheit

Gezinkte Karten
- Calling Cards

Mathe-Exkurs: Bruteforce

Telefonzellen und andere Hexenhäuschen
- Definitiv kostenlose Gespräche
- Anrufen von T-Zellen
- R-Gespräche in T-Zellen annehmen
- Aus einer Telefonzelle umsonst Telefonieren

Basteleien
AWADo/AMS
ISDN-Tester

Normaltariflines (Party Lines)
Youth International Party Line

Telefonterror
Telefon-Terror Tutorial by outsiderz

Nummergassen in Deutschland

Colorboxen

Mythen, Horaxes, Unfug

Hotlines
Telefongesellschaften, Auskünfte, R-Gespräche

Abkürzungen

Links



Vorwort

Die Hochzeit des Phreaking war in den 1980er Jahren als das Telefonnetz noch auf analogen, nur teilweise digitalisierten Vermittlungsstellen beruhte. Damals wurde auch das Internet populär. Über ihren Heimcomputer und dem Modem konnten sich interessiere Jungforscher in die Phreaking-Mailboxen in aller Welt einwählen.

Heute, zu Beginn des 21. Jahrhunderts, ist das Telefonnetz vollständig digitalisiert.
Die Literatur, die man im nun Hochglanz-WWW findet, ist aber oftmals die von vor 20 Jahren.
Was darin beschrieben steht kann nicht mehr funktionieren. Und das obwohl viele Teile des deutschen Telefonnetzes bereits 50 Jahre alt sind…

Es wird also Zeit, erneut zusammen zufassen, was Stand der Technik ist und das diese moderne Technik an Schwachstellen hat.

Dabei möchte ich zunächst auf reine CONS-Netze beschränken, also die klassische Telefonie und DFÜ.
Die mittlerweile genauso weit verbreiteten CLNS-Netze (z.B. IP-Netze) bieten genauso viel, wenn nicht noch mehr, Angriffsfläche. Allerdings hat bei ihnen nicht allzu viel zum anfassen. Phreaking sollte nicht nur was für Script-Kiddies sein, sondern vielmehr was für den interessierten Bastler.

Das Hacker-Manifest

[…]
Dies ist unsere Welt... die Welt des Elektrons und des Switches, der Schönheit des Baud. Wir machen gebührenfrei von einem bereits existierenden Service gebrauch, der kaum was kosten würde, wenn er nicht von unersättlichen Profiteuren betrieben würde... und ihr nennt uns Kriminelle.
Wir streben nach Wissen... und ihr nennt uns Kriminelle.
Wir existieren ohne Hautfarbe, ohne Nationalität, ohne religiöse Vorurteile... und ihr nennt uns Kriminelle. Ihr baut Atombomben, ihr führt Kriege, ihr mordet, ihr belügt und betrügt uns und versucht uns einzureden, dass es nur für unser eigenes Wohlergehen sei.
Ja, ich bin ein Krimineller. Mein Verbrechen ist das der Neugierde.
Mein Verbrechen ist es, die Leute nach dem zu beurteilen, was sie sagen und denken, und nicht danach, wie sie aussehen. Mein Verbrechen ist, dass ich euch austrickse, etwas, was ihr mir nie vergeben werdet.
Ich bin ein Hacker, und dies ist mein Manifest. Ihr könnt dieses Individuum aufhalten, aber ihr könnt uns niemals alle stoppen...

by ‚The Mentor'

übersetzt aus dem Englischen von 7SAC7

Mitgehört und aufgeschaltet

Das Bestreben beim Phreaking ist es, unauthorizierten Einfluss auf ein Telekommunikationssystem zu nehmen. Meistens mit dem Ziel kostenlos (gebührenpflichtige) Dienste in Anspruch zu nehmen und/oder Informationen zu erlangen, die nicht für den Phreaker bestimmt sind.
Um es mal ganz einfach zu sagen, der Phreaker will umsonst telefonieren/surfen oder die Gespräche anderer Abhören.
Und darum geht es in den ersten Lektionen auch.

Da heute alles über Computer läuft und auch das Vermittlungssystem der Telefongesellschaft nur ein großer Computer ist, kann man natürlich das System von innen heraus manipulieren. Für die Servicemitarbeiter ist das ihr tägliches Brot für den Phreaker eine verborgene Welt.
Einfach als auf ein Computerprogramm kann man natürlich Einfluss auf alles nehmen, was sich auch anfassen lässt. Daher fangen wir mit den physikalischen Angriffen auf eine Telefonleitung an. Und damit ist nicht das durchtrennen mit dem Seitenschneider gemeint ;-)

Seit den Anfängen der klassischen Telefonie haben Kunde und Servicetechniker was zum anfassen. Der Kunde das Telefon, die Anschlussschnur und die Telefondose. Der Servicetechniker zusätzlich noch die Strippen, die zum Teilnehmer führen.
Denn daran hat sich seit 100 Jahren nichts geändert: Für die Übertragung der Gespräche zwischen Teilnehmer und Vermittlungsstelle werden Kupferleitungen verwendet. Diese sind mal gut unter der Erde und mal wenige gut überirdisch versteckt.

Da also ein Gespräch in den meisten Fällen (Mobilfunk und z.T. VoIP einmal ausgeschlossen) über ebenso eine Leitung geführt wird, bietet sie die beste Angriffsfläche fürs Phreaking. Schaltet man sich richtig auf die Leitung auf, kann man dort drüber geführte Gespräche abhören, eigene Gespräche über fremde Leitungen führen oder die Leitung ganz zerstören.

Natürlich ist klar, dass an der Telefonleitung nicht jeder Hinz und Kunz rumbasteln darf. Der Otto-Normal-Laie darf höchstens zwischen Telefondose und Telefon rumbasteln.
Aber auch nicht jeder Otto weiß woher die Drähte aus der Telefondose herkommen. Und das schauen wir uns jetzt erstmal an…

Angriffspunkte

Wie erwähnt ist unser Angriffsziel eine Kupferleitung, die so genannte TAL (Teilnehmer-Anschluss-Leitung). Das ist ein Adernpaar, eine s.g. Doppelader (DA), die von der zentralen Technik der Telefongesellschaft zur Telefondose des Kunden führt.
Klar sein sollte, dass es sich dabei nicht um eine durchgängige DA handelt. Wenn jemand an der einen Seite zieht, fällt auf der anderen Seite garantiert nicht Euch der Telefonapparat vom Tisch.
Vielmehr ist die Leitung auf dem Weg zwischen Amt und Teilnehmer an mehreren Punkten aufgetrennt und verschaltet. Die durchgängig geschaltete Leitung bezeichnet man als Ortnetzanschlussline.
Diese Verteil- und Verzweigungspunkte liegen allesamt im Wirkungsbereich der Telefongesellschaft. In Deutschland zu fasst 99% der Deutschen Telekom AG, auch wenn der Teilnehmer Arcor-Kunde ist o.ä.
Die Technik die dahinter steckt bezeichnet man als Linientechnik. Die ist definitiv nicht öffentlich!

Gebäude
Aber wir wollen uns mal ansehen, was hinter den verborgenen Türen steckt.
Fangen wir dabei hintern den Türen der Fernmeldeämter an. Diese werden seit Zeiten der Deutschen Reichspost betrieben. Bevor der rosa Riese, die Deutesche Telekom AKTIEN-GESELLSCHAFT, auf den Markt kam, war die Post eine Behörde. Daher wurden die Gebäude als Ämter bezeichnet, insbesondere da früher dort auch Beamte (ständig) gearbeitet haben.
Heutzutage ist die Telekommunikationstechnik nicht mehr so wartungsintensiv und die ständige Überwachung durch Postmitarbeiter entfällt. Also stehen in den „Ämtern" Anlagen, die – zum größten Teil unbeaufsichtigt – ihren Dienst tun. Hin und wieder kommen mal Servicetechniker vorbei um nach den Rechten zu sehen, die Anlagen zu reparieren, Schaltungen vorzunehmen oder Anschlüsse zu prüfen.

Verwaltet werden die Gebäude übrigens von der DeTeImmo (Hotline 0800-3304040).
Einbruch ist zwecklos, die Gebäude sind alarmgesichert. Für viele Gebäude braucht man eine Zutrittskarte. Wenn die jemand verliert wird die einfach von der DeTeImmo gesperrt.
Hofeinfahrten stehen entgegen den Dienstanweisungen oftmals offen, aber wenn auf dem Hof DTAG-Fahrzeuge parken, Türen oder Fenster offen stehen und irgendwo Licht brennt ist das Gebäude sicherlich gerade bewohnt.

Kollokation

Fast jede Telefongesellschaft (engl. Carrier) hat ihre eigenen Vermittlungssysteme (z.B. EWSD von Siemens oder S-12 von Alcatel). Diese stehen auch in den Gebäuden der ehemaligen Deutschen Bundespost, die ihren ganzen alten Plunder damals der Telekom geschenkt hat. Und weil die Post ja eine Behörde war, hat sie den Krempel von unseren Steuergeldern gekauft. Damit die Telekom-Konkurrenten deswegen keinen Nachteil haben, muss die Telekom ihnen die Räumlichkeiten untervermieten.

Und das ist alles höchst sinnvoll, weil von Amt ja eine Leitung zu jedem Teilnehmer im Umkreis führt. Der Bereich, den ein Fernmeldeamt mit Anschlüssen versorgt, nennt sich Anschlussbereich (AsB). Jeder AsB hat eben so ein Amtsgebäude. Die Gebäude sind je nach Bauweise eher unauffällig oder total auffällig weil ein Sendemast daneben steht oder ein großes *T*** drauf prangert.

Gehen wir jetzt mal davon aus, die Leitung die wir verfolgen ist eine Arcor-Leitung.
Das Arcor-eigene Vermittlungs-Equipment (EWSD bzw. die abgesetzen DLUs) stehen in einem Kollokationsraum oder auf einer Kollokationsfläche. Für beides zahlt die Fremdgesellschaft Miete an die Telekom.

Dort steht also der Vermittlungscomputer an dessen Rückseite die Teilnehmerports (analog oder ISDN) rauspurzeln. Die Ports sind winzige Pin-Paare auf die ein Systemstecker auf gesteckt wird. Das daran angeschlossene Systemkabel wird auf dem ÜVt aufgelegt

ÜVt

ÜVt bedeutet Übergabeverteiler. Ein ÜVt besitzt mehrer Buchte, Endverschlüsse (EVS) genannt. Ein EVS wiederum besteht aus mehreren Trennleisten. Auf eine Trennleiste können 8 oder 10 DA aufgelegt werden.

Auf einem Teil der EVSe sind die Systemkabel aufgelegt. Das hat natürlich den Vorteil, dass die Servicetechniker nicht an den winzigen PINs der Anlage rumfummeln müssen. Da könnte man sehr leicht extrem teure Hardware beschädigen oder sich schlichtweg verzählen. Auf einem Teil der EVS-Leisten liegen also die Teilnehmerports, auf den anderen Leisten sind DA in Richtung DTAG abgelegt. Jede der dort abgelegten DAs führt vom ÜVt zum HVt. Da der HVt in der alleinigen Hoheit der DTAG liegt, findet hier eine Übergabe vom Arcor-Netz ins Liniennetz der Telekom statt. Daher auch Übergabeverteiler.
Zwischen den Arcor-Ports und den DTAG-Ports wird bei Bedarf eine Rangierung mit Schaltdraht einlegt.

Wie die jeweilige Telefongesellschaft die Teilnehmer-Ports auf ihrer Seite des ÜVts ablegt ist allein ihre Sache und sehr unterschiedlich.
Nur die Belegung der Telekom-Seite ist immer dieselbe.
Angeben wird in entsprechenden Formularen eine eindeutige Bezeichnung der DTAG-DA.

Beispiel:
Die Angabe lautet ÜVt0102-DUASB55-04-32.
Dann heißt das:
Suche im ÜVt 0102. Der steht in Duisburg im AsB-Gebäude 55 (Stadtteil Wedau). Die 01 bezeichnet die 1. fremde Telefongesellschaft (neben der DTAG) im Gebäude. Also suche in deren Kollolaktionsbereich. Ein Carrier kann mehrere bereiche mit mehren ÜVts haben. 02 ist der 2. ÜVts des 1. Carriers.
Der gesuchte Port befindet sich dann im ÜVt 0102 im 4. EVS auf Stift. Ein EVS umfasst 10 Leisten, gezählt werden die EVS von oben links. Wenn eine Lücke muss mitgezählt werden.
Im EVS liegt der gesuchte Port auf der 32. Doppelader. Gezählt wird vom ersten Port auf der erste Leiste des jeweiligen EVS.

Wichtig ist, dass man sich hier natürlich auch nicht verzählt.

Was kann man am ÜVt machen? Der Servicetechniker kann natürlich messen und prüfen (mehr dazu später), der Phreaker-Strolch kann sich aber ebenso auf Leitungen aufschalten oder diese sabotieren.
Aber das fällt i.d.R. sehr schnell auf, weil bei Störungen als erstes am ÜVt geprüft wird. Veränderungen werden dann korrigiert und Eure Mühe war dann meistens umsonst.
Mal von der Gefahr einer Anzeige wegen Einbruch oder Hausfriedensbruch einmal abgesehen, wenn ihr erwischt werdet.

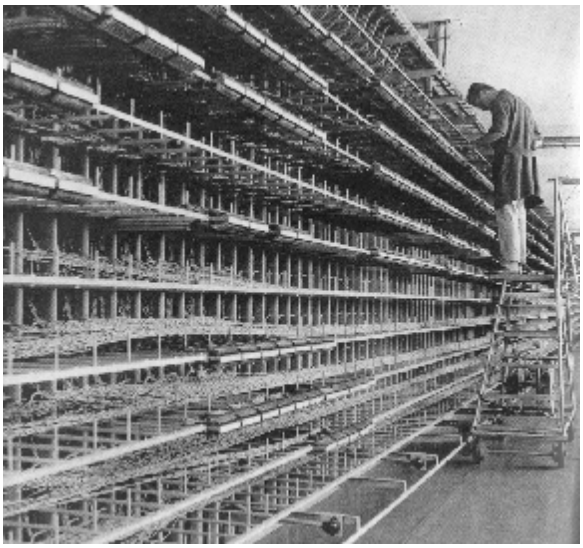
HVt

Der Name Hauptverteiler (HVt) sagt schon alles. Hier kommen nicht nur die Leitungen von den ÜVts an, sondern auch die Leitungen der Telekom-eigenen Anlagen. Das Prinzip ist aber bei allen das gleiche, im Übrigen auch bei privaten HVts im Zusammenhang mit einer Telefonanlage. Nur das bei privaten HVts (z.B. bei Behörden, Krankhäusern oder großen Unternehmen) die Leitungen direkt durch das Haus zu den Telefondosen führen.

Ein HVt hat zwei Seiten. Eine mit horizontalen Reihen und eine mit vertikalen Buchten. Alle Leitungen, die von einer Vermittlungsanlage kommen, sind auf der horizontalen Seite aufgelegt.
Auf den Stiften der vertikalen Seite sind die TALs aufgelegt, also die Leitungen die zum Kunden gehen.
Dazwischen wird ebenfalls bei Bedarf eine Rangierung vorgenommen. Diese wird von einen DTAG-Mitarbeiter oder einem Subunternehmer im Auftrage der DTAG eingelegt. Fehler können hier schon mal passieren, z.B. das ein Stift vertauscht wird. Da telefoniert im schlimmsten Fall jemand über einen falschen Port also auf fremde Kosten und ist unter seiner Nummer erreichbar.

Das kann man natürlich gewollt herbeiführen wenn man die entsprechenden Stiftangaben hat. Diese Angaben heißen bei der DTAG übrigens ORKA-Daten.
Fehler bzw. Manipulationen fallen auch hier schnell auf, weil im Störungsfall auch hier zuerst geprüft wird.
Außerdem trennt die DTAG gekündigte Leitungen hier auf. Sofern die TAL nicht auch woanders unterbrochen ist, reicht u.U. das wiederherstellen der Rangierung. Allerdings wird in den meisten Fällen auch der Port auf der Vermittlungsstelle in der Software deaktiviert.



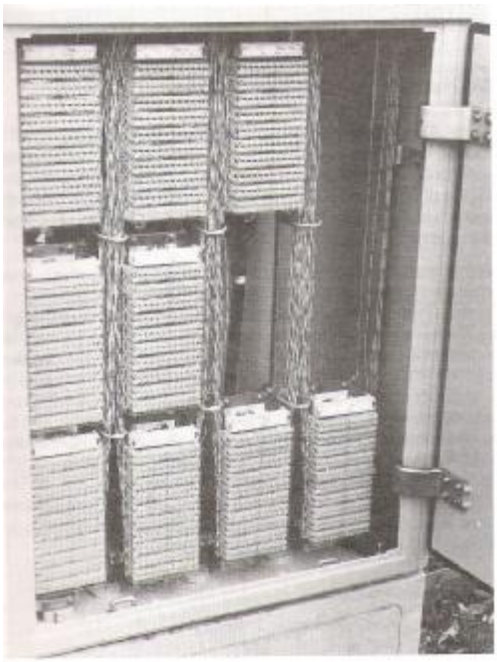


KVz

Von der vertikalen Seite des HVts kriecht die DA durch den Kabelaufteilungsraum im Keller endlich ins Freie.
Aber sie darf sich nicht direkt zum Endkunden schlängeln.
Nur wenige Teilnehmer, die in direkter Nachbarschaft zum HVt-Gebäude wohnen sind direkt an den HVt angeschlossen.
Jedes Gebäude im Anschlussbereich direkt anzubinden würde ein gewaltiges Kabelchaos im Erdboden verursachen.
Deshalb wird alles in vernünftige Bahnen gelenkt. Von HVt gehen Kabelstränge in verschiedene Himmelsrichtungen weg.
Diese Kabel heißen Hauptkabel (HK). Oftmals laufen sie entlang vorhandener Fahrstraßen.





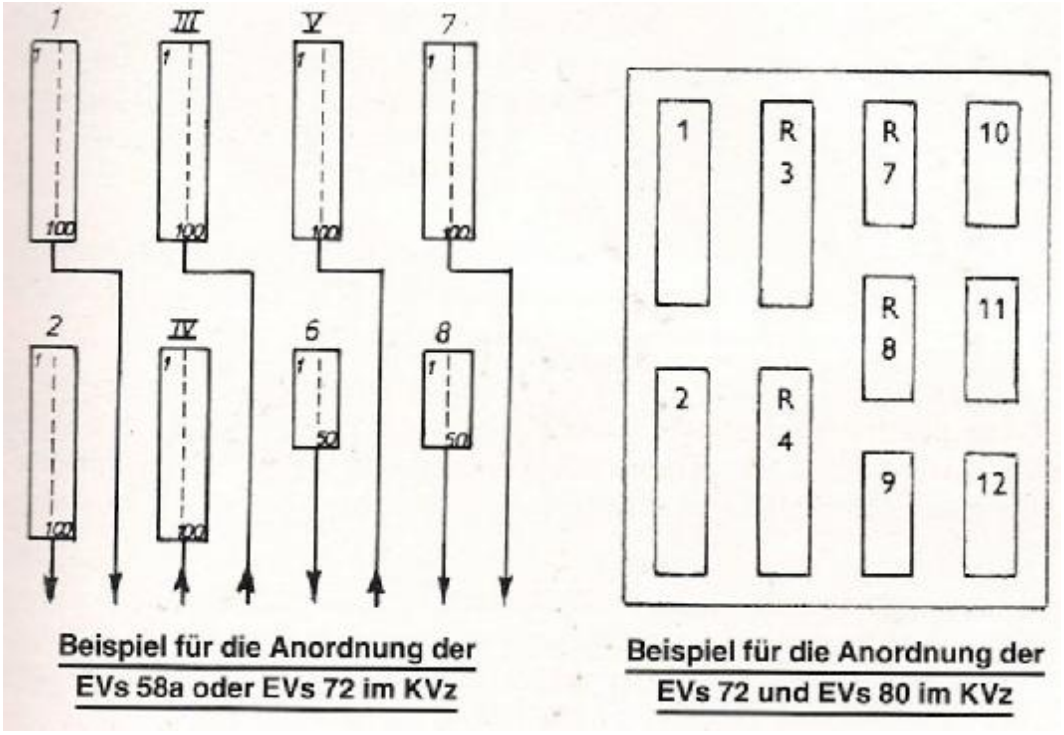


Am Straßenrand, an Kreuzungen oder vor Gebäuden stehen fast immer unbeachtet und oft verunziert die Kabelverzweiger (KVz) der DTAG. Es gibt verschieden Gehäusemodelle und Schlösser.

Die Funktion ist aber einheitlich: Der KVz trennt das HK auf und zwackt sich einige der Doppeladern ab. Nicht alle, denn die anderen Doppeladern führen weiter zum nächsten KVz. Die KVz sind wie Perlen auf dem HK aufgereiht.
Für den richtigen Standort gibt es bei der DTAG geheime Listen.

Jeder KVz hat eine Bezeichnung z.B. 55A34.
Das bedeutet: Der 34. KVz am Hauptkabel A im AsB 55.

Die DAs, die am KVz abgegriffen werden, sind wie beim ÜVt auf Leisten aufgelegt, die in EVSe gruppiert sind.
Auf einem Teil der EVSe sind also die Adern, die vom Amt kommen. Auf den anderen EVSen sind Verzweigerkabel (VzK) aufgelegt, deren Adern führen zu den Gebäuden in denen die Telefonanschlüssen sind.
Im KVVz sind die EVS für das HK mit römischen Ziffern und die EVS für die VzK mit arabischen Ziffern näher gekennzeichnet.
In elektronischen Darstellungen wird statt I, II, III, IV, V, VI,… ein R vor die entsprechende arabische Ziffer gesetzt: R1 = I, R2 = II, R4 = IV, usw.



Ein Schaltpunkt wird mit 07-08-05 angegeben. Das bedeutete EVS 07 – Leiste 08 – Stift 05.
Zwischen den EVSen wird wieder rangiert, es kann geprüft und gemessen werden. Achja, und all das andere illegale Zeug.
Dazu muss man sich natürlich einen passenden Schlüssel organisieren, die von Telekom-Niederlassung zu Niederlassung UNTERSCHIEDLICH sind, oder den Kasten aufbrechen.

Für einen verlorenen Schlüssel haftet ein DTAG-Mitarbeiter bzw. ein Subunternehmer mit je 1.000,- Euro.
Und fürs Aufbrechen habt Ihr mindestens ne’ Anzeige wegen Sachbeschädigung am Hals.

EVz

Kommen wir nun zu dem Punkt, der für jeden Phreaker interessant ist. Er ist einfach zu finden und weniger risikoreich zu öffnen.
Vom KVz führt das VzK weg, dessen Adern (meist noch durch eine Erdmuffe abgegriffen) zum letzten wichtigen Verteiler gehen. Der letzte Verzweiger zwischen Amt und Kunde ist der Endverzweiger (EVz). Auf Grund seiner finalen Position im Liniennetz auch "Abschlusspunkt des Allgemeinen Liniennetz" (APL) genannt.

Auffinden

Jedes Gebäude in dem ein Telefonanschluss vorhanden ist, hat einen oder mehrere APLs. Diese Verzweigerkästen befinden sind dort wo das Verzweigerkabel von der Straße ins Haus gelangt. Meistens befindet sich der APL also im Keller oder an einer der Außenwände.



Es gibt eine Vielzahl an EVz-Modellen. Je nach Anforderung und Epoche wurden unterschiedliche Typen verbaut.
Aber auf fast jedem Modell stehen die Worte POST, Bundespost, BP, TELEKOM oder Deutsche Telekom. Außerdem haben die meisten ein Schloss oder gar eine Plombe. (Es gibt natürlich immermal wieder Ausnahmen ohne Schloss oder mit der Aufschrift Reichspost).



Rechtliches

Hier wird schon sichtbar, was das rechtlich Besondere an einem APL ist. Die meisten wurden von der Deutschen Bundespost (DBP) montiert.
Die Bundespost war eine Behörde mit hoheitlichen Aufgaben und dieser APL erfüllte damit genauso hoheitliche Aufgaben wie ein Polizeiwagen. Das Betreiben eines Fernsprechnetzes war eine Behördenaufgabe. Die Bundespost hatte nicht nur ein Monopol sonder auch als einzige das Recht dazu. Das Recht und die Pflicht der deutschen Bevölkerung ein funktionsfähiges Telefonnetz bereitzustellen.
Um den sicheren Betrieb dieses wichtigen Netzes zu gewährleisten durften nur von Amts wegen bestellte Personen an diesem Netz arbeiten. Ein DBP Fernmelder war also nicht nur ausgebildet sondern auch meist Beamter.
Allen anderen Personenkreisen war das Arbeiten am Fernmeldenetz untersagt.

Um dies zu gewährleisten und zu kontrollieren besitzen die EVz also Schlösser und amtliche Plomben. Auch heutzutage noch, wo das Netz einem Privatunternehmen gehört. Denn die Telekom ist immer noch von Gesetzes wegen zum reibungslosen Betrieb eines Fernsprechnetzes verpflichtet und außerdem sind die Leitungen ihr Kapital.
Das unbefugte Öffnen eines EVz ist immer noch als Sachbeschädigung oder Eingriff in das Fernmeldenetz strafbar.

An einem privaten Netz darf jeder Fachmann und jeder Laie rumpfuschen, Die Liberalisierung des Telefonmarktes endet aber an der 1.TAE. Jenseits dieser Dose dürfen nur Telekommitarbeiter oder -beauftrage arbeiten.

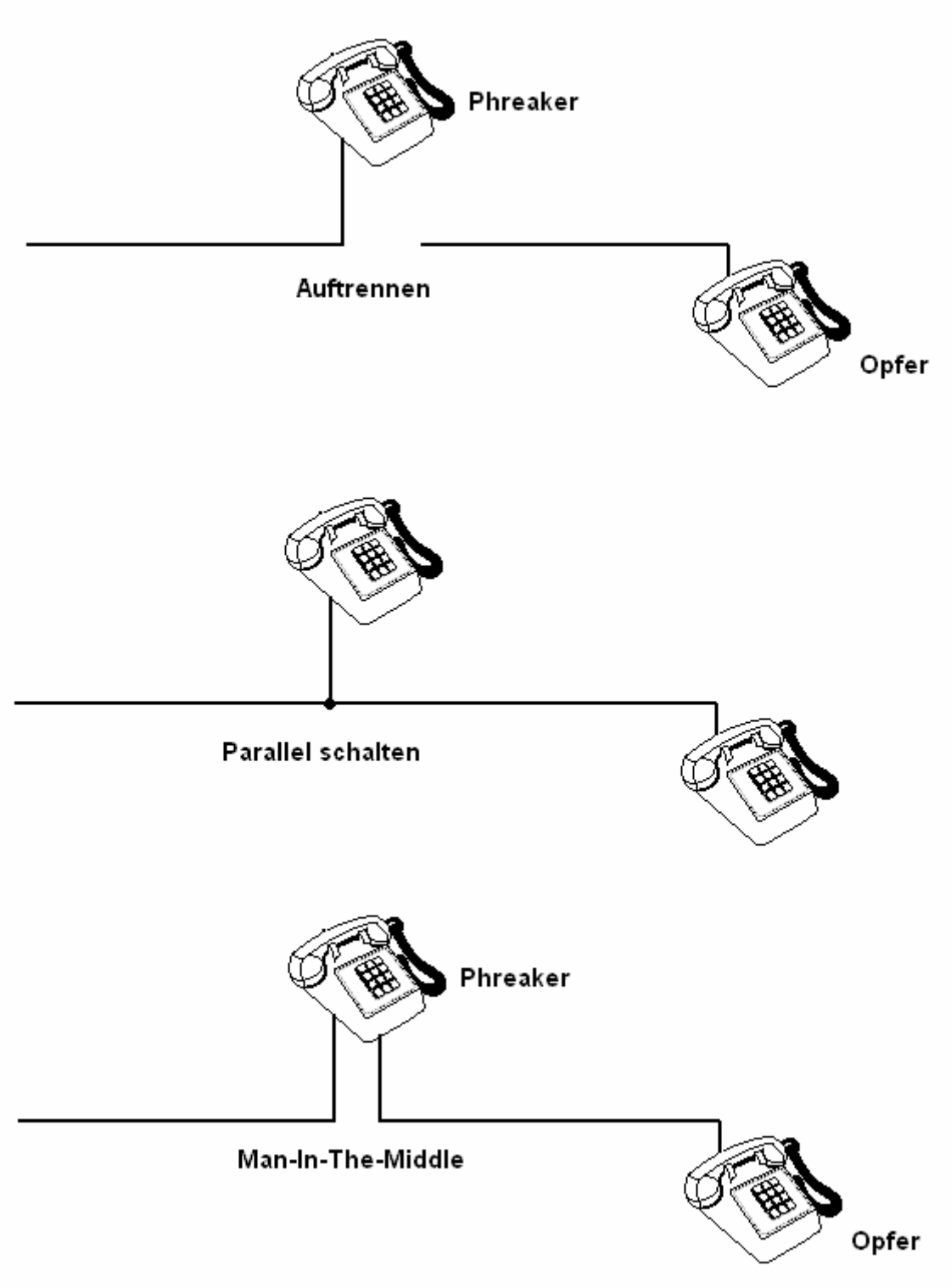
Funktion des EVz

Von außen werden wird das Verzweigerkabel vom nächstgelegen Kabelverzweiger (KVz) ober- oder unterirdisch in das Gebäude geführt. Dieses Kabel endet im EVz. Dort sind auf einer Anschlussleiste alle Doppeladern (DA) des Kabels aufgelegt. Ob auf diesen DA überall Telefonanschlüsse geschaltet sind ist dabei egal, es handelt sich bei den freien Adern um eine Reserve.
Im EVz enden auch die Endstellenleitungen des neudeutsch "Inhouse-Netz" genannten Hausnetzes. Diese Leitungen gehen von EVz in die Räume, wo ein Telefonanschluss geschaltet ist und enden in der so genannten 1. TAE-Dose.
Zwischen den Klemmen mit den Amtsleitungen und den Klemmen mit den DA des Inhouse-Netz kann eine Zuordnung vorgenommen werden.

Des Weiteren dient der APL als Bezugspunkt fürs Messen und Prüfen im Außendienst (PUMA). Kann der Anschluss am APL geprüft werden aber nicht an der 1.TAE, so ist wahrscheinlich die Endstellenleitung unterbrochen. Ist der Anschluss hingegen am KVz vorhanden, aber nicht mehr APL, so wird vermutlich das VzK defekt sein.

Dämmert's, was ihr hier sollt? Is doch klar…
Das Ding hängt im Keller, da ist man ungestört. Und gerade im Mehrfamilienhaus kann keiner nachweisen wer wann in der Nähe des APLs gekommen ist ;-)
Apropos Mehrfamilienhaus, hier kommen alle Telefonleitungen auf den Wohnungen an.
Also ist es ein Einfaches sich auf die Leitung eines (ungeliebten) Nachbars aufzuschalten.
Natürlich gerät man als hausbekannter Telefonfreak als erster unter Verdacht :-(

Angriffsarten



Alle Methoden eignen sich für alle genannten Angriffspunkte.

Auftrennen

Wenn eine Leitung aufgetrennt wird, dann ist die Teilnehmerseite vom Netz getrennt. Wenn man sich nun in Richtung Amt aufschaltet, telefoniert man anstelle der vorherigen Sprechstelle.
Die vorherige Sprechstelle ist tot. Für den Sprechstellenbetreiber ist es zunächst einmal nicht unergründlich, ob es sich um eine Störung handelt oder um Manipulation.
Eine ungewollte Manipulation ist eine Störung. So etwas kommt täglich vor wenn sich ein Servicetechniker an einem Verteiler verschaltet. Wenn die „Störung" länger andauert, dann wird der Sprechstellenbetreiber sich bei seiner Telefongesellschaft eine Störung melden. Damit steigt die Gefahr einer Entdeckung.

Parallel schalten

Die einfachste und klassischste Methode. Natürlich nicht erlaubt. Theoretisch noch nicht einmal, wenn man das wissentlich an seinem eigen Anschluss macht. Naja, war früher mal relevant, heute kräht kein Hahn danach.
Der Grund ist nämlich die Gegenseitige Beeinflussung der angeschlossenen Geräte, die zusätzliche Belastung der Vermittlungsstelle und natürlich die Abhörsicherheit.

Man-In-The-Middle

Insbesondere digitale Netze erfordern die Man-In-The-Middle Methode. Anders ist es kaum möglich den Fluss von 1 und 0 mitzuverfolgen.
Gerade die Uk_0-Leitung (Amtsleitung bei einem ISDN-Anschluss) stellt eine Herausforderung dar. An einer solchen Leitung darf immer nur ein NTBA betrieben werden. Wird ein zweiter NTBA parallel aufgeschaltet, so wird keiner der beiden funktionieren.
Um eine Uk_0-Leitung oder den internen S_0-Bus jenseits des NTBA mitzuhören, ist sehr teure Profitechnik von Nöten.

Werkzeuge

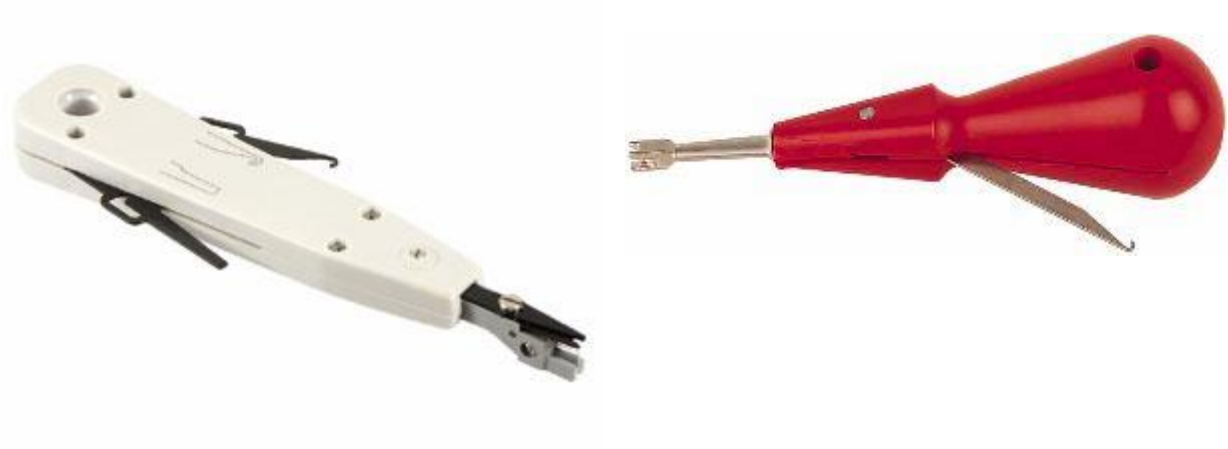
So, in der Theorie wissen wir nun, wo wir wie angreifen können. Uns fehlen nur noch die Waffen.

Schraubendreher und Zangen



Ein Standartsatz verschiedener Schraubendrehergrößen reicht aus. Die zwei wichtigsten Zangen sind der Seiteschneider und die Telefonzange

Auflegewerkzeuge



Es gibt mehrer verschiedene Typen von Trennleisten (TrL). Diese TrL in Verteilen (ÜVt, HVt, KVz, EVz) Verwendung und ermöglichen das Löt- und Schraubfreie Auflegen von Adern. Dabei werden die Adern mit dem passenden Auflegewerkezueg in Messerkontakte gepresst und so eine Verbindung erzeugt.
Wichtig: Jeder Trl-Typ hat sein eigenes Werkzeug.
Gerade auf der Kundenseite und insbesondere bei Netzwerkverkabelung hat sich das System „LSA+" durchgesetzt. Passende Werkzeuge gibt es ab 10,- Euro aufwärts in verschiedener Qualität.
Andere Systeme sind SDI-C von Quante (benötigt Quanteknubel, Bild rechts) oder HVT71 von Siemens.

Wenn man kein passendes Werkzeug hat, dann kann man stümpferhaft versuchen die Adern mit dem Schraubendreher in die Kontakte zu pressen. Allerdings beschädigt man so die Leisten und die Kontakteigenschaften sind auch mies.

Draht

An Verteilern und Verzweigern wird rangiert.
Dazu braucht man auch den geeigneten Schaltdraht.
An einem ordentlichen Verteiler fällt eine Wild-West-Verkablung SOFORT auf. An einem Verzweiger mit sonst nur schwarz-weißen Drähten fällt ein blau-weißer Draht SOFORT auf.
Nur wenn der Verteiler aussieht wie Kraut und Rüben, fällt fast gar nichts auf…
Nützlich ist die Rolle Schaltdraht auch, wenn man mal eben irgendwo eine Leitung ziehen will, z.B. aus dem Fester in die nächste Etage.
Als Stolperfalle ist der Draht natürlich auch ganz nützlich ;-)

Verbinder

Wer Leitungen auftrennt muss sie meistens auch wieder zusammenführen. Die meisten würden sicher die blanken Enden miteinander verdrillen. Das ist nicht die feine Art, weil die blanken Drahtenden Kurzschlüße verursachen können. Und bei DSL-Leitungen könnten sich Bitfehler einschleichen.



Lüsterklemmen bieten zwar eine innige Verbindung, die macht der Elektriker aber an den Kronleuchter und nicht an die Telefonleitung :-P
Die beste und professionelste Lösung, die einem Telekomtechniker nicht auffallen würde, sind Einzeladerverbinder. Achtung: Für eine Doppelader (DA) werden ZWEI Einzeladerverbiner benötigt, logisch oder. Und eine Zange zum zusammenpressen. EAVs sind im übrigens Einweg-Produkte

Leitungssucher
Gibt es schon ab 30,-€ bei Conrad, Profigeräte sind um einiges teurer und Leistungsfähiger.
Der Tongenerator des Leitungssuchers wird an einem Ende einer Telefonleitung (niemals an 230V-Leitungen!!!) angeschlossen und sendet einen Ton aus. Die Leitung fungiert dabei quasi als angeschlossene Antenne. Mit einem Tonempfänger kann die entsprechende DA wieder gefunden werden.
Der Leitungssucher ist unerlässlich wenn man z.B. herausfinden will, wo am Verteiler eine Leitung ankommt. Ohne entsprechendes Gerät bleibt oft nur die Trail&Error-Methode.

Prüfhörer



Die Servicetechniker der Telefongesellschaften sind i.d.R. mit einem ISDN-Prüfhörer ausgerüstet. Das ist nicht nur ein tragbares ISDN-Telefon, sondern beinhaltet zudem einen NTBA und viele nützliche Prüffunktionen. So ein Gerät ist frei verkäuflich, kostet aber leider an die 1000.- Euro.

Verschiedene Modelle
http://guest.engelschall.com/~martin/isdn/isdntest.htm
Des öfteren gibt es solche Prüfhörer auch bei ebay, ebenfalls für mehrere hundert Euro.

Stattdessen tut es für den Anfang auch ein normales analoges DTMF-Telefon (am besten so ein kompaktes) bzw. ein ISDN-Telefon + NTBA wenn man nach ISDN jagt.
Für DSL-Piraten zusätzlich noch ein Splitter und DSL-Modem (aber scheiße wenn man keine Steckdose in der Tasche hat).

Was sich aber jeder leisten oder selbstbauen kann ist ein

S_0-Bus-Installations-Tester



Damit lässt sich anhand der LEDs feststellen ob ein S_0-Bus korrekt verkabelt ist. Das ist besonders hilfreich, wenn man sich mit der Adernbelegung nicht sicher ist.

Adernfarben

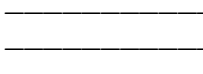
Hier werdet langsam heiß, nicht wahr? Nagut, aber ein letztes Kapitel grundlegender Theorie muss noch sein.

Wer schon mal eine Telefondose oder gar einen Verteiler geöffnet hat, sieht eine Menge bunter Drähte. Jeweils 2 Drähte bilden ein Adernpaar, eine so genannte Doppelader (DA). Die erste Ader eines solchen Paars ist die a-Ader, die zweite die b-Ader. Zum analogen telefonieren bzw. um eine NTBA anzuschließen reichen a- und b-Ader aus.
Und das beste ist, in den meisten Fällen, darf man a und b sogar vertauschen.

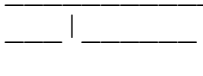
Jetzt hat dummerweise jedes Telefonkabel immer mehr als eine Doppelader. Wie gesagt, man darf a und b untereinander ungestraft vertauschen. Aber niemals sollte man die a-Ader der 1. DA mit der a-Ader der 2. DA vertauschen. Das geht schief…

So, welche ist denn nun die 1., 2., 3., … Doppelader?
Dazu haben sich findige Kabeldesigner fast idiotensicheres Farbschemata einfallen lassen.

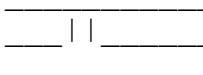
Bei den dicken Erdkabeln der Telekom und den meisten deutschen Telefonkabel, die man als Meterware kaufen kann, sind die Adern durch Ringe und Farben markiert.



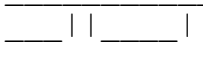
a-Ader, 1. DA (1. Ader im Kabel)
(keine Ringe)



b-Ader, 1. DA (2. Ader im Kabel)
(ein Ring)



a-Ader, 2. DA (3. Ader im Kabel)
(zwei Ringe, langer Abstand)



b-Ader, 2. DA (4. Ader im Kabel)
(zwei Ringe, kurzer Abstand)

Die Adern werden der Kürze wegen auch als a1, b1, a2, b2 bezeichnet. Je mehr Ringe pro Meter, desto höher die die Adernnummerierung. Um die Ringe und deren Abstand eindeutig erkennen zu können, sollte man den Kabelmantel ausreichend weit absetzen.

Mit der Ring-Codierung lassen sich also 2 Doppelader einwandfrei von einander unterscheiden.
Bei einem Kabel mit nur 2 DA (so genanntes 2x2-Kabel) reicht das ja auch völlig aus. Aber wenn man mehr als 2 DA hat (10x2, 20x2, 100x2)??? Hier kommen die Farben ins Spiel.

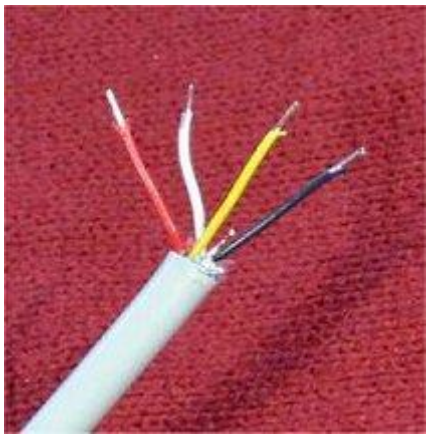
Die ersten beiden DA sind rot,
das dritte und vierte DA grün,
das fünfte und sechste DA grau,
das siebte und achte DA gelb
und
das neunte und zehnte DA weiß.

Jeweils 10 DA bilden eine Lage. Eine Lage ist mit einem Kennfaden gekennzeichnet. Mit Beginn einer neuen Lage, beginnt das Zählen wieder mit der roten DA.

Wie man ein Erdkabel mit 500 DA richtig auszählt, lernt bei der Telekom während der Ausbildung…

Es gibt aber nicht nur Telefonkabel mit Telekom-Farbgebung. Insbesondere bei Privatinstallationen (nachträgliche Kabelverlegung, S_0-Bus, etc.) findet man oft 2x2-Kabel mit folgenden Farben

1. DA	a-Ader	rot
	b-Ader	schwarz
2. DA	a-Ader	weiß
	b-Ader	gelb



Eigentlich auch ganz einfach, da die DA aber keine Grundfarbe haben, lassen sich die Einzeladern beliebig miteinander kombinieren. Und das tun mache Laien fleißig, so dass man sich nicht immer sicher sein kann, die richtige DA erwischt zu haben.

Jetzt sind wir gut gerüstet und begeben uns in Medias Res.
Als erstes mit der ältesten Anschlussvariante.

Analoge-Anschlüsse

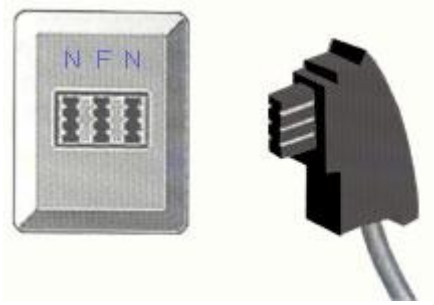
Wie der Name schon sagt, werden die Signale auf der Leitung analog, d.h. wert- und zeitkontinuierlich übertragen.
Mit einem geeigneten Umwandler kann man an jedem Punkt der Leitung diese Signale hörbar machen. Der geeignete Umwandler heißt im Volksmund „Telefon".

Da ich davon ausgehe, dass der Hobby-Phreaker keinen Prüfhörer hat wie ein Telekom-Techniker, reicht auch ein normales Telefon. Das wollen wir erstmal etwas tunen.

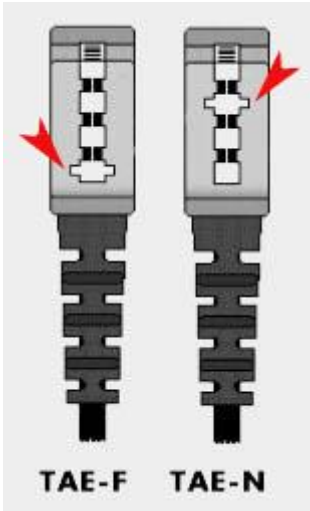


Ganz praktisch für unterwegs ist natürlich so ein Kompakttelefon.

Schaut euch mal den Stecker an. Das müsste bei deutschen Geräten ein solcher TAE-Stecker sein, der in die dazugehörige Wanddose passt.



Es gibt dabei zwei verschiedene Stecker-Typen:

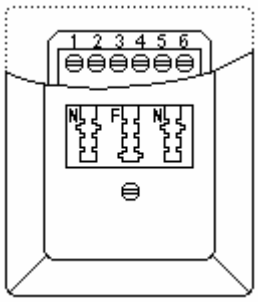


F-Codierte für Fernsprecher (Telefone) und
N-Codierte für Nicht-Fernsprecher (Fax, Modem, Anrufbeantworter).
Die Codierung erkennt man den Ausbuchtungen.

Bei F-Steckern ist diese unten (F wie Fuß), bei N-Steckern oben (N wie Nase).
Zu den Steckern gibt es auch passende Buchsen. Aber F-Stecker passen nicht in N-Buchsen und umgekehrt.
Das kann man ändern, in dem man die überstehenden Plastikflanken einfach mit einem Messer wegritzt.
So erhält man einen U-Stecker (Universal), der in beide Buchsen passt.



Jetzt wollt Ihr eurer Phreak-Telefon sicher nicht nur an der heimischen Telefondose anschließen :-)
Deshalb bauen wir uns gleich auch noch Telefondose zum mitnehmen.
Dazu besorgt Ihr euch eine NFN-TAE. Die gibt's überall wo man Telefonzubehör kaufen kann oder reißt sie irgendwo aus der Wand.



Wenn man die Dose aufschraubt sieht man oben eine Reihe von Schraubkontakten, sechs Stück an der Zahl.
Solltest Du statt Schrauben eine LSA-Leisten sehen, hast du höchstwahrscheinlich eine Monopol-TAE der Telekom erwischt. Egal, wenn man das richtige Werkzeug hat…

Für uns sind erstmal nur die ersten beiden Kontakte interessant. Wenn die beschriftet sind, dann mit 1 und 2 oder mit a1 und b1 oder mit La und Lb.
Dort schließen wir ein Stück Telefonkabel mit offenem Ende an.



An die offenen Adern auf der anderen Kabelseite bastelt Ihr dann noch zwei Krokodilklemmen dran. Mit diesen könnt Ihr euch später besser auf Löt- und Schraubkontakte aufklemmen.
Das geht schneller und ist weniger Aufwand als wenn man erst noch mit Schraubendreher oder Lötkolben rumhantieren muss. Besonders wenn man die Nachbarn, die Telekom oder die Bullen im Nacken hat.

Es gibt es wie schon erwähnt auch LSA-Klemmen. Hier steckt man keinen Stecker rein, sondern die Adern werden mit einem speziellen Werkzeug in Messerkontakte reingedrückt.
Deshalb schrauben wir an den gleichen Klemmen noch ein längeres Stück Schaltdraht. Schaltdraht hat immer einen Massivleiter, keine Litze. Schaltdraht reicht eh völlig aus, weil bei jedem aufklemmen ein bisschen Draht abgeschnitten wird. Wenn der Draht aufgebraucht ist, kann man ihn einfach gegen neuen ersetzen.

An eurer TAE-To-Go habt Ihr nun einerseits Krokoklemmen und ein Stück offenen Draht. Zusammen mit eurem Telefon eurer wichtigstes Zubehör. Diese Bastelei kann man sogar bei ISDN-Anschlüssen auf der Uk_0-Seite verwenden. Dazu später mehr.

Jetzt wollen wir aktiv werden und als erste Übung euren Telefonanschluß am APL identifizieren.
Denn APL habt Ihr hoffentlich schon gefunden, wenn nicht geht erst mal suchen. Wenn ihr ihn nicht findet, Pech gehabt. Wenn er verschlossen ist, könnt Ihr euch gerne dran vergreifen, ich weiß von nichts ;-)

So, ihr steht nun vor einem offenen Verteiler und seht eine Menge bunter Drähte. Aber welche DA führt nun zu eurer Teledondose? Es gibt nun eine Reihe von Möglichkeiten wie man dies herausfindet…

(1) Ihr habt einen Leitungssucher (keinen Metallsucher für Stromleitungen!!!). Den Tongenerator schließt Ihr an die Dose an, mit dem Tonempfänger geht ihr zum APL und lasst ihn langsam über die Drähte wandern. Das Paar, beim der Ton am deutlichsten ist, ist Eures.

(2) Ihr schraubt die Dose auf und nehmt die beiden Drähte von den Kontakten. Die blanken Ende verdrillt ihr miteinander. Dann geht Ihr mit einem Durchgangsprüfer zum APL und probiert alle Stiftpaare durch. Das Paar mit dem Kurzschluss drauf ist wahrscheinlich das eure.

(3) Die Trail ‚n' Error Methode wäre die DAs am APL der Reihe nach abzunehmen und dann ausprobieren ob eurer Telefon noch funktioniert. Aber diese scheiß Rennerei…

(4) Besser Ihr schaltet euch mit dem Prüftelefon der Reihe nach auf die APL-Stifte. Dann ruft Ihr mit dem Handy eure Nummer an und wenn das Phone klingelt, habt Ihr euren Anschluss erwischt.

(5) Kein Handy(empfang). Gut, trotzdem mit dem Telefon aufklemmen, Hörer abnehmen, Amtston abwarten und ERNA anrufen (siehe Kapitel „ERNA und andere Schlampen"). Die sagt euch dann die Nummer des Anschlusses an, von dem Ihr aus anruft (kostenlos!). Wenn Ihr eure Nummer wieder erkennt, habt ihr auf diesem Stift euren Anschluss gefunden.
Auf diese Art kann man vorsorglich auch eine Bestandsaufnahme aller Stifte und ihrer „Inhaber" machen.

Wenn man auf einem Stift keinen Wählton hört oder nur ein Rauschen, dann ist darauf entweder keine aktive Leitung oder ein ISDN-Anschluss.

Wenn man zwar einen Wählton hört, aber das Wählen einer Nummer nicht klappt (nach einigen Ziffern kommt sofort besetzt, ein Fehlerton oder eine Ansage):
Dann ist die Leitung zwar geschaltet und der Port in der Vermittlungsstelle aktiv, aber der Anschluss ist für abgehende Gespräche gesperrt.
Das ist der Fall wenn der Anschlussinhaber ausgezogen ist oder seine Rechnung nicht bezahlt hat. Dann sperrt die Telefongesellschaft den Anschluss damit darauf niemand (weitere) Kosten verursachen kann.

Beim Ausprobieren kann es passieren, dass man sich in gerade geführtes Gespräch einschalt. Dann haltet ja eurer Maul.
Man kann jetzt nämlich nicht nur mithören, sondern auch mitsprechen.
Also besteht beim Aufschalten auf fremde Leitungen ein gewisses Entdeckungsrisiko.
Tipp für erstes Problem: Beim Mithören stets das Mikrofon abschalten!

Erweiterung der TAE2Go

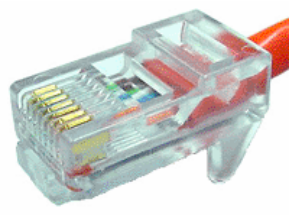
Bislang war die TAE2Go für den Einsatz an den diversen Verteilern ausgerüstet. Auf euren Streifzügen werdet ihr sich euer Telfon auch an anderen Telefondosen anschließen wollen. Da es nicht nur TAE-Dosen gibt, bauen wir uns einen Fast-Universal-Adapater.
Dazu nimmt allerlei Telefonstecker, findet heraus auf welchen Kontakten die a und die b Ader der Telefonleitung liegt und schließt die entsprechenden Adern mit Kontakt 1+2 der TAE-Dose.



Einfach zu besorgen, aber schwer anzuschließen ist der RJ11-Western-Stecker. Man kann die leere Steckern einzeln kaufen, benötigt aber eine spezielle Crimpzange zum Zusammenpressen. Deshalb ist es einfacher sich eine handelsübliche Telefonschnur TAE-RJ11 zu kaufen und den TAE-Stecker ab zu schneiden.
Der Westernstecker hat 4 Kontakte von denen 2 mit der Telefonleitung belegt sind. Aber es gibt keine Norm, welche beiden Pins das sind. Das legt jeder Hersteller selbst fest. Am gängigsten sind folgende Kombinationen:
2+3 – die beiden mittleren
1+2 – die beiden linken
1+4 – die beiden äußeren
3+4 – die beiden rechten
Andere Kombinationen sind auch möglich, aber eher untypisch.



Hier kann man nicht viel verkehrt machen, die Telefonleitung liegt auf Kontakt 1 + 2 (die meisten Stecker habe eine Beschriftung), dass sind die weiße und die braune Ader.
Wenn man solche AS-4 Stecker nicht auftreiben kann, ist das nicht weiter schlimm. Die Leitung kann an der Dose auch mit den Krokoklemmen abgegriffen werden. Die Kontakte an der Dose werden von rechts nach links gezählt, man klemmt sich einfach auf die beiden rechten.



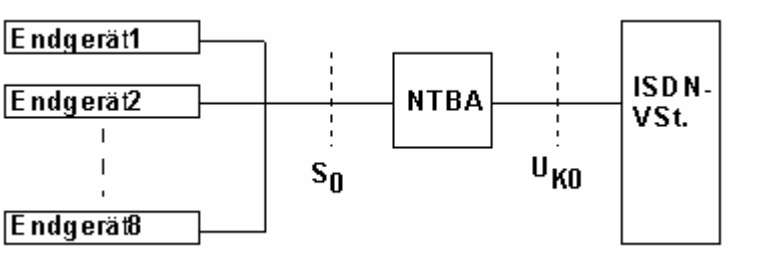
Auch ganz einfach sind die RJ45-Stecker. Für analoge Telefonie braucht man nur die beiden mittleren (4+5), bei ISDN kommen noch 3+6 hinzu.
Ob man nun ein ISDN-Kabel oder ein Netzwerkkabel abzwackt ist nebensächlich. Schaut einfach auf den Stecker und nehmt die entsprechenden Adernfarben.

ISDN-/DSL-Anschlüsse

Es gibt zwei Arten von ISDN-Anschlüssen. Den Basisraten-Anschluss (2 B-Kanäle + 1 D-Kanal) und den Primärraten-Anschluss (39 B-Kanäle + 2 D-Kanäle), auch Primärmultiplex-Anschluss genannt.
Die B-Kanäle sind die Nutzkanäle für Telefonie, Fax und Datenübertragung. Die D-Kanäle dienen hingegen der Übertragung von Steuerinformationen (gewählte Rufnummern, Auslösegrund, tc.).

Wenn im Folgenden von einem ISDN-Anschluss die Rede ist, denn meine ich stets den Basisraten-Anschluss. Das ist das gängigste ISDN-Produkt. Primärmultiplexer sind was für Behörden und Firmen mit hohem Kommunikationsaufkommen. Für den gewöhnlichen Phreaker aber erstmal eine Nummer zu groß.

Uk_0



Die Uk_0-Seite an einem ISDN-Anschluss ist die 2-Draht-Verbindung zwischen der Vermittlungsstelle und dem NTBA. Dabei handelt es sich um die gleiche Leitung wie beim analogen Telefonanschluss. Wer also von analog auf ISDN wechselt bekommt kein neues Kabel ins Haus gelegt. Alles sich ändert ist die Signalform auf der Leitung. Bei ISDN werden digitale Signale übertragen. Diese Folgen von Nullen und Einsen sind bedingt abhörsicher.
Schaltet man sich mit einem herkömmlichen Telefon auf die Leitung hört man nichts oder nur ein Rauschen. Selbst mit ein ISDN-Telefon welches man direkt an die Uk_0-Leitung anschließt funktioniert nicht. Es fehlt der NTBA, der die Signale erst noch umcodieren muss.

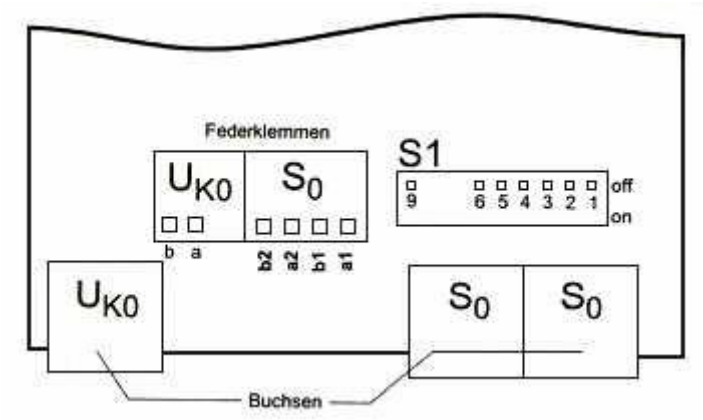


Aber: An einer Uk_0-Leitung darf nur ein NTBA hängen. Dieser tauscht nämliche Daten mit der Vermittlungsstelle aus. Und diese redet immer nur mit EINEM NTBA. Werden zwei NTBAs angeschlossen funktioniert keiner von beiden.

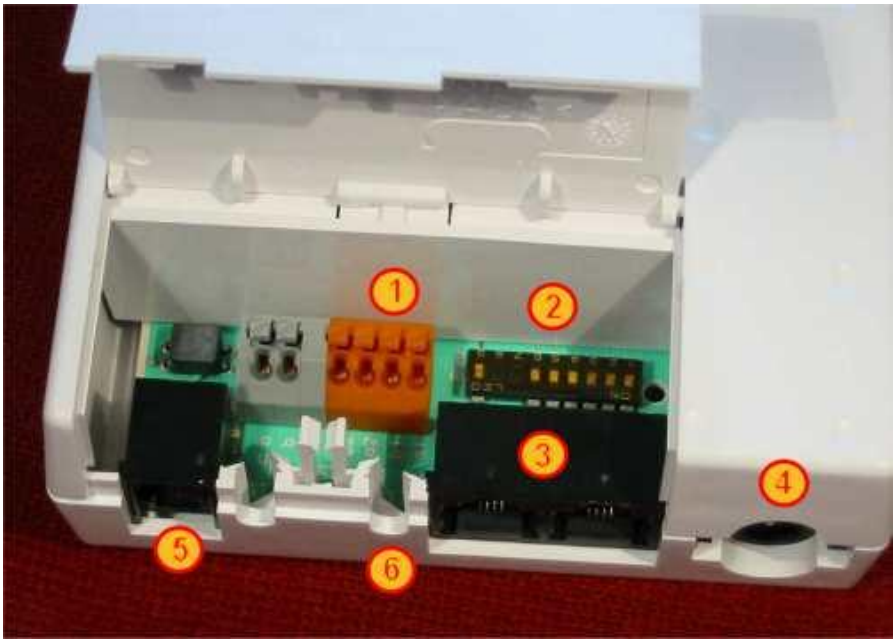
Deshalb ist es Unfug sich mit einem zweiten NTBA parallel auf eine ISDN-Leitung schalten zu wollen, um sie so abzuhören.
Dazu bedarf es professioneller Überwachsungstechnik.

Aber natürlich kann man die Leitung auch so auftrennen und einen eigenen NTBA aufklemmen. Wenn Ihr keinen habt oder einen zweiten zum phreaken haben wollt, geht mal in den T-Punkt und fragt dort nett ob ihr „zu Studienzwecken" einen alten bekommen könnt. Die Rückläufer, auch die intakten, werden im T-Punkt in großen Kisten gesammelt und dann einfach verschrottet.

Denn NTBA könnt Ihr mit der beiliegenden TAE-Schur anschließen, z.B. an eure TAE-To-Go mit den Krokoklemmen. Alternativ oder zusätzlich könnt Ihr auch wieder ein Stück Schaltdraht anbringen. Dazu hat jeder eine NTBA das Uk_0-Klemmenpaar.



1 Klemmleiste für den S_0-Bus
2 DIP-Schalter zur Konfiguration des NTBAs
3 2 S_0-Buchsen
4 Netzanschluß des NTBA (Wird in aller Regel nicht benötigt.)
5 Buchse für das Kabel zur Telefondose
6 Klemme zur Zugentlastung



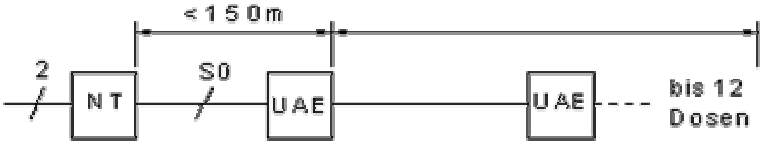
Wenn der NTBA mit einer aktiven ISDN-Leitungen verbunden wird, dann beginnt nach einiger Zeit die grüne LED zu leuchten. Wenn Ihr nun an die S_0-Buchse ein ISDN-Telefon anschließt, könnt Ihr theoretisch telefonieren.

Es gibt auch wie beim analogen Anschluss die Möglichkeit einen gesperrten oder deaktivierten ISDN-Anschluss erwischt zu haben. Die LED leuchtet zwar, d.h. nur das die Leitung zur Vermittlungsstelle geschaltet ist und der Port aktiv. Ob auf dem Port auch ein Anschluss (mit einer Rufnummer) eingerichtet ist, steht auf einem anderen Blatt.

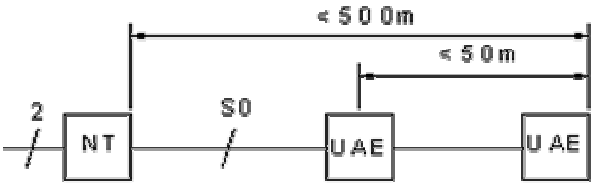
S_0

An einen S0-Bus können nur gleichzeitig acht ISDN-Endgeräte angeschlossen werden. Davon dürfen nur 4 sprachliche Endgeräte sein.
Insgesamt dürfen an einen S0-Bus 12 Anschlussdosen installiert werden. In der letzten Dose müssen die Abschlusswiderstände sitzen (2 x 100 Ohm). Die Länge der Anschlussschnur vom Endgerät zur Anschlussdose sollte 10m nicht überschreiten.

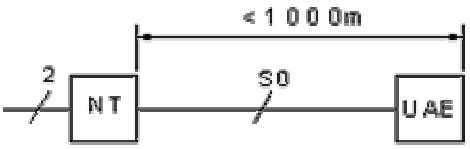
Kurzer passiver Bus



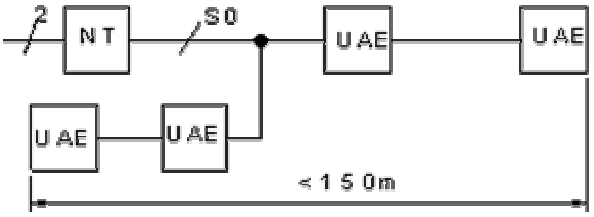
Verlängerter passiver Bus



Punkt-zu-Punkt-Verbindung



Punkt-zu-Mehrpunktverbindung

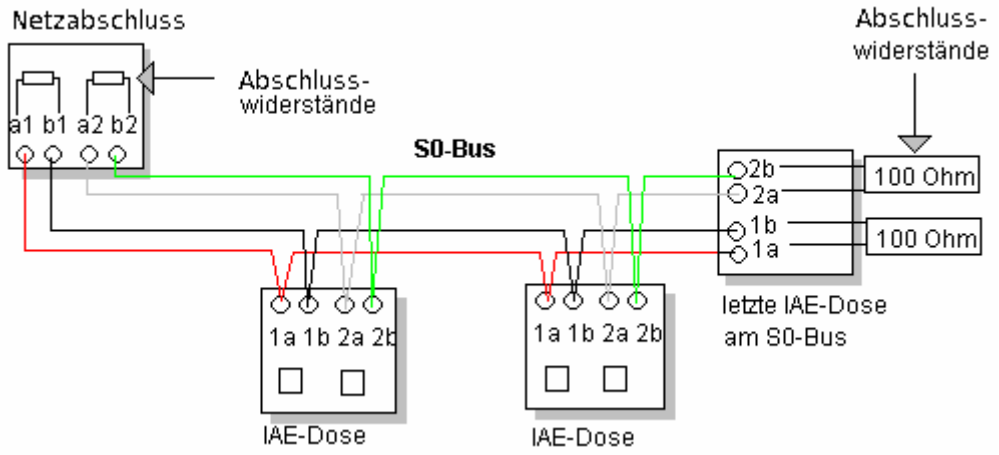


Der Unterschied zwischen dem S_0-Bus und der Amtsleitung sind 2 Drähte. Die externe Amtsleitung benötigt nämlich nur eine Doppelader, der interne Bus hingegen 2 DA. Der NTBA fungiert dabei u.a. als 2Draht-4Draht-Umsetzer.

Während man auf der Amtsseite nur einen NTBA pro Leitung anschließen darf, lassen sich am Bus mehrere Endgeräte anschließen.

Wenn man einen solchen Bus ausfindig macht und daran ein weiteres Endgerät (EG) anschließt, kann man den fremden ISDN-Anschluss mitnutzen.
Endgeräte können ISDN-Telefone, ISDN-Karten für den Computer oder Terminaladapter /Telefonanlagen sein.

Der S_0-Bus hat wie schon erwähnt zwei DA. Jeweils eine für Sende- und Empfangsrichtung. Innerhalb einer DA dürfen die Einzelader miteinander vertauscht werden. Aber niemals nicht eine Sendeader mit einer Empfangsader.
Weil es damit immer wieder Schwierigkeiten gibt, ist der Einsatz eines S_0-Bus-Installations-Testers empfehlenswert.
Man trennt die Bus-Verkabelung also an einer unauffälligen Stelle auf und schließt dort eine zusätzliche IAE oder UAE an.



Wie den Abbildungen auf der vorherigen Seite zu entnehmen ist, gibt es verschiedene Bus-Typen.
Bei einer Punkt-zu-Punkt (Point-To-Point, P-P) darf nur eine Dose/ein Endgerät angeschlossen sein. Denn dieses EG ist eine Telefonanlage, weil es sich bei P-P um einen Anlagenanschluss handelt.

Weniger Schwierigkeiten macht ein Mehrgeräteanschluss mit seiner Punkt-zu-Mehrpunkt (Point-to-Multipoint, P-MP) Verbindung. Hier fällt ein zusätzliches Endgerät nicht auf. Wenn dieses richtig angeschlossen ist, kann man damit abgehend telefonieren. Es klingelt aber nur mit, wenn keine MSN oder nur die richtige programmiert ist.

Paralleles Mithören am S_0-Bus ist so aber nicht möglich. Wer als erstes den Hörer abnimmt hat das Gespräch, Weitergabe oder interne Gespräche sind am Bus nicht möglich.

Mithören und protokollieren, welche Gespräche und Daten über den Bus laufen, lässt sich nur mit teurem Profi-Equipment.

Für den Phreaker bietet das im Normalfall zusätzlichen Schutz vor Entdeckung. Der eigentliche Anschlussinhaber kann nicht versehentlich in eines eurer Gespräche platzen. Im Idealfall bekommt er auch gar nichts mit, weil Ihr natürlich nicht beide B-Kanäle belegt. Der Inhaber kann so jederzeit telefonieren. Die Manipulation fällt erst dann auf, wenn der EVN ins Haus kommt oder ausnahmsweise mal der 2. B-Kanal benutzt werden soll.

Apropos Equipment, was tun wenn man gar kein ISDN-Telefon hat, sonder nur analoge Endgeräte. Dann hat man hoffentlich einen Terminaladapter, auch a/b-Wandler genannt. Damit lassen sich analoge EG an einem ISDN-Anschluss betreiben, das Gerät braucht allerdings eine freie Steckdose.
Geräte gibt’s als Telekom-Hausmarke, von DeTeWe (nennt sich TA33), als FritzBox, von TELES (wird nicht mehr hergestellt, nur noch über ebay), Siemens, Telnet, etc.
Die von Arcor angebotene Starterbox ist NTBA, Splitter und Terminaladapter in einem und funktioniert auch an Nicht-Arcor-Anschlüssen. Allerdings nur direkt an der Uk_0-Seite. Die anderen a/b-Wandler werden an die S_0-Seite angeschlossen.

ISDN-Tutorial der Netzmafia
http://www.netzmafia.de/skripten/telefon/index.html

ISDN-Leistungsmerkmale

Was sind ISDN-Leistungsmerkmal nennt, ist mittlerweile nicht nur an ISDN-Anschlüssen verfügbar. Da die Vermittlungsstellen vollständig digitalisiert sind, können die beschriebenen Funktionen auf von analogen Anschlüssen genutzt werden (DTMF-Telefon vorausgesetzt). Verkauft werde Leistungsmerkmale dann als Komfortfunktionen. Aber das ist das selbe in grün.

Rufnummernunterdrückung
Bei modernen Telefon-Anschlüssen kann der Angerufene eure Nummer sehen (dazu müssen das Endgerät und der Telefon-Anschluss des Angerufenen diese Funktion unterstützen - > CLIP).
Ihr könnt die Anzeige der Nummer für ein einzelnes Gespräch unterdrücken, indem ihr vor der Zielrufnummer diesen Code eingeben:

31 Nummer

Dieses Leistungsmerkmal (LM) nennt sich übrigens CLIRonRequest.

Hinweis:
Bei den Notruf-Zentralen 110 und 112 wird eure Rufnummer trotzdem immer angezeigt!
Das auch eine eigentlich unterdrückte Rufnummer angezeigt wird, ist ein weiteres ISDN-Leistungsmerkmal (CLIRO = *Calling Line Identification Restriction Override)*, welches der Otto-Normal-Kunde aber nicht beauftragen kann. Schade eigentlich…

Rufumleitung
Bei allen T-ISDN Anschlüssen außer dem T-ISDN Standard - und dem Komfortanschluss ist die Anrufweiterschaltung im Grundpreis enthalten. Bei einen T-ISDN Standard Anschluss muss das Leistungsmerkmal gesondert eingekauft und monatl. bezahlt werden.
Bei Arcor-Anschlüssen ist die Anrufweiterschaltung immer im monatl. Grundpreis enthalten.
Ankommende Anrufe können auf einen anderen, externen Anschluss umgeleitet werden.
Dafür gibt es verschiedene Varianten:

Rufumleitung sofort – alle Anrufe werden umgeleitet.
Aktivierung: *21*Nummer #
Deaktivierung: #21#
Abfrage: *#21#

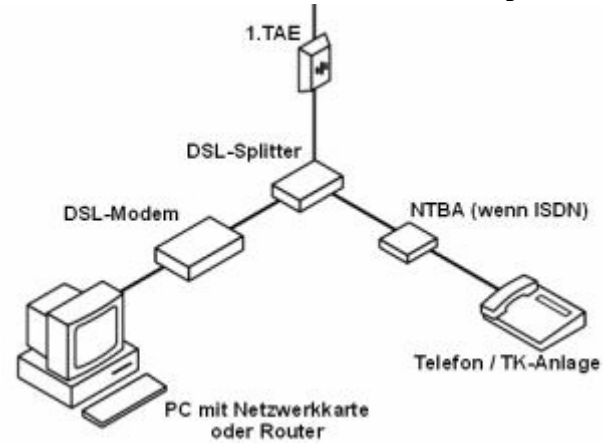
Rufumleitung bei Besetzt – Anrufe werden nur dann umgeleitet, wenn der Anschluss besetzt ist.
Aktivierung: *67*Nummer #
Deaktivierung: #67#
Abfrage: *#67#

Rufumleitung bei Nicht Melden – Anrufe werden umgeleitet, wenn nach 15 Sekunden noch niemand rangegangen ist.
Aktivierung: *61*Nummer #
Deaktivierung: #61#
Abfrage: *#61#

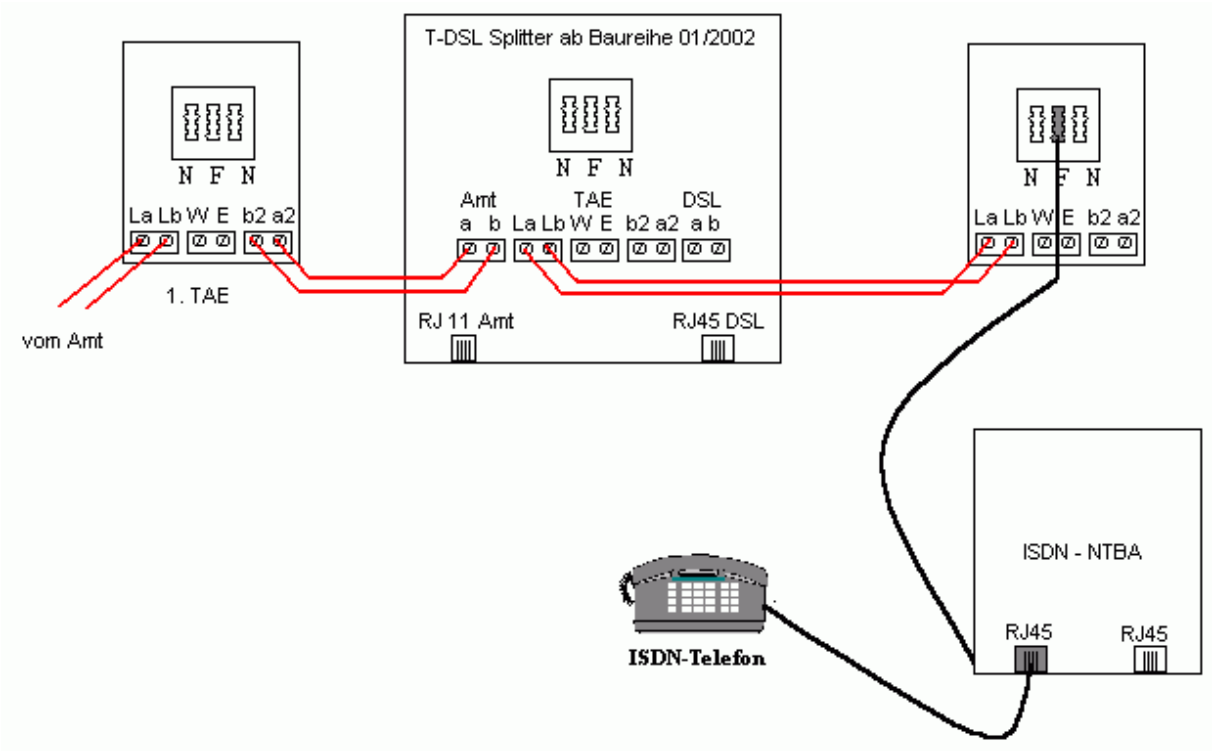
Hinweis: Ist bei einem Anschluss AWS-sofort aktiviert, so hören Sie einen Sonderwählton. Die Varianten AWS-20s und AWS-besetzt können gleichzeitig – zu unterschiedlichen Zielrufnummern – aktiviert werden. Ist jedoch die AWS-sofort aktiviert, so kommen die AWS-20s und AWS-besetzt nicht zur Wirkung. Hier muss man erst die AWS-sofort deaktivieren, damit die Anrufe bei Besetzt oder bei Nichtmelden nach 20 Sekunden weitergeleitet werden. Die Aktivierung einer Anrufweiterschaltung zu den Notrufnummern 110 und 112 sowie zu den Dienste-Rufnummern beginnend mit 11, 0900, 0137, 0138 ist nicht möglich.

DSL

Die schematische Verkablung sieht so aus



Wer beim verschrauben keine Fehler machen will, sollte auf folgendes Schaltbild achten. Es gilt für die DSL-Anschlüsse aller Anbieter.



Wer statt eines ISDN-Anschlusses nur einen analogen Anschluss hat, steckt anstelle des NTBAs natürlich das analoge Telefon in den Splitter.

Übersicht der Anschaltevarianten:
http://www.stingel.de/dsl/dslv.htm

Was kann man daran nun phreaken?

Als erstes sei gesagt, dass paralleles Anschalten eines zweiten DSL-Modems auf die Amtsleitung nicht funktioniert. Das Modem muss die Verbindungskonditionen ja mit dem DSL-Knoten (DSLAM) in der Vermittlungsstelle aushandeln (sich synchronisieren). Und das macht der DSLAM natürlich immer nur mit einem Modem pro Leitung :-(

Was können wir trotzdem mit so einer Leitung anstellen? Nun, zuerst muss mal so eine Leitung gefunden werden. DSL riecht nicht… Dafür lassen sich die DSL-Signale sowohl mit einem ISDN-Anschluss als auch mit einem analogen Telefonanschluss kombinieren. Hat man eine DSL-Leitung gefunden hat man fast auch immer eine Telefonie-Leitung gefunden.
Ausnahmen gibt es natürlich auch, so bietet QSC DSL ohne Telefonie an.

Zum Aufstöbern basteln wir uns erstmal ein geeignetes Prüfkabel. Mit einem RJ45-Stecker fürs DSL-Modem auf der einen Seite und Kroko-Klemmen zum aufklemmen an der anderen Seite.

Die Belegung des RJ45-Steckers ist wie folgt:
Genutzt werden die mittleren Kontakte 4 und 5. Dort kommen a- und b-Ader rein.
Am einfachsten schneidet man ein Netzwerk- oder ISDN-Kabel auf, sucht sich das Adernpaar, das auf 4+5 liegt (gut zu erkennen an der Farbe) und mach dort die Krokodil-Klemmen fest.

Jetzt begeben wir uns mit unserem Geraffel zum APL und hoffen, dass wir dort eine Steckdose für unser DSL-Modem haben.
DSL-Modem in die Steckdose und Prüfkabel ins Modem einstecken.
Am zu prüfenden Port müssen wir leider die Inhouse-Leitung abnehmen (hinterher wieder auflegen!), weil ja nicht zwei Modems gleichzeitig an einer Leitung funktionieren.
Dann klemmen wir die Klemmen an den Port und warten ob das Modem sich synchronisiert. Falls ja, ist es eine DSL-Leitung, falls nicht anderen Port ausprobieren.
Da ja massiv für die DSL-Anschlüsse geworben wird, ist es unwahrscheinlich in einem Mehrfamilienhaus nicht auf eine solche Leitung zu stoßen.

Was kann man mit der so entdeckten DSL-Leitung anfangen?
Nun ja, man könnte an das Modem einen Laptop hängen und dann ins Internet gehen. Dazu braucht man leider Benutzerme und Passwort.
Praktischerweise aber nicht unbedingt die des Kunden, auf dessen Leitung man sich geschaltet hat. Irgendwelche Daten die zum Anschlusstyp passen reichen aus.
So braucht man für einen T-DSL Anschluss T-Online Zugangsdaten und für eine Arcor-Leitung Arcor-Zugangsdaten.
Die muss man sich halt irgendwo beschaffen. Da eine Flatrate heute wohl Standart sein dürfte, entstehen dem Opfer auch keine zusätzlichen Kosten.
Legal, wenn auch nicht im Sinne der AGBs, ist es sich die Daten von Freunden geben zu lassen.

Die nötige Infrastruktur habt Ihr ja schon umsonst am APL gefunden und braucht keine eigene Leitung für teueres Geld bei Telekom, Arcor und Co. zu mieten.
Jetzt ist da aber das Problem mit den zwei Modems an einer Leitung. Wenn man die Leitung aufgetrennt lässt, fällt die ganze Sache auf, weil beim Opfer weder Telefon noch Internet funktioniert.
Was kann man also machen? Man kann sich immer dann Problemlos parallel auf die Leitung schalten, wenn das Modem des Opfers ausgeschaltet ist. Also z.B. nachts, während der Arbeitszeit oder der Urlaubszeit…
Legt einfach die zweite freie Doppelader eurer Inhouse-Leitung auf den Port eures DSL-Nachbars und schließ oben in eurer Wohnung an diese DA ein Splitter und Modem an.
Nachts lasst ihr eurer Modem laufen, morgens schaltet ihr es wieder aus.

Was geht sonst noch?
Oftmals hängt hinter einem DSL-Modem auch ein WLAN-Router. Der funkt das Internet in die Luft und ihr braucht das nur noch einsammeln.
Wie das geht lest ihr am besten in einschlägigen WLAN-Tutorials nach.

Exkurs: Die Starterbox



Schaut Euch mal diese beiden Boxen an. Die linke ist die „Arcor Starterbox", die rechte die „Verstatelbox"
Das ist in beiden Fällen das gleiche Gerät des Herstellers Saiphron. Nämlich das „NT 1 + *split*" - eine Kombination aus NTBA, DSL-Splitter und einem integrierten Terminaladapter.
Hier das offizielle Datenblatt:
http://www.sphairon.com/media/download/Datenblatt_Sphairon_ISDN_NT_dt.pdf

Die Geräte gibt es bei jedem ISDN-Neuanschluss gratis dazu, wenn man zuvor nur einen Anlogen-Anschluss hatte. Entsprechend häufig sind diese Geräte bei ebay wieder zu finden.
Die Anleitungen gibt es auf den Homepages der Telefongesellschaften:

StarterBox 2.1 (blaues Arcor Logo)
http://www.arcor.de/pdf/arcor/privat/produkte/arcor_dsl/arcor_starterbox_bedienungsanleitung3.pdf

StarterBox 2.0 (schwarzes Arcor Logo)
http://www.arcor.de/pdf/arcor/privat/produkte/arcor_dsl/arcor_starterbox20_1004.pdf

Anleitung Versatelbox:
https://service.versatel.de/downloads/docs/produkt/dsl_flat/ex_beschreibungen/bedienungsanleitung_versatelbox.pdf

Das besonders praktische ist nicht nur, dass man statt 3 Geräten nur eines mitschleppen muss. Das Gerät kommt z.T. sogar ohne Stromversorgung aus. Denn die Notspeisung der Vermittlungsstelle versorgt in diesem Fall genau einen a/b-Port.
D.h. man kann sich im Keller oder am KVz auf einen Uk_0-Port klemmen und trotzdem sein analoges PhreakPhone anschließen. Und das alles ohne lästige Steckdose.

Hier sind die Codes mit denen man die Notspeisung an die jeweiligen Ports vergibt. Es funktioniert immer nur ein Endgerät im Notbetrieb!!!

ISDN S0-Anschluss aktiv:	*30#
Analoge Leitung 1 aktiv (Werkseinstellung):	*31#
Analoge Leitung 2 aktiv:	*32#
Automatische Aktivierung von Leitung 1/2:	*33#

PUMA und anderes Viehzeug

PUMA ist eine dieser hirnrissigen DTAG-Abkürzungen und steht für Prüfen und Messen im Außendienst.
Dazu steht dem Außendienstmitarbeiter (ADM) eine Reihe von Instrumentarien zur Verfügung.

SEPT

Nein, funktioniert nicht nur im September ;-)
SEPT bedeutet System Externe Prüf-Technik

Den Begriff gibt es bei der DTAG schon seit Jahren.
Im Internetz gibt es dazu auch einen Text:

„Spass mit SEPT" (written in 1997 by Hitronic)
http://www.phreak.de/infos/german/sept.txt
http://www.pinguhuhn.de/text.php?id=136&s=read

Viele Infos sind aber längst veraltet.
Zum Beispiel haben sich die Zugangsnummern geändert. Diese sind mittlerweile zentral erreichbar.

Zugangsnummern
DTMF 0800-3307752
V.24 0800-3307758

Gebraucht werden ein Login-Code und ein achtstelliges Passwort.
Das SEPT wird immer speziell für einen Mitarbeiter freigeschaltet, der bekommt dann auch ein Passwort das regelmäßig geändert wird und sich beim 3. mal falsch eingeben sperrt...

Ansonsten dürften die historischen Informationen im Grunde stimmen. Einfach mal ausprobieren wenn Ihr drin seit.

Einfacher erhält man Zugang zu den modernen Prüfplätzen. Diese haben den ArPl abgelöst.

ERNA und andere Schlampen

Verwendung
Wenn ein neuer Telefonanschluss gelegt wird, oder an einem altem Änderungen vorgenommen werden, kommt normalerweise ein Techniker des jeweiligen Netzbetreibers ins Haus. Nach seinen Arbeiten muss der überprüfen, ob der Anschluss einwandfrei funktioniert. Dass der Wählton beim Abheben zu hören ist, spricht noch lange nicht für eine hundertprozentig korrekte Funktion des Anschlusses.
Dafür gibt es so genannte automatische Prüfplätze. Der Techniker wählt eine bestimmte Nummer und kann dann je nach Art und Umfang des Prüfplatzes verschiedene Tests durchführen. Das spart den Einsatz von extra dafür abgestelltem Prüf-Personal. Ansonsten müsste der Techniker in seiner Zentrale anrufen, damit die Kollegen von dort aus den Anschluss überprüfen.

Grundfunktionen
Die wichtigste Grundfunktion ist die Ansage der Rufnummer des Anschlusses, von dem aus der Prüfplatz angerufen wurde. Besonders von Vorteil ist dieses Funktion wenn der Servicetechniker mit mehreren Endgeräten konfrontiert ist, deren Nummern er nicht kennt. Oder wenn er vor einem Verteiler steht und nicht weiß welcher Anschluss auf welchem Port liegt.

Für den Phreaker ist natürlich ebenso interessant zu wissen, an wessen Anschluss er gerade rumwerkelt.

Ein weiterer wichtiger Test ist der automatische Rückruf (im Volksmund auch „Selbstanruf" genannt). Beim Rückruf wird ebenfalls die Nummer zurückgerufen, von der aus der Prüfplatz angewählt wurde.

Zugang
Erreichbar sind die Prüfplätze meist alle unter einer kostenfreien Servicenummer. Denn dem Kunden, von dessen Anschluss der Prüfplatz angerufen wird, sollen keine Kosten entstehen.
Zugang erhält aber nicht jeder, der die eigentlich geheimen Nummern anruft.
Na gut, Top Secret sind die Nummern nun nicht, aber eben nicht für Hinz und Kunz bestimmt. Daher ist manchmal ein allgemeiner PIN, persönliche Zugangsdaten oder auch gar keine Angaben nötig. Natürlich lassen sich manche Testnummern nur aus dem Netz des jeweiligen Festnetzbetreibers erreichen und selten übers Handy.

Voraussetzungen
Wichtig ist bei allen Prüfplätzen, dass ein Tastentelefon mit Tonwahlverfahren (auch DTMF genannt) benutzt wird. Von Telefonen mit Nummernschalter (Drehscheibe) oder mit Impulswahlverfahren aus funktioniert der Service nicht. Mit einem DTMF-Generator, wie er zur Fernabfrage von Anrufbeantwortern eingesetzt wird, lässt sich der Service aber genauso gut bedienen.

Folgende Prüfplätze sind zur Zeit (Juli 2006) erreichbar.

Deutsche Telekom

Bei der Deutschen Telekom AG ist ERNA, die **E**lektronische **R**ufnummer**N**-**A**nsage, unter
der gebührenfreien Rufnummer 0800-3003762 zu erreichen.
Damit sich der gestresste Telekom-Techniker die Nummer auch merken kann, ist sie als Vanity Number konzipiert und ergibt auf der Telefontastatur 0800-330ERNA.
Erreichbar ist ENRA fast aus dem gesamten deutschen Festnetz.

Wenn man die Nummer anruft hört man nur den bekannten Telekom-Jingle, dann folgt Stille.
Denn diese Nummer ist zwar von überall aus dem DTAG-Netz zu erreichen (auch Telefonzellen), aber eigentlich nicht für die Öffentlichkeit bestimmt. Daher muss nach dem Jingle ein PIN eingeben werden. Deutschlandweit gültig ist z.B. die 1420#.
Bei einem richtigen Pin ertönt eine Glocke, ansonsten eine Sirene. Nach der Sirene erhält man nochmals den Jingle und die Gelegenheit den PIN richtig einzugeben sonst fliegt man aus der Leitung.

Wenn man sich mit dem PIN angemeldet hat, begrüßt ERNA einen auch schon direkt mit der Rufnummer des Anschlusses, von dem man ERNA angerufen hat. Dabei spielt es keine Rolle, ob die Rufnummerübermittlung deaktiviert oder unterdrückt (CLIR) wurde.
Zu beachten ist allerdings, dass nur die Teilnehmerrufnummer ohne Ortsvorwahl angesagt wird.

„Die Rufnummer lautet 4-7-1-1. Wenn Dir das zu schnell ging dann gleich noch mal: 4-7-1-1. Vielen Dank für deinen Anruf."

Während dieser Ansage kann ERNA jederzeit eine weitere Aufgabe zugeteilt werden. Dazu muss einfach der jeweilige Code eingetippt werden.
Verfügbar sind
1# Automatisierter Rückruf
2# Ansage des benutzen Service-Indikators
4# Rückfax in normaler Auflösung
5# Rückfax in feiner Auflösung

Wählt man eine falsche Menüoption wechselt ERNA zum „Sie“ und trennt die Verbindung.
Ansonsten bleibt sie beim vertraulichen „Du“, man ist halt unter Kollegen.

Nach der Wahl von 1# bittet ERNA „Bitte leg jetzt auf. Ich rufe dich zurück.“
Wenn das Telefon dann schließlich klingt und man abnimmt, stöhnt die geile Schlampe von der Telekom:
„Hallo! Ich bin’s! Ich hoffe mein Rückruf hat dir geholfen. Tschüss bis zum nächsten Mal.“
Bei vorhandener CLIP-Anzeige wird übrigens eine regionale ERNA-Nummer angezeigt.

Bei 2# wird von ERNA angesagt, ob es sich beim ISDN-Dienst um Telefon, Fax oder Modem handelt.
Die Optionen 4# und 5# sind natürlich nur bei angeschlossenen Faxgeräten sinnvoll, ansonsten hört man beim Rückruf nur ein Faxsignal.

Arcor

Auch bei Deutschlands zweitgrößtem Festnetzbetreiber, der Arcor AG & Co KG, wurde ein Prüfplatz eingerichtet. Erreichbar ist er allerdings nur aus dem Arcor-Netz unter der gebührenfreien Rufnummer 0800-1071023.
Dafür ist der Zugang ohne PIN möglich und die nette Arcor-Stimme führt den Anrufer durchs Menü.

„Willkommen beim Arcor ISDN-Testdienst.
Zur Wiedergabe Ihrer Rufnummer drücken Sie die 1.
Für einen automatisierten Rückruf drücken Sie die 2.
Für einen Sprachtest drücken Sie die 3.
Für einen DTMF-Test drücken Sie die 4.
Für das Abspielen von Testtönen drücken Sie die 5.
Zum Abrufen von Leitungsschlüsselzahl und Rangierpunkt drücken Sie die 6.“

Die Rufnummernansage erfolgt hier sogar mit der Ortsvorwahl direkt zweimal hintereinander. Danach gelangt man zurück ins Menü.

Bei Wahl des Rückrufes wird das Gespräch sofort beendet und mit unterdrückter Rufnummer zurückgerufen. Hebt man ab, wird die angerufene Rufnummer vorgelesen.

Beim Sprachtest wird eine 15 sekündige Aufnahme gemacht und anschließend vorgespielt.

Während beim DTMF-Test die Tastenzahl der gedrückten Taste angesagt wird.
Die Testtöne sind jeweils 60 Sekunden lang mit zuerst 440 Hz, dann folgt ein reiner ISDN-Inbound-Test mit 1 KHz. Beendet werden kann der Test mit der #-Taste.

Unter Menüpunkt 6 sollen die Leitungsschlüsselzahl (LSZ) und der dazugehörige Rangierpunkt am ÜVt in der T-Com Stiftnotation angesagt werden. Dieser Service ist allerdings nicht für alle Anschlüsse verfügbar, d.h. es wird keine LSZ angesagt. Nach der erfolgten Ansage, kann diese mit 1 wiederholt werden. Mit 2 gelangt man auf einen Anrufbeantworter, auf dem Servicetechniker ggf. Korrekturen aufsprechen können.

HanseNet

Die HanseNet, der Norddeutsche Festnetzbetreiber und überregional durch „Alice" bekannt, besitzt keinen automatischen Prüfplatz. Unter der gebührenfreien Rufnummer 0800-9377546 wird die Rufnummer mit Ortsvorwahl angesagt und ob sich diese im Netz von HanseNet befindet. Danach wird das Gespräch sofort getrennt.

Ansage des Netzbetreibers

Unter den kostenfreien Rufnummern 0310 und 0311 hört man die Ansage des Netzbetreibers über denn man gerade telefoniert. Da man ja beliebig die Telefongesellschaften wechseln kann, ist das ein nettes Feature. Am Tag der Umschaltung kann so z.B. erkennen ob man noch mit Telekom oder schon mit Alice telefoniert.

DTMF und andere Flötentöne

Das MFV wird englisch auch **DTMF** (Dual Tone Multiple Frequency, dt. "Doppeltonmehrfrequenz") genannt. Da das Verfahren mit hörbaren Tönen arbeitet wird es im deutschen Sprachgebrauch als *Tonwahlverfahren* bezeichnet.
Diese Bezeichnung erklärt die Sache auch recht anschaulich. Denn während das Impulswahlverfahren (IWV) die Wahlinformationen in Form von Impulsen (kurzeitige Unterbrechung der Leitung) überträgt, werden beim MFV Töne übermittelt.

MFV ist daher ein In-Band-Signalisierungsverfahren, das heißt die Signale befinden sich innerhalb des normalen Sprachfrequenzbandes (330 bis 3400 KHz) und können vom Telefonierenden mitgehört werden. Daher könnten natürliche Geräusche (zum Beispiel Musik) von der Vermittlungsstelle ebenfalls als Signal aufgefasst werden. Die Frequenzen von MFV-Signalen wurden daher so gewählt, dass sie Disharmonien erzeugen, welche mit sehr geringer Wahrscheinlichkeit in der Umgebung eines Telefons auftreten.

MFV Tastenbelegung				
1209 Hz	**1336 Hz**	**1477 Hz**	**1633 Hz**	
1	2	3	A	**697 Hz**
4	5	6	B	**770 Hz**
7	8	9	C	**852 Hz**
*	0	#	D	**941 Hz**

Die Tasten „A" bis „D" werden heutzutage kaum noch genutzt; eine Verwendung besteht in der Festsetzung der Priorität eines Gespräches im Telefonsystem „Autovon" des US-Militärs.

Bei der Erkennung (Decodierung) der Töne besteht natürlich eine gewisse Fehlertolleranz:

	Normalbereich	Verwerfbereich
Frequenz	<= 1.5%	>= 3.5%
Tondauer	>= 40ms	<= 23ms

Funktion, Vorteile und Anwendungen

Das ältere IWV hat die Teilnehmeranschlussleitung (TAL) physikalisch beeinflusst. Ein IMV-Impuls war eine kurze Unterbrechung der TAL durch eine mechanische Schaltung (Nummernschalter). Das MFV kommt ohne einen physikalischen Bezug zur TAL aus.
Die Töne werden nun elektronisch erzeugt. Die Erzeugung entsteht durch die Überlagerung zweier Sinuswellen mit jeder entsprechenden Frequenz. Diese Encodier-Schaltungen sind relativ einfach und kostengünstig aufzubauen. Z.B. in Form eines Handsenders für die Abfrage eines Anrufbeantworters. Denn ein weiterer wesentlicher Vorteil des MFV ist, dass sich nicht nur Wahlinformationen übertragen lassen. Die Wahlinformation ist die Übermittlung der gewünschten Rufnummer an die Vermittlungsstelle vor dem Aufbau der Verbindung. Nach der erfolgreichen Übermittlung können bei IMV keine weiteren Wahlinformationen an die VSt oder den anderen Teilnehmer gesendet werden.
Da das MFV jedoch ein In-Band-Signalisierungsverfahren ist, können hier auch während einer bestehenden Verbindung Wahlinformationen an die verbundene Gegenstelle übertragen werden. Die Gegenstelle, ein Anrufbeantworter z.B. oder so ein Sprachcomputer, hört in die Leitung rein. Der Frequenzbereich von 900 Hz bis 1700 Hz wird herausgefiltert und in den Eingang eines DTMF-Decoders geschickt. Erkennt der Decoder eine gültige Frequenzkombination, wird ein vorher definiertes Event gestartet.
So könnte ein AB auf das Drücken der Taste 5 während der Ansage mit dem Abspielen aller aufgenommen Anrufe reagieren, auf die Taste 6 mit dem Löschen der Aufnahmen und auf 9 würde er nicht reagieren.

Verbreitung

Das MFV ist der aktuelle Stand der Technik und hat mittlerweile die größte Verbreitung. Es löst damit das ältere IMV ab. Da jedoch immer noch Endgeräte in Benutzung sind, die nur die Impuls-Wahl unterstützen, sind alle Vermittlungsstellen und die meisten Nebenstellenanlagen abwärtskompatibel. Andere Länder haben aber noch ältere Vermittlungsanlagen, so dass auch neue Telefone die für einen internationalen Markt produziert werden, das alte IWV weiter unterstützen, damit sie auch dort angeschaltet werden können Nur Sprachcomputer können mit den alten Wählscheibentelefonen oder IMV-Tastentelefonen nicht mehr genutzt werden. Es sind ab und an auch noch alte private Telefonanlagen in Betrieb, die nur das alte IWV oder auch nur das Dioden-Erd-Verfahren (DEV) unterstützen.

Erzeugung

Wer ein gutes Gehör und etwas Übung besitzt, kann sicherlich die DMTF-Ziffern unterscheiden. Aber selbst gültige DTMF-Töne zu pfeifen wird kaum jemand schaffen. Das liegt nicht unbedingt am Toleranzbereich, sonder weil es sich um Tonüberlagerungen handelt. Aber zwei Pfeifende könnten den richtigen Ton treffen…
Um die Töne immer und überall richtig zu erzeugen, gibt es DTMF-Tongeber. Sie liegen bei vielen Anrufbeantwortern bei oder können im Fachhandel preisgünstig erworben werden. Selbstbauen geht natürlich auch, Anleitung gibt's im Netz, ist aber kniffelig und teurer als ein Fertiggerät.



DTMF-Töne Online Erzeugen
http://www.matthis.thorade.de/mfv/
http://www.dsptutor.freeuk.com/dtmf/ToneGenerator.html

DMTF-FAQ:
http://margo.student.utwente.nl/el/phone/dtmf.htm

Phreaker's Anwendungsbereich

Der größte Vorteil der DTMF-Töne ist wahrscheinlich, dass es sich um Töne handelt. Und Töne kann man immerhin speichern und wieder abrufen. Auf Diktiergeräte, MP3-Player, etc. lassen sich Tonfolgen speichern.

Hier sind zwei Szenarien:

Hörer abnehmen und mit dem DTMF-Geber statt dem Tastenblock wählen. Vorteil: Die gewählte Nummer erscheint nicht in der Wahlwiederholungsfunktion des Telefons. Es gibt zudem so kleine Diktiergeräte mit 10 Sekunden Aufnahmezeit für den Schlüsselbund. Darauf kann z.B. eine wichtige Telefonnummer in DTMF-Folge abgespeichert werden.
Das führt auch schon zum nächsten Szenario.

Du hörst eine Leitung ab, auf der jemand gerade die PIN fürs Online-Banking oder seinen Anrufbeantworter eintippt. Diese geheimen Ziffern werden auch durch DTMF-Töne übertragen.
Wenn Du sie mitgeschnitten hast, kannst Du sie abspielen, wenn dich das System zur Eingabe der PIN auffordert.

Apropos,

Anrufbeantworter

Wie ihr sicher wisst, verfügen viele Modelle über eine Fernabfrage-Funktion. D.h. man kann von unterwegs seinen eigenen AB anrufen, sich mit einer PIN identifizieren und dann die aufgenommen Nachrichten abhören und löschen.
Für den Phreaker bietet sich ebenso die Möglichkeit sich von der Ferne aus einzuwählen.
Optimal wäre natürlich, wenn man weiß um welches Modell es sich beim Ziel-Gerät handelt. Dann besorgt man sich nämlich aus dem Internet die passende Bedienungsanleitung.
Dort steht auch immer der Standart-PIN. Viele Leute ändern diesen PIN nicht oder verwenden so etwas wie 0815, 4711,666 oder ihr Geburtsdatum.
Da es keine Sperrfunktion gibt, hat beliebig viele Versuche.

Tastensperren

Es gibt Telefonmodelle, bei denen lässt sich die Tastatur mittels eines Schlüssels oder eines Codes sperren, um so abgehende Gespräche zu verhindern.
Das ganze ist heute aber mehr als ein Witz für Phreaker. Hörer abnehmen, Amtston abwarten und mit der mitgebrachten Tastatur (DTMF-Geber) wählen. Fertig ist der Lack.

Blueboxing

Eine Blue Box ist eine technische Schaltung, mit der ein 2.600 Hertz-Ton produziert werden kann. Dieser Ton wurde von CCITT v5-kompatiblen Vermittlungsstellen (z.B. in den Vereinigten Staaten, Japan und Frankreich), benutzt, um sich untereinander Gesprächsweiterleitungen anzuzeigen. Beim Phreaking wurden damit illegal kostenlose Telefonate erschlichen. Modernere Vermittlungstechnik lässt das Blue Boxing nicht mehr zu.
Entdeckt wurde das Blue Boxing von einem blinden Jungen namens Joe Engressia. Der Junge entdeckte durch Zufall, dass er mit einer Plastikpfeife aus einer Tüte Cap'n Crunch-Frühstücksflocken kostenlose Telefonate führen konnte. Die Plastikpfeife erzeugte einen 2.600 Hz-Ton, der von der damaligen Telefongesellschaft der 60er Jahre Ma Bell benutzt wurde, um die Leitungsbelegung zu regeln. Dennie verriet das Geheimnis an einen Bastler namens John T. Draper, der die Methode mit eigenen Kenntnissen stark erweiterte und unbewusst daraus eine Subkultur des Hackens machte. John T. Draper (der sich später Captain Crunch nannte) wurde kurze Zeit später vom FBI verhaftet und später zu einer Gefängnisstrafe verurteilt und gehört heute noch zu den Top-Ten-Hackern der Welt.
Nachdem bei einem Telefongespräch die Gegenstelle aufgelegt hatte, stoppte das 2.600 Hz-Signal den Gebührenzähler und eine kostenlose neue Verbindung konnte gewählt werden. Inzwischen gibt es verschiedene Methoden mit Signaltönen Telefonnetze

entgegen den Vorstellungen ihrer Besitzer zu verwenden, man spricht in Fachkreisen von Phreaking.
Später baute John T. Draper sogenannte Multi-Frequency-Geräte, mit denen er weitere Töne generieren konnte. Sie wurden zunächst MF-Boxen genannt. Als John T. Draper eins der ersten MF-Boxen dem blinden jungen Dennie schenkte, wollte er die Farbe wissen. Weil John T. Draper den Frequenzgenerator in eine alte blaue Kiste eingebaut hatte, bestand Dennie darauf, das Gerät Blue Box zu nennen. Später setzte sich der Begriff Blue Box auch als die Methode selbst durch und wurde weltweit als Blue Boxing bekannt.

BLUEBOXING FUNKTIONIERT HEUTE NICHT MEHR!!!! DEFINITV !!!!!!!

Denn die heutigen Vermittlungsstellen kommunizieren im CCITT7-System (auch SS7 genannt). Das Signalisierungs-System 7 kommt gänzlich ohne Töne aus und auf die Signalisierungskanäle hat der Teilnehmer schon gar keinen Einfluss.
Aus der Traum, Leute…

Secrets of the Little Blue Box
http://www.webcrunchers.com/crunch/esq-art.html

Virtuelle Anrufbeantworter

T-Net-Box (Telekom)

Da die Bedienungsanleitung der Telekom-Box sehr umfangreich ist, ladet euch die aktuellste Version bitte auf www.t-com.de runter.
Der PIN ist übrigens 4 bis 10stellig. Vom eigenen Anschluss erreicht man die Box kostenlos unter 0800 330 2424. Aus der Ferne gebührenpflichtig unter 01805066033 (= 0800-TNETBOX).

PIA (Arcor)

Zu jeder Arcor-Emailadresse gehört eine Voicebox, die unter 069er-Nummer in Frankfurt zu erreichen ist. Der PIN-Code ist nur vierstellig. Hier die offizielle Bedienungsanleitung:

So greifen Sie mit Ihrem Telefon auf die Nachrichten im PIA zu:
1. Telefon auf das Mehrfrequenzwahlverfahren (MFV) einstellen (bei Mobil- und ISDN- Telefon nicht erforderlich)
2. Wählen Sie Ihre PIA Telefon / Faxnummer
3. Drücken Sie die Raute-Taste Ihres Telefons vor Beendigung des Ansagetextes
4. 4-stelligen PIN-Code eingeben (kann über die Weboberfläche eingerichtet werden)
5. Drücken Sie erneut die Raute-Taste Ihres Telefons
6. Weiter mit dem Telefonmenü

Das Telefonmenü ist wie folgt gegliedert

Ziffer 1
ggf. neue Sprachnachrichten
Sprachmenü (1 = anhören, 2 = löschen)

Ziffer 2
ggf. neue Faxnachrichten
Faxmenü (1= Faxpolling, 2 = löschen, 3 = weiterleiten)

Ziffer 3
ggf. neue E-Mails
E-Mailmenü (1 = E-Mails vorlesen,
2 = löschen, 3 = beantworten

Ziffer 4
alle Nachrichten
(1 = Sprachnachrichten, 2 = Faxnachrichten, 3 = E-Mails)



Ziffer 8
Ansagen verwalten
(1 = Begrüßung, 2 = Verabschiedung)

Ziffer 0
Beenden des Anrufes/
Vorheriges Menü

Steuerung
* für vorherige Nachricht
# für nächste Nachricht

Versatel MailBox

https://service.versatel.de/downloads/doku/Handbuch Mailbox.pdf

Nachrichten vom beliebigen Telefon abrufen:
eigene Telefonnummer wählen und während der Ansage die PIN eingeben
Nachrichten vom eigenen Telefon abrufen:
0800 - 22 22 22 1 wählen. Ist die Direktabfrage ausgeschaltet, bitte nach Aufforderung
die PIN eingeben.

Die nette Stimme führt einen durch das Menü und liest störrisch die Menüführung vor.
Hier das wichtigste

Sprachnachrichten	Fax-Nachrichten
1 : Die Nachricht wird wiederholt. 2 : Die Nachricht wird gespeichert. 3 : Die Nachricht wird gelöscht. 6 : Zeitstempel anfordern. 7 : Die Nachricht wird um 10 Sekunden zurückgespult. 9 : Zum Faxmenü wechseln. 0 : Hilfe zum Sprachnachrichtenmenü. * : Zum Einstellungsmenü wechseln. # : Die Nachricht wird abgebrochen	1 : wenn Sie ein Fax zur Weiterleitung auswählen möchten. Mögliche weitere Faxe werden angesagt. Die können Sie dann natürlich auch zur Weiterleitung auswählen. 2 : Das Fax wird gespeichert. 3 : Das Fax wird gelöscht. 5 : Keine weiteren Faxe auswählen. 6 : Hier werden alle Faxe zur Weiterleitung ausgewählt. Sie gelangen direkt ins Faxweiterleitungsmenü 0 : Hilfe zum Faxempfangsmenü. *: Zum Einstellungsmenü. #: Dieses Fax überspringen auswählen.

DECT, GAP und die große Freiheit

Die Zeiten in denen man das schnurloses Telefon sein Nachbars mit dem Radio oder einem Funkscanner abhören könnte sind schon seit mehreren Jahrzehnten vorbei.
Die Telefonmodelle bei denen das möglich war werden weder produziert noch sind sie zum Betrieb in Deutschland zugelassen.
Die einzigen heute verwendeten Funkstandarts sind das analoge CT und das digitale DECT.
Alle modernen Systeme arbeiten aber mit Verschlüsselung und Authentifizierung. Das alles erschwert das Abhören der Funkwellen.
Aber ein schnurloses Telefon ist eben nicht ganz schnurlos und schon gar nicht kabellos (sonst wäre es ein Mobiltelefon).
Angriffpunkte sind immer noch die Telefonleitung im Keller ;-)

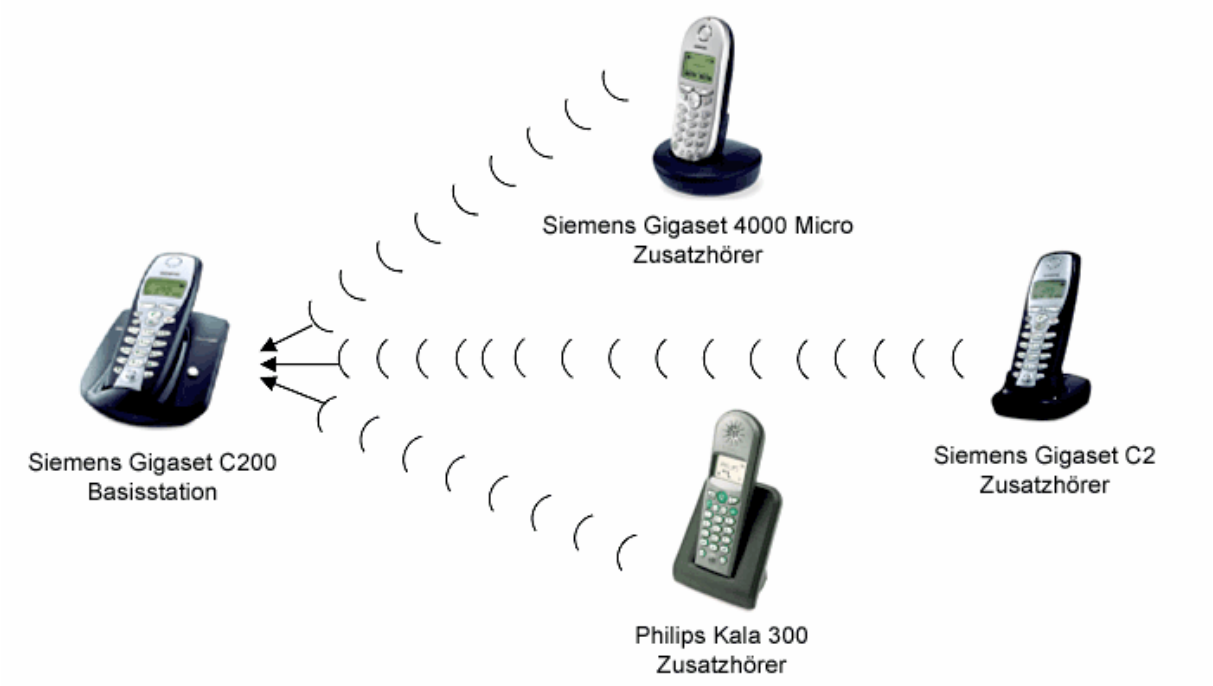
Unbefugte Benutzung und unbefugtes Mithören wird bei DECT wie bei anderen Mobilfunksystemen auch durch drei Methoden verhindert:

- Anmelden: Der mobile Teilnehmer meldet der Basisstation seine Empfangsbereitschaft.
- Ausweisen: Bei jedem Rufaufbau muss sich das Mobilgerät bei der Basisstation durch Verwendung eines geheimen Schlüssels ausweisen.
- Verschlüsseln: Die Nutzdaten (Sprache oder Daten) werden während der Funkverbindung kodiert und auf der Gegenseite dekodiert, wobei ein Schlüssel verwendet wird, der beiden Gegenstellen bekannt ist, aber selbst nicht über Funk übertragen wird. Der verwendete Verschlüsselungsstandard nennt sich DECT Standard Cipher.

Die Verschlüsselung ist ein **optionaler** Teil der DECT-Spezifikation und wird nicht von allen Geräten unterstützt.

Was aber möglich ist, weil von den Herstellern so vorgesehen, ist das Anmelden eines zusätzlichen Mobilteils an der Basisstation des Opfers ist. Bei modernen DECT-Systemen mit GAP-Funktionalität muss an eine Basisstation nicht unbedingt nur mit einem Mobilteil verbunden sein. Sondern es können mehrere Mobilteile an ein und dieselbe Basisstation angemeldet werden. Und der Clou ist: Es müssen noch nicht einmal Mobilteile des gleichen Herstellers ein.
Hauptsache, Basisstation und Mobilteile unterstützen GAP.
Das ist eigentlich bei allen modernen DECT-Stationen so.

Um ein fremdes Mobilteil an einer Basisstation anzumelden, benötigt man die Basis-PIN. Diese PIN ist in der Basis eingestellt und muss auch im „neuen" Mobilteil hinterlegt werden.
Wenn man weiß, um welche Basissstation es sich handelt, kann man sich im Internet die Bedienungsanleitung besorgen. Oftmals ändern die Kunden nämlich nie den Auslieferungs-PIN.
Also kann man durchaus mit „0000" Erfolg haben. Weitere beliebte Kombinationen sind auch 1234, 4711, 0815 o.ä.



Wie kann dieser Nepp auffallen?
Wenn sich die Basisstation nicht gerade an einem ISDN-Anschlus befindet, kann immer nur eines der anmeldeten Mobilteile ein Amtsgespräch führen. Alle anderen Mobilteile erhalten in dem Moment ein internes Besetztzeichen.
Außerdem gehört es zur GAP-Funktionalität, dass man unter den angemeldeten Mobilteilen intern und kostenlos telefonieren kann. Um das zu erleichtern, wird in der Basisstation eine interne Liste mit allen angemeldeten Mobilteilen geführt. Diese Liste ist von jedem angemeldeten Mobilteil einsehbar. Wenn da nun ein zusätzliches Gerät auftaucht, dann ist das höchst verdächtigt.

Achja, wenn der Besitzer der Basisstation den Telefonstecker rauszieht wird euer Gespräch natürlich unterbrochen. Und wenn er den Stromstecker rauszieht, ist auch eure Anmeldung futsch.

Gezinkte Karten

Hier entsteht demnächst ein Artikel über das Fälschen von Telefonkarten!!!



Aber eins lässt sich schon mal sagen: Aufladen von Telefonkarten klappt nicht!!! Auch nicht in der Mirkowelle!!!

Calling Cards

Unter dem Begriff Callingcard versteht man eine Kreditkarte, von der aus man weltweit bargeldlos telefonieren kann. Sie sind sehr beliebt, da mehr als 70% der amerikanischen Telefonkunden über eine solche Callingcard verfügen. Callingcards werden aber zum Beispiel auch von deutschen Firmen genutzt. Sie können so die Kosten eines Anrufes in die USA minimieren, da die amerikanischen Gesellschaften einen Anruf viel billiger anbieten als die teure deutsche Telekom. Die Kosten für ein Gespräch werden vom jeweiligen Anbieter der Karte übernommen und auf das normale Telefonkonto des Inhabers umgelegt oder über eine andere Kreditkarte abgerechnet. Das Telefonieren mit Callingcards gestaltet sich denkbar einfach. Der Karteninhaber ruft von einem beliebigen Land der Welt eine gebührenfreie Telefonnummer des Anbieters an. Nun gibt es zwei Möglichkeiten. Die erste ist, dass er mit einem Operator verbunden wird. Diesem nennt er die gewünschte Rufnummer, die Kartennummer und eine 4- stellige Geheimnummer. Wenn der Operator die Daten verifiziert hat, stellt er das Gespräch durch. Die zweite Möglichkeit ist, dass der Anrufer mit einem so genannten Dial-Up verbunden wird. Hier kann er selbstständig, also ohne Operator, über DTMF Töne Rufnummer, Kartennummer und Geheimnummer eingeben und wird dann verbunden. Die Dial-Ups lassen dreimal eine falsche Eingabe zu, dann wird der Benutzer automatisch mit einem Operator verbunden. Auch hier in Deutschland gibt es mit der Einführung der T-Card eine solche Callingcard. Diese wird jedoch wenig frequentiert da die deutsche Telekom im internationalen Vergleich zu teuer ist.

Angriffe auf Callingcards

Natürlich war man bei der Masse der zur Verfügung stehenden Karten schon immer sehr bestrebt diese zu phreaken. Zunächst einmal ist es wichtig zu wissen, dass sich die Kartennummer aus der Telefonnummer des Inhabers ableiten lässt und nahezu identisch mit dieser ist. Das einzige Problem besteht also in der Beschaffung der zur Karte gehörenden Geheimnummer. Um diese herauszufinden kann man die automatischen Dial-Ups benutzen. Phreaker setzen dazu Scanner Programme ein, die die Dial-Ups anrufen und zu einer Kartennummer dreimal eine Geheimnummer ausprobieren. Danach legt sie Software automatisch auf, um nicht mit einem Operator verbunden zu werden. Nun wird erneut angerufen und die nächsten drei möglichen Geheimnummern ausprobiert. Da die Fehleingaben nirgendwo gespeichert werden, hat man quasi unendlich viele Versuche zur Verfügung. Bei der nur 4-stelligen Geheimnummer beträgt die Ausbeute einer Nacht in der Regel eine bis drei Geheimnummern. Eine wesentlich elegantere Lösung des Geheimnummernproblems bot sich an, als man herausfand, dass die Geheimnummern aus der Kartennummer mit einem recht simplen

Algorithmus berechnet wurde. So kam es dazu, dass die Szene bald mit Callingcard-Generatoren überflutet wurde. In den folgenden Monaten mussten die Telefongesellschaften diese Nachlässigkeit teuer bezahlen. Daraufhin änderte man den Verschlüsselungsalgorithmus der Geheimnummer und gab neue Nummern an alle Karteninhaber aus. Trotzdem wird auch heute noch die Geheimnummer aus der Kartennummer berechnet. Dieser Algorithmus ist zwar für den Laien nicht mehr nachzuvollziehen, stellt aber für einen Cryptoanalytiker keine Herausforderung dar.

Abwehr des Callingcard Missbrauchs

Allein aufgrund des Funktionsprinzips von Callingcards gibt es für den Anbieter wenig Möglichkeiten einem Missbrauch entgegenzuwirken. Man beschränkte sich daher bei den großen amerikanischen Gesellschaften darauf, den Leistungsumfang einer solchen Karte einzuschränken. Eine Einschränkung ist das Kostenlimit. Übersteigen die Kosten ein festgelegtes Limit so wird der Anrufer automatisch mit einem Operator verbunden, der sich die Karte noch einmal verifizieren lässt. Eine weitere Einschränkung ist die Verminderung der zur Verfügung gestellten Leitungskapazität. So kann immer nur eine Verbindung über die Karte aufgebaut werden. Versucht man gleichzeitig eine zweite Verbindung aufzubauen, wird die Karte automatisch gesperrt. Außerdem lässt das System keine unnötigen Anrufe mehr zu. Man kann zum Beispiel bei Auslandskarten keine Verbindung von Deutschland nach Deutschland aufbauen.
Des Weiteren werden auch die Rufnummern der verwendeten Anschlüsse geloggt und bestimmte Rufnummern/Anschlüsse auf eine BlackList gesetzt. Anrufe beim Dial-Up von diesem Anschluss werden nicht durchgelassen.

Lösungen

Funktionsfähige Code-Generatoren sind defacto ausgestorben und das zufällige Ausprobieren führt auch nicht sehr weit.

Die sinnvollste Lösung ist sicher, jemanden seine Kennung + PIN zu klauen. Dazu schaut man jemanden, der gerade diese Nummern eintippt, unauffällig über die Schulter. Geeignete Orte sind Hauptbahnhöfe oder Flughäfen. Orte eben, wo viele Reisende sind, die solche Karten häufig nutzen.
Zu beobachten ist übrigens, dass die Leute bei der Benutzung öffentlicher Telefone weitaus sorgloser sind als bei der Benutzung von Geldautomaten…

Deutsche Card-Anbieter

DeTeCard (T-Card):	www.detecard.de
GoBananas:	www.gobananas.de
Vica24 (Call Germany):	www.vica24.de
Hagenuk:	www.hagenuk-phonecard.de
C3:	www.cardsville.com
Median (HELLO Card):	www.median-telecom.de
AS Callingcard:	www.as-callingcard.de

Mathe-Exkurs: Bruteforce

Viele Systeme erfordern die Authentifikation des Benutzers durch ein Kennwort. Bei Systemen, in die man sich mit dem Telefon einloggt, ist dieses Kennwort zwingend numerisch. Denn was anderes als Zahlen kann mit der Telefontatstur nicht eintippen.
Was kann man tun, wenn man den geforderten Zahlencode nicht kennt? Man kann versuchen ihn zu erraten oder alle möglichen Codes durchprobieren. Die Methode „Durchprobieren" nennt sich Bruteforce.

Das Erraten basiert auf einer simplen Erfahrung. Wenn ein das Kennwort durch einen Menschen vergeben wird, dann neigen viele Menschen eine in sich logische, einfach zu merkende Ziffernfolge zu wählen. Diese ein einfacher zu merken, wenn man die nicht all zu häufig verwendet bzw. schnell abrufbar wenn man sie sehr häufig eintippen muss.
Daher sind beliebte vierstellige Codes z.b. für Anrufbeantworter: 0000,1234,0815,4711. Nahe liegend wäre auch ein Geburtsdatum wie 0903 für den 9. März.
Auf Grund dieses psychologischen Phänomens, werden sichere Zugangscodes stets durch Algorithmen erzeugt und können vom Benutzer nicht geändert werden.

Wenn man mit diesen Standart-Kennwörtern nicht weiter kommt und sich das gültige Kennwort auch nicht anderweitig verschaffen kann (stehlen, Eingabe beobachten, Bestechung), bleibt einem nichts anderes übrig als alle möglichen Ziffern folgen durchzuprobieren. Und das können verdammt viele sein…

Wenn man Größe des Zeichenvorrat n und die Länge k des Codes kennt, kann man die Anzahl aller Möglichkeiten mit n^k berechnen. Der Zeichenvorrat der Telefontastatur ist {0,1,2,3,4,5,6,7,8,9}, n ist damit 10.

Für eine vierstellige PIN gibt es also $n^k = 10^4 = 10.000$ Möglichkeiten.
Angenommen für das ausprobieren einer Kombination benötigt man 10 Sekunden (eintippen und Rückmeldung des Systems abwarten), dann braucht man 10.000x10s = 100.000s = 27,8h um alle Variationen auszuprobieren.

Schneller geht es wenn man weiß, dass keine Ziffer im Codewort doppelt vorkommt.

Hier gibt es dann $\frac{n!}{(n-k)!}$ Variationen. Dies wird auch als fallende Faktorielle $n^{\underline{k}}$ dargestellt.
Ein wissenschaftlicher Taschenrechner erspart hierbei durch die Funktion(staste) **"nPr"** viel Tipparbeit: i.d.R. Eingabe **n**-Wert, Taste **"nPr"**, Eingabe **k**-Wert, Taste **"="**. Außerdem führen Fakultäten von großen Zahlen zum Überlauf, zum Beispiel 300P3=26730600 lässt sich kaum mit der Fakultät berechnen.

Anhand der vierstelligen PIN würde das bedeuten:
Es gibt $n^{\underline{k}} = 10^{\underline{4}} = 5.040$ Variationen.
Dauer zum Ausprobieren nur noch 5.040 x 10s = 14h

Wenn man also lange genug Zeit hat, bekommt man auch ein 10stelliges Kennwort raus.
Damit dass niemand versucht, haben einige Systeme einen Zähler für ungültige Angaben. Beispiel: Handy-PIN, EC-Karte, etc. Gibt man dreimal (in beliebigen zeitlichen oder örtlichen Abstand) einen falschen Code ein, wird der Zugang zum System für den Benutzer gesperrt.

Telefonzellen und andere Hexenhäuschen

Definitiv kostenlose Gespräche

Notrufnummern (110, 112) und freeCall-Rufnummern (0800) können bei allen öffentlichen Fernsprechern auch ohne Münzeinwurf und ohne Karte erreicht werden.

Anrufen von T-Zellen

Zellen, die man zurückrufen kann, erkennt man am einfachsten daran, dass die Zellen-Rufnummer irgendwo sichtbar in der Zelle angebracht ist. Telekomzellen haben oftmals eine magentafarbenes Glocken-Sysmbol.
Aber Zellen, die man anrufen kann werden seltener. Bzw. die T-Com hat diese Funktion deaktiviert. Immer mehr Leute haben sich in der T-Telle zurückrufen lassen. Ist doch klar, ein Gespräch aus der Zelle kostet mind. 10 Cent, und für 10 Cent kann man im normalen Festnetz ca. 5 Minuten telefonieren.

Aber wie bekommt an die Nummer raus?
Jeder Apparat mit dem man abgehend telefonieren kann, hat auch eine Rufnummer. Diese erfährt man entweder

a) bei ERNA (siehe in dem Kapitel)

b) sie steht irgendwo im Klartext im Aushang der Zelle

c) sie steht verschlüsselt im Aushang der Zelle

a) und b) sollten klar sein.
Jede Telekom-Zellen hat zudem eine Standortnummer, die ebenfalls gut lesbar in der Zelle angebracht ist. Meistens unten rechts an der Informationstafel.
Die Standortnummer setzt sich aus der Ortsvorwahl + einigen Nullen + Rufnummer zusammen. Man kann daraus also die Rufnummer der T-Zelle ablesen.

Ruft man diese Nummer an, so wird man höchstwahrscheinlich eine Fehleransage erhalten z.B. „Diese Rufnummer ist nicht vergeben“.

Einige Modelle können zwar angerufen werden, klingeln aber nicht. Wenn man den Höre im richtigen Moment abnimmt, kann man das Gespräch entgegen nehmen.

Z.B. die von New World Payphones (www.nwpayphones.de; Hotline: 0800-PAYPHONE).
Diese Geräte sind weis und stehen in Deutschland an öffentlichen Plätzen mit hohem Publikumsverkehr. Z.B. an Bahnhöfen, Flughäfen, Kinos, Stadien, etc.
Hier ein Bild:



Diese Gerät sind i.d.R. anrufbar, klingeln jedoch nicht (der Wecker ist abgeschaltet). D.h. man muss wissen dass jmd anruft und im richtigen Moment den Hörer abnehmen.
Jetzt noch ein kurzes Tutorial wie man dieses Wissen anwenden kann:

1. Suche dir einen NWP Fernsprecher
2. Ruf eine Rufnummernansage an und notiere dir die Rufnummer
3. Aktiviere den Selbstanruf und drücke die Gabel mit den Fingern runter (gedrückt halten)
4. Warte 10 Sekunden und lass die Gabel dann hochschnellen
5. Wenn sich der Computer meldet, ist die T-Zelle anruf bar. Wenn nicht such dir eine andere
6. Rufe einen Kumpel an und gib ihm die Nummer der T-Zelle durch
7. Mache ihm klar, dass er dich genau 30 Sekunden (60 Sekunden) nach du eingehangen hast zurück rufen soll. Er soll es mindestens 1 Minute lang klingen lassen!
8. Lege den Hörer auf und warte die vereinbarte Zeit +10 Sekunden
9. Nimm den Hörer ab, jetzt sollte dein Kumpel dran sein!

R-Gespräche in T-Zellen annehmen

Man könnte jetzt meinen, wenn man ein Payphone anrufen kann, kann man dort ein R-Gespräch annehmen und der Besitzer müsste es bezahlen. Weit gefehlt.
Auf den Trichter sind Telefongesellschaften und Payphone-Hersteller schon längst gekommen.
Deshalb senden Payphones einen so genannten „Kuckkuckston" (Payphone Recognition Tone (PRT), auch Kuckuckston oder Münzerkennungston) aus. An dieser Tonfolge erkennt der Operator, dass sich bei dem Teilnehmer um ein Payphone handelt und stellt der R-Gespräch NICHT durch.
Automatisierte Systeme erkennen diesen Ton manchmal aber nicht korrekt.
Außerdem lässt sich bei vielen Geräten der PRT per Programmierung abstellen.

Aus einer Telefonzelle umsonst Telefonieren

Ein Tutorial von Munin[F5G]
gefunden auf www.Fuckup5Group.de.vu

Moin Leutz, heut will ich euch mal erklären wie man aus ner schönen Gelben Telefonzelle umsonst telefoniert unds tolle an der Sache ist das es auch noch geht und nix mit irgendwelchen piepstönen zu tun hat ;)

als erstes suchen wir uns dazu nee einsam stehende gelbe Telefonzelle, wenn wir eine gefunden haben, gucken wir sehen uns erst mal ganz genau an. Unterm Telefon auf dem Boden der Zelle müsstet ihr nen großenrechteckigen Kasten sehen mit nem dicken Schloss und zwei bleiblomben dran. die blomben müsst ihr nun irgendwie abkriegen, ich empfehle dazu nen akkubohrer, das schloss ist nur nee atrappe. wenn der kasten auf ist sieht das dann ungefähr so aus...



der linke kasten davon ist der sicherungskasten mit zwei sicherungen drin (schätzungsweise eine fürs tel und eine fürs licht)der rechte kasten ist der stromkasten, also finger wech ;)



uns interessiert aber mehr der kleine kasten ganz links, das schwarze dicke kabel was außer erd kommt ist das telefonkabel. Na sch neugierig was im kasten drin is?!? *g* dann machen wir ihn jetzt mal auf...

die zwei roten kabel die anner linken seite von dem kasten raus gehn sind die telefonkabel wie ihr sie im haus auch habt. da braucht ihr jetzt nur noch nee tae Buchse rann klemmen unser Modem bzw. Telefon einstöpseln.. kleiner tip macht die Zelle danach wieder zu dass es keiner sieht und ihr sie länger benutzen könnt. das wars eigentlich schon, hoffe es hat euch ein bissel geholfen. falls ihr noch fragen habt ab ins Forum damit machts jut Denta



Hinweis: Heute laufen fast alle Zellen über ISDN. D.h. man muss sich mit einem ISDN-Pürfhörer oder einem NTBA+ISDN-Telefon auf die gefundene Leitung schalten!

Basteleien

AWADo/AMS

Wenn man zwei Telefon parallel auf eine Leitung schaltet, kann an jedem Telefon alles mitgehört werden und sogar untereinander gesprochen werden.
Das ist natürlich höchst verräterisch wenn man sich widerrechtlich auf eine Leitung aufschaltet.

Beispiele:
Du hörst deiner Nachbarin beim Telefonsex mit ihrem neuen Lover zu, plötzlich musst Du niesen und schon hast Du dich verraten.
Oder andersrum: Wenn man also gerade mit der heißen Lady aus dem TV-Nachtprogramm zugange ist und das Opfer rein zufällig in dem Moment den Hörer an seinen Apparat abnimmt, dann ist die Manipulation doch sehr offensichtlich!

Also besteht beim Aufschalten auf fremde Leitungen ein gewisses Entdeckungsrisiko.
Tipp für erstes Problem: Beim Mithören stets das Mikrofon abschalten!

Aber wie verhindert man nun, dass das Opfer die Gespräche des Phreakers mithört.
Halt, bevor wir wieder kriminell werden, hier noch eine andere legale Anwendung. Du teilst dir mit deinen Eltern einen Telefonanschluss, die Telefone hängen parallel an der Leitung. Tja, Arschkarte, deine Eltern können mithören was Du und deine Kumpels zu bequatschen habt…

Die Lösung für alle Probleme: Ein Automatischer Mehrfach-Schalter (AMS). Das ist das nachfolge Model zur AWADo. Die AWADo-Technick ist aber out-of-date, weil sie 3 Adern benötigt, AMS kommt mit 2 aus.

Mit automatischen Umschaltern können zwei oder mehr Telefone (legal) an einem Anschluss betrieben werden. Die prinzipielle Arbeitsweise eines Umschalters für zwei Telefone kann wie folgt beschrieben werden: Ein ankommender Ruf wird auf beiden Apparaten signalisiert, d.h. es läuten beide Telefone. Das Gespräch kann an beiden Apparaten entgegengenommen werden, dabei erhält der Teilnehmer das Gespräch, der als erster den Hörer abhebt. Der andere Apparat ist dann abgeschaltet. Das Gespräch kann zum anderen Apparat weitergegeben werden, indem ein weiterer Teilnehmer dort den Hörer abnimmt und der zur Zeit gesprächsführende Teilnehmer dann seinen Hörer auflegt. Interne Gespräche, wie bei Telefonanlagen, sind bei einem automatischen Umschalter nicht möglich.

Zum Aufbau einer Telefonverbindung sind beide Telefone wahlberechtigt. Während auf einem Apparat telefoniert wird, bekommt man auf dem anderen Apparat den Besetztton, wenn man den Hörer abhebt.

Allerdings gibt es die Möglichkeit der Vorberechtigung. Dabei ist das 1. Telefon dem 2. Telefon vorberechtigt. D.h. wenn beim 1. Telefon der Hörer abgenommen wird, wird das Gespräch beim 2. Apparat unterbrochen.

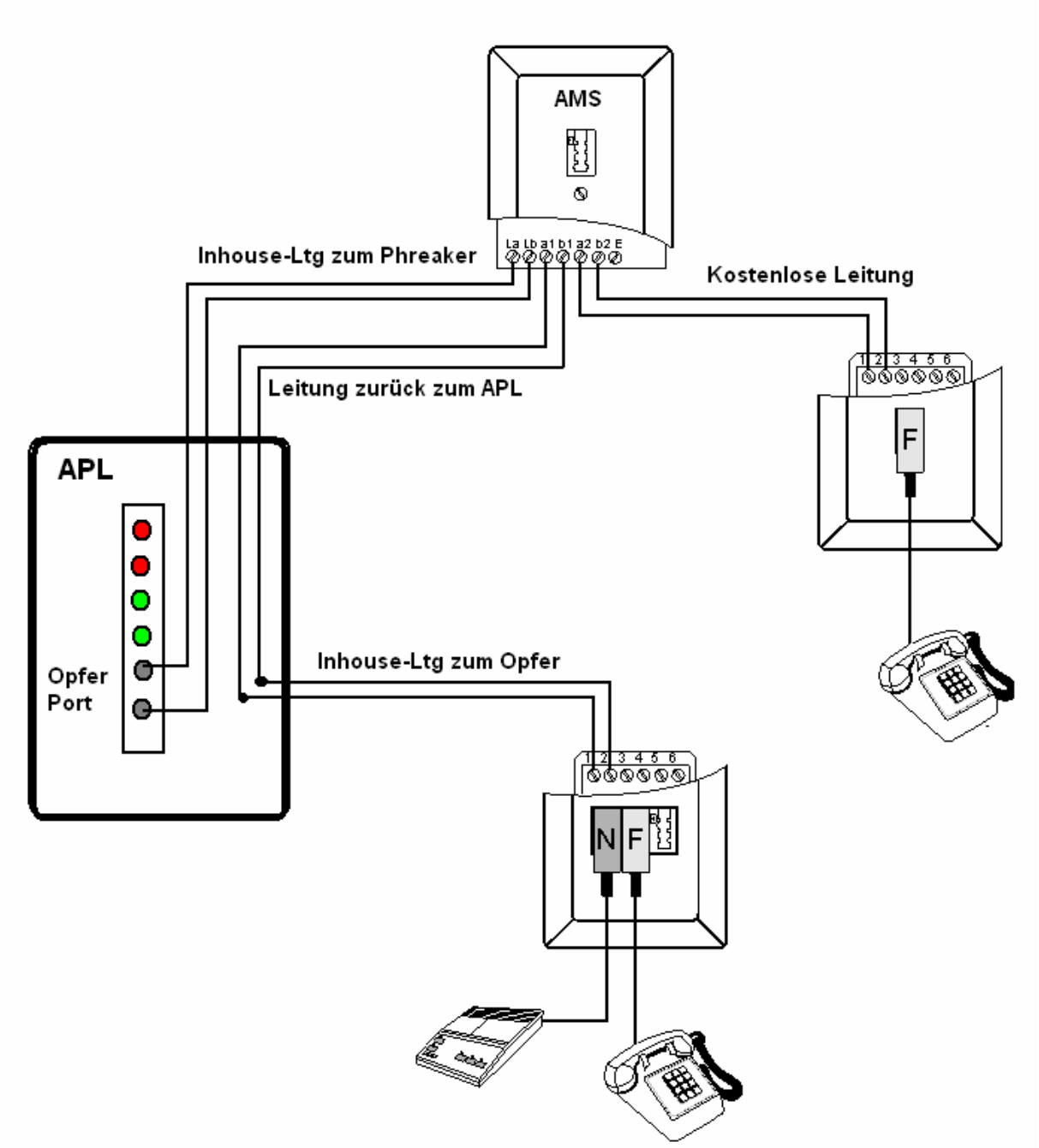
Der Einsatz beim Phreaking ist also ganz einfach. Dazu macht man sich am besten am APL zu schaffen. Wenn alles optimal ist, dann führen aus deiner Wohnung 2 DA zum APL. Über die erste DA läuft dein Anschluss (falls Du einen hast), die andere ist hoffendlich frei und unbeschädigt. Die kannst Du nun hervorragend nutzen.
Amtsleitung des Opfers auftrennen, deine 1. DA auf den APL-Port schalten und in deiner Wohnung AMS dranhängen. Die 2. DA auf Port 1 des AMS schalten und am APL mit der „alten" Amtsleitung die zum Opfer führt verbinden.
Dein neuer kostenloser Anschluss kommt an Port 2.

Tipp: Deinen Telefonapparat auf lautlos stellen. Denn immer wenn das Opfer angerufen, klingelt dein Telefon mit. Wenn Du drangehen würdest, würde es beim Opfer aufhören zu klingeln. Das an sich wäre schon verdächtig, aber wer ist schon so dumm die Anrufe seines Opfers zu beantworten. Ok, Psychos gibt es immer wieder.

Diese Schaltung eignet sich also nicht unbedingt zum abhören und mitschneiden. Zweck ist eher ein ungestörtes Telefonieren auf fremden Rechnungen.

Mit der Entdeckung ist das so ne Sache. Wenn man die Leitungen am APL geschickt versteckt, was bei unübersichtlichen APLs natürlich einfacher ist, sieht man den Nepp nicht auf Anhieb. Die Leitung, die von deiner Wohnung über den APL in die Wohnung des Opfers führt, ist aber Beweis genug…

ACHJA: Der AMS funktioniert nur bei analogen Leitungen, NICHT bei ISDN!!!


AMS
La Lb a1 b1 a2 b2 E
Inhouse-Ltg zum Phreaker
Kostenlose Leitung
Leitung zurück zum APL
APL
Opfer
Port
Inhouse-Ltg zum Opfer
1 2 3 4 5 6
F
N F

Bausatz: ISDN-Tester

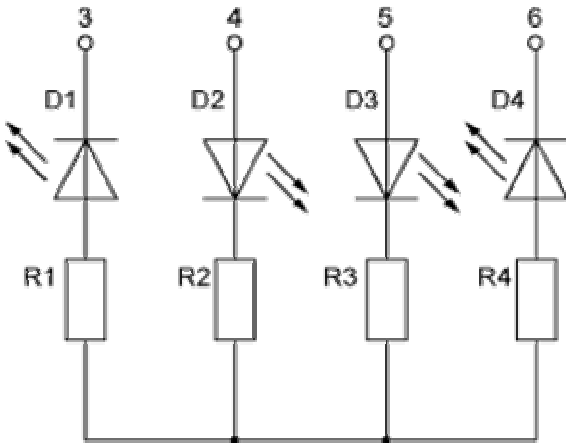
Geklaut bei http://www.elektronik-kompendium.de/sites/praxis/bausatz_isdn-tester.htm

Mit diesem ISDN-Tester kann ein ISDN-Anschluss darauf geprüft werden, ob er richtig angeschlossen ist. Über die Leuchtdioden wird angezeigt, ob die Adern richtig angeschlossen sind, Vertauschungen bestehen oder ein Kabelbruch vorliegt.
Damit die Schaltung richtig funktioniert müssen alle Abschlusswiderstände (2 x 100 Ohm) aus dem S0-Bus ausgebaut werden.

Funktionsbeschreibung

Eine grün leuchtende Leuchtdiode zeigt, dass die Ader richtig angeschlossen ist. Eine rot leuchtende Leuchtdiode zeigt, dass die Ader an der falschen Klemme angeschlossen ist. Meist leuchtet dann noch eine andere Leuchtdiode rot. Es richt dann, wenn man diese beiden Adern miteinander tauscht.
Leuchtet eine Leuchtdiode gar nicht, dann besteht keine Verbindung zwischen TK-Anlage/NTBA und UAE-Dose (RJ-45). Eventuell ist sogar die Dose defekt.

Schaltung



Materialliste:

Zeichen	Bauteil	Wert / Typ
R1	Widerstand	3,3 kOhm
R2	Widerstand	3,3 kOhm
R3	Widerstand	3,3 kOhm
R4	Widerstand	3,3 kOhm
D1	Leuchtdiode	Duo-LED, rot/grün, 2 Pin, 3mm
D2	Leuchtdiode	Duo-LED, rot/grün, 2 Pin, 3mm
D3	Leuchtdiode	Duo-LED, rot/grün, 2 Pin, 3mm
D4	Leuchtdiode	Duo-LED, rot/grün, 2 Pin, 3mm
	RJ-45-Stecker mit Kabel	Belegung 3-4-5-6

Sicherheitshinweise

Bitte bauen Sie die Schaltung mit viel Sorgfalt auf. Unsachgemäße Behandlung der Bauteile kann zur Zerstörung führen. Berücksichtigen Sie auch, dass die Bauteile für diese Schaltung ausgewählt wurden und eventuell für eine andere Anwendung nicht geeignet sind.
Der Nachbau und Betrieb geschieht auf eigene Gefahr! Jegliche Haftung für Schäden wird ausgeschlossen!

Schwierigkeitsgrad

Dieser Bausatz ist einfach aufzubauen. Einziger Knackpunkt ist die richtige Polung der Leuchtdioden. Wird hier ein Fehler gemacht, dann ist die ganze Schaltung Murks.

Normaltariflines (Party Lines)

Eine Party Line hatte ursprünglich gar nichts mit feiern zu tun. Eine PL ist eine Leitung an der mehrere Telefonanschlüsse gleichzeitig und gleichberechtigt angeschlossen sind. Eine Art Gemeinschaftsanschluss eben, z.B in sehr ländlichen Regionen. Später kamen findige Phreaker auf die Idee durch Manipulation der Vermittlungsstellen mehrere Telefonanschlüsse in einer Art weltweiten Konferenz zusammen zuschalten. Damit wurde der Begriff Party wortwörtlich.

Eine solche Bewegung, die in den 1970er Jahren die kostenlose Nutzung des Telefonnetz propagierte und Party Lines organisierte, waren die Yippies. Sie organisierten die weltweiten YIPL – Youth International Party Lines.

Heute im 21. Jahrundert gibt es in Deutschland mehre öffentliche und legal zugängliche Konferenzsysteme. Diese quasi nichts anderes als ein auf Sprache basierendes Chatsystem, wie man es aus dem Internet kennt. Es können sich mehre Teilnehmer gleichzeitig einwählen und sich auf mehrere Räume verteilen. Entweder man bleibt anonym oder richtet sich einen festen Benutzer ein. Dann hat man die Möglichkeit eigene Jingles zuspeichern und bekommt ein eigenes Postfach zu gewiesen.

Die Verbindung zu diesen Communities kostet nicht mehr als ein Ferngespräch nach in den Ort wo der Computer steht bzw. ein Orts- oder Nahbereichsgespräch wenn man die regionalen Einwahlnummern benutzt oder in der gleichen Stadt wohnt.

Das ganze nennt man „Normaltariflines“.
Da es ja mittlerweile auf Telefon-Flatrates gibt, kann man völlig kostenfrei und stundenlang den Psychos aus ganz Deutschland lauschen.

In Anlehnung an die legendären YIPL-Veranstaltungen, nennt der Hamburger Betreiber Telefonmonster (kurz: Telemon) seinen Dienst YIPL.de

Youth International Party Line



Telefonmonster - Sprachkonferenz Testsystem
(040) 80 80 16 99 Festnetztarif Hamburg
Keine Service- oder Sonderrufnummer

www.yipl.de

Hier nun die offiziellen Nummern und das Handbuch:

Diese Rufnummern sind bei Alice/Hansenet geschaltet und
kommen auf dem Chat in Hamburg raus.

Fuer den Anrufer aus der jeweiligen Stadt ist der Anruf
ein Ortsgespraech oder wenn er selbst bei Alice Kunde ist
ein netzinternes Gespraech, obwohl er in Hamburg rauskommt.

```
Muenchen    : 089  9616-6169 -> Raum 101
Berlin      : 030  9440-0449 -> Raum 102
Frankfurt   : 069  4107-7014 -> Raum 103
Stuttgart   : 0711 4107-7014 -> Raum 104
Essen       : 0201 474-1-474 -> Raum 105
Dortmund    : 0231 4741-1474 -> Raum 106
Karlsruhe   : 0721 500 79 79 -> Raum 107
Wuppertal   : 0202 44 868 44 -> Raum 108
Oberhausen : 0208 445 89 89 -> Raum 109
Solingen    : 0212 401-5-104 -> Raum 110
Rostock     : 0381 44 68 999 -> Raum 111
Luebeck     : 0451 38 94 999 -> Raum 112
```

In die "dreistelligen" Raeume kommt man auch mit *xxx#
also in Raum 100 mit *100# aber nur, wenn man sich
ueber die jeweilige Stadt eingewaehlt hatte.

Bedienhandbuch:

```
Hauptauswahl
============
1 Persoenliche Einstellungen
2 Suchmodus
3 Privatraum
4 Karussell     (Jungen und Mädchen werden zufällig zusammengeschaltet)
5 Raumwechsel: gefolgt von der Raumnummer 0 bis 9
6 17+4 (Blackjack)
7 Informationsmenue
8 Eigenes Postfach / oeffentliche Nachrichtenbretter
9 Ansage wieviele Leute im Raum sind
0


Informationsmenue
=================
1 Selbstbedienungshotline      (= Sex-Hotline)
2 Letzte 100 Anrufer
3 Raumliste
4 Zeitansage
5 Liste deiner Freunde
6
7 Anwesenheitsliste
8
9 Die Besten 10
0 Zurueck

Die Besten 10
=============
1 Die haeufigsten Anrufer
2 Die beliebtesten Teilnehmer
3
4
5
6
7
8
9
0 Zueueck


Persoenliche Einstellungen
==========================
1 Namen aufnehmen. Jeder sollte seinen Namen einsprechen.
2 Mailboxbegruessung aufnehmen (OGM).
3 Pool Login aufnehmen. Wird hoechstens einmal je Pool und Minute
abgespielt.
4
5
6
7 Pin aendern
8 Mailbox Adresse festlegen z.b. *GELLER# *55555# *LANY# ...
9
0 zurueck in die Konferenz
```

Suchmodus
=========
Nach Aktivieren des Suchmodus wird der Anrufer, der zuletzt
in den Pool kam automatisch ausgewaehlt. Ist ein Teilnehmer in seiner
Mailbox oder einem Menue, dann kann man ihn nicht finden.

123 Teilnehmer auswaehlen
4   Privatgespraech mit dem ausgewaehlten Teilnehmer (OP-Funktion)
5   Stummschalten (OP-Funktion)
6   Rauswerfen (OP-Funktion)
7   Namen und Stummschaltestatus abfragen
9   Quaelen/Trillerpfeife (OP-Funktion)
0   zurueck in die Konferenz

Chatmaster
==========
In den Pools 10 bis 30 kann man sich zum Chatmaster machen und
dadurch den Pool fuerr andere Teilnehmer sperren.
Anschliessend kann man ausgewaehlte Teilnehmer fue□r seinen Pool
freischalten, sodass sie den Pool betreten koennen.
Um seinen Pool ein wenig heimelig auszugestalten, kann man
ein Jingle aufnehmen, was jeder hoert, der den Pool betritt.

3   Chatmaster Status aufgeben = den Pool freigeben
4   Das Pool-Login aufnehmen.
0   zurueck in die Konferenz

*4*MAILBOX# Den Teilnehmer mit MAILBOX fuer seinen Pool freischalten
*6*MAILBOX# Den Teilnehmer mit MAILBOX aus seinem Pool entfernen

Anwesenheitsliste
=================
123 Durch die Teilnehmerliste gehen
4   Teilnehmer in seinen Pool einladen
5   Teilnehmer auf dem ausgewaehlten Kanal eine Nachricht schicken
6   Teilnehmer aus seinem Pool entfernen
9   Teilnehmer in die Buddyliste aufnehmen
0   zurueck in die Konferenz

*1# Zum ersten Kanal in der Liste springen
*3# Zum letzten Kanal in der Liste springen
*XXX# Einen Kanal direkt anspringen. Kanalnummer dreistellig.

Buddyliste
==========
123 Durch die Buddyliste gehen
4   Dem Buddy eine Nachricht schicken
5   Den Buddymodus an- oder ausschalten
6   Den Buddy aus der Liste loeschen
0   zurueck ins Infomenue

```
Mailbox / Bretter
=================
123 Nachricht auswaehlen
4   Nachricht beantworten (oeffentliche Antwort auf dem Brett)
5   Nachricht beantworten (private Antwort)
6   eigene Nachricht loeschen (OP: alle Nachrichten)
7   Informationen ueber die Nachricht abfragen (Absender, Zeit)
8   Ins naechste Brett springen
9   Absender in die Buddyliste aufnehmen
0   zurueck in die Konferenz

*1#  Zur aeltesten Nachricht springen.
*3#  Zur neusten Nachricht springen.
*43# Anklopfen an- oder abschalten.
     Wenn der Teilnehmer, dem man eine Nachricht senden moechte grade
online ist,
     und Anklopfen angeschaltet hat, dann spricht man ihm nicht auf die
Mailbox,
     sondern "klopft" bei ihm an.
     Er hoert dann alle 15 Sekunden ein Anklopfsignal und kann den Ruf mit
der
     Taste # annehmen und ein Privatgespraech fuehren.
*75# Buddymodus an- oder ausschalten

Alle Nachrichten werden nach einer bestimmten Anzahl von Tagen automatisch
geloescht. Die maximale Anzahl von Nachrichten, die Minimal- und
Maximallaenge
jeder Nachricht und eine Mindestpause zwischen zwei Nachrichten (Flooding)
wird vom System ueberwacht.
Wichtige persoenliche Nachrichten sollten nicht auf der Mailbox gespeichert
werden.

Allgemeine Stern-Raute Tastenkombinationen
==========================================
*00# bis *99# In einen der 99 Pools springen.
              Nur Pools 10-30 sind mit den Chatmasterfunktionen
abschliessbar.
*ADRESSE#     Nachricht an einen Teilnehmer schicken.
              Die Adresse (Sprachdomain) ist mindestens vierstellig.
              z.B. *4444# oder *XENA# (Vanity)
*ALT*NEU*NEU# Zugangsdcode aendern. Muss achtstellig sein.


Userlevel
=========
0 GAST     Zugangscode gesperrt
1 USER     normaler Zugangscode
3 OPERATOR Zugangscode mit zusaetzlichen Funktionen
```



Hier sind noch weitere Normaltariflines aus Deutschland.
Es gibt dabei nicht nur Chatsysteme, sonder auch Info-Ansagen, Radiosender denen man Telefon zuhören kann oder Live-Veranstaltungen die übertragen werden.

Service/Betreiber	Nummer	Kategorie	Website	Anmerkung
Deutscher Bundestag	030/ 22720018	Verantstal tungen	www.bundestag.de/	Bundestagsdebatten
Radio NRW	0208/ 8587444	Radio	www.radionrw.de/	Lokalradio aus NRW
RTL Berlin	030/ 88484333	Radio	www.rtl.de/	Live Radio aus Berlin
Spreeradio	030/ 23144456	Radio	www.spreeradio.de/	Live Radio aus Berlin
BITS	089/ 55988288	Vorlese-service		Videotext für Blinde. ARD, ZDF, BR
WDR Vera	0221/ 2726622	Info-service	www.wdr.de	Verkehrsfunkmeldungen aus NRW
Irrenhaus	040/ 18881010	Community	www.bbtel.de/	Virtuelle Welt/ virtual world
Chaos-Box vom CCC	040/ 40180131	Info-service	www.ccc.de/	div. Foren (nur 1 Leitung)
Funbox von W. Spallek	04551/ 967878	Community		div. Foren (nur 1 Leitung)
Phonecaster	0931/ 663927 + Pod-ID	Podcasts	www.phonecaster.de/	Podcasts am Telefon anhören. Pod-IDs auf der Website
Chat-House Berlin	030/ 74757677	Community	www.chathouse.tv/	diverse Talkräume
Lunes Revista	03635/ 492802	Community		wenig besucht
Fahrschule des Lebens	0708/ 4927744	Ansage-dienst	www.fahrschule-des-lebens.de	tägl. Wechselnde Lebensweisheiten
Partyline Leverkusen	0214/ 40404	Community	www.partyline-leverkusen.de/	max. 30 Teilnehmer
030chat Berlin 1	030/ 66664444	Community	www.030chat.de/	Virtuelle Welt/ virtual world
030chat Berlin 2	030/ 66664040	Community	www.030chat.de/	Virtuelle Welt/ virtual world
030chat Berlin 3	030/ 66664333	Community	www.030chat.de/	Virtuelle Welt/ virtual world

Telefonterror

Telefon-Terror Tutorial by outsiderz

1. Die benötigte Nr. "0800 - 76 26 000" (kostenlos!).
2. Nachdem man angerufen hat, kommt man in ein Telefonmenü. Nun gibt man "*" damit das Telefon auf Tonwahl überprüft wird. Wenn euer Telefon keine Tonwahl unterstützt geht einfach in eine Telefonzelle.
3. Bevor man sich erzählen lässt um was es sich bei diesem Fax-Angebot handelt, drückt man die "2" und überspringt das Ganze.
4. Jetzt muss man sich für eine Inforubrik entscheiden. Einfach mal "1" drücken, das sind AGB's, Anmeldeformular, etc.
5. Jetzt wird man aufgefordert die gewünschte Fax-Nr. einzugeben. Da es für Fax-Geräte keine automatische Erkennung oder eigens zugewiesene Nr. gibt, kann man jede Tel.Nr. der Welt eingeben.
6. Zum Ende dieses Gesprächs wiederholt das Gerät die angegebene Nr., um nun den Auftrag zu bestätigen gibt man die "1" ein. Sollte man sich vertippt haben, gibt man "3" ein um eine Korrektur vorzunehmen.
7. Auflegen

Anmerkungen: Wiederholt man diesen Vorgang bis zu 10x so wird die geschädigte Person für ca. 22 Std. belästigt. Die Belästigung erfolgt dadurch, dass alle 3 Min das Telefon klingelt. Nimmt die geschädigte Person ab so bekommt sie nur das übliche Fax-Geräusch zu hören. Nimmt die geschädigte Person nicht ab, so klingelt das Telefon 2 Min lang, bis der Anruf automatisch vom Netz beendet wird. Die Belästigungsdauer variiert von Anruf zu Anruf: 2x = 2 1/2 Std. Terror 10x = 22 1/2 Std. Terror.

Bonus: Das interessanteste hierbei, sobald die geschädigte Person 2 Std. Terror erhalten hat, wird sie so clever sein und den Stecker der Telefonbuchse ziehen. Der resultierende Effekt: Die Person ist nicht mehr erreichbar solange der Stecker gezogen bleibt, sobald aber der Stecker wieder eingesteckt wird, setzt der Terror dort ein wo er aufgehört hat und vollendet diesen. Das heißt: 10x angerufen, nach 2 Std. ausgesteckt, 5 Std. wieder eingesteckt, 20 Std. bis zur Vollendung, diese wird fortgesetzt

Und noch was: Dieser Service funktioniert nicht für Handys! Abgesehen von Talkline bietet auch O² einen solchen Service an (0800 - 55 222 77). Einfach mal ausprobieren

Written by outsiderz - Edited by p3pp3r

Nummergassen in Deutschland

Alle gültigen Vorwahlen und die evtl. damit verbundenen Kosten legt die Bundesnetzagentur fest

http://www.bundesnetzagentur.de/enid/5a9c5715d5d2605dfd9642b8ff441c7d,0/Nummernverwaltung/Uebersicht_Nummernraum_1hz.html

Der Nummernraum für das öffentliche Telefonnetz in Deutschland

- zusammenfassende tabellarische Darstellung -

Stand: 18.01.2006

Nummer bzw. Nummernraum	**Verwendung**	**Planungen**
0	nationale Verkehrsausscheidungsziffer	
00	internationale Verkehrsausscheidungsziffer	
010xy, 0100yy mit x = 1 ... 9 und y = 0 ... 9	optional der Verkehrsausscheidungsziffer vor-anzustellende Ziffernfolge zur Verbindungs-netzbetreiberauswahl Call-by-Call	
(0)11	frei	Reserve
(0)12	Innovative Dienste	
(0)13	frei; Ausnahmen:	soweit frei: Reserve
(0)137	- Televotum, Teledialog	Verlagerung geplant; danach Reserve
(0)14	frei	Reserve
(0)15*)	Mobilfunk (GSM und UMTS/IMT-2000):	
(0)1505	Group3G (Quam)	
(0)1511	T-Mobile	
(0)1515	T-Mobile	
(0)1520	Vodafone	
(0)1566	MobilCom	
(0)1570	E-Plus Mobilfunk GmbH & Co. KG	
(0)1577	E-Plus Mobilfunk GmbH & Co. KG	
		Reservierungen: (0)150 Group 3G (0)151 T-Mobile (0)152 Vodafone (0)155 E-Plus 3G Luxb. (0)156 MobilCom (0)157 E-Plus (0)159 O2 (Germany)

Nummer bzw. Nummernraum	**Verwendung**	**Planungen**
(0)16*)	Mobilfunk:	
(0)160	T-Mobile	
(0)161	frei	Reserve
(0)162	Vodafone	
(0)163	E-Plus Mobilfunk	
(0)164	e*message (Funkruf)	
(0)165	frei	Reserve
(0)166	e*message (Funkruf)	
(0)167	Bündelfunknetze:	
(0)1672	Dolphin Telecom (Deutschland)	
(0)168	e*message (Funkruf)	
(0)169	e*message (Funkruf)	
(0)17*)	Mobilfunk (GSM und UMTS/IMT2000):	
(0)170	T-Mobile	
(0)171	T-Mobile	
(0)172	Vodafone	
(0)173	Vodafone	
(0)174	Vodafone	
(0)175	T-Mobile	
(0)176	O2 (Germany)	
(0)177	E-Plus Mobilfunk	
(0)178	E-Plus Mobilfunk	
(0)179	O2 (Germany)	
(0)180	Shared Cost-Dienste	
(0)181xxx, (0)181xxxx	Kennzahlen für Internationale Virtuelle Private Netze (IVPN)	
(0)18xy, (0)18xyy, (0)18xyyy, (0)18xyyyy, (0)18xyyyyy, (0)18xyyyyyy mit x = 2 ... 9 und y = 0 ... 9	Kennzahlen für geschlossene Nutzergruppen	

Nummer bzw. Nummernraum	**Verwendung**	**Planungen**
(0)19	frei; Ausnahmen:	soweit frei: Reserve
(0)190	- bis 30.06.2006: kostenlose Bandansage (Hinweis auf Premium Rate-Dienst in anderem Nummernbereich)	ab 01.07.2006: Reserve
(0)19xz, (0)19yzzz mit x = 1 ... 3, y = 1 ... 4 und z = 0 ... 9	- Online-Dienste	
(0)1987	- Routingnummern für Rufnummern der Struktur 116xyz	
(0)1988	- Zielnetzbetreiberkennungen zur Generierung von Routingnummern für Internationale entgeltfreie Mehrwertdienste	
(0)1989	- Routingnummern für Auskunftsdienste	
(0)199	- Netzinterne Verkehrslenkung	
(0)xy, (0)xyy, (0)xyyy, (0)xyyyy mit x = 2 ... 9 und y = 0 ... 9	Ortsnetzkennzahlen (ONKz); Ausnahmen:	
(0)31	- Testrufnummern	
(0)31-0	- Test der Betreiberauswahl und der Betreibervorauswahl bei Fernverbindungen	
(0)31-1	- Test der Betreiberauswahl und der Betreibervorauswahl bei Ortsverbindungen	
(0)32	- Nationale Teilnehmerrufnummern	

Da die ONKZ von einer Behörde zugewiesen sind, findet sich auf der Webseite der Bundesnetzagentur eine umfangreiche Datenbank mit allen Gemeinden Deutschlands und deren Vorwahl.
Diese DB wird jährlich aktualisiert und umfasst in der aktuellen Version von 2005 über 20.000 Einträge.
Es gibt aber weitaus weniger Ortsnetze, denn die Datenbank ist nach dem offiziellen Gemeindeschlüssel als Primärschlüssel aufgebaut. Dadurch wird fast jede Gemeinde in Deutschland aufgeführt, auch wenn sie als Stadtteil zu einer Stadt eingemeindet wurde.

Der direkte Link auf die Seite lautet
http://www.bundesnetzagentur.de/enid/05c5ad5cc6fef42128264301e703dda7,0/Ortsnetze/Verzeichnisse_1gg.html

Nummer bzw. Nummernraum	**Verwendung**	**Planungen**
(0)500, (0)501	- frei	Reserve für Telekom-munikationsdienste
(0)600	- ONKz	bei Bedarf freizuräumen
(0)601	- frei	Reserve
(0)700	- Persönliche Rufnummern	
(0)701	- frei	Reserve für Persönliche Rufnummern
(0)800	- Freephone Dienste	
(0)801	- frei	Reserve für Freephone Dienste
(0)900x mit x = 1, 3 und 5	- Premium Rate-Dienste	
(0)9009	- Registrierungspflichtige Anwählprogramme	
(0)901, (0)902, (0)903, (0)904, (0)905	- frei	Reserve für Telekommunikationsdienste
xyy (auslaufend), xy yy (auslaufend), x yy yy, xy yy yy, x yy yy yy, xy yy yy yy mit x = 1 ... 9 und y = 0 ... 9	Teilnehmerrufnummern; Ausnahmen:	
110	- Polizei	
112	- Notruf, Feuerwehr	
116 116	- Sperrrufnummer für elektronische Berechtigungen	
118xy mit x = 1 ... 9 und y = 0 ... 9 1180yy	- Auskunftsdienste	Rufnummern der Struktur 1180yy werden nur zugeteilt, wenn keine Rufnummern der Struktur 118xy mehr verfügbar sind
übrige Bereiche der Gasse 11	- netzinterne Nutzung	

*) In den Nummernbereichen (0)15, (0)16 und (0)17 sind die Zuteilungsnehmer von Rufnummernblöcken (RNB) angegeben. Aufgrund der gesetzlichen Verpflichtung zur Netzbetreiberportabilität in Mobilfunknetzen können Rufnummern aus diesen RNB von anderen Mobilnetzbetreibern betrieben werden.

Colorboxen

Es gibt verschiedene Schaltungen die man bauen kann um besser phreaken zu können. Solche Schaltungen nennt man Box(en). Anschließend findest Du die bekanntesten Boxnamen aufgelistet. Zu jeder gibt es im Netz mindestens zwei Txts mit Bauanleitungen. Allerdings sind die meisten in Englisch und auch nicht im deutschen Telfonnetz möglich. Es gibt neben diesen noch zahlreiche andere Boxen aber diese sind wohl die „gebräuchlichsten".
Wenn Du dir die Anleitungen zu einzelnen Boxen durchliest wirst Du auf Schaltpläne stoßen die wie gesagt meist nicht für das Deutsche oder Europäische Telefonnetz zutreffend sind. Die Widerstandsgrößen und die Größen der anderen Bauelemente müssen daher vielleicht neu berechnet werden. Die meisten Schaltungen sind allerdings mit Angaben über Ein- und Ausgangsspannung und vielleicht sogar mit eine Größenangabe über den Strom versehen. So kannst Du ganz leicht mit Hilfe des ohmschen Gesetzes und einen paar elektronischen Grundrechenregeln die Schaltung neu berechnen.
Wenn Du damit nicht klar kommst, nimm einfach die gegebenen Werte und probiere etwas herum. Ich weise hier allerdings noch mal daraufhin das es verboten ist an das Telfonnetz eigenwillig Schaltungen anzuklemmen.

SILVER Box.....[DTMF Töne für A, B, C und D erzeugen]
Noch möglich, aber in D'land nutzlos
GOLD Box.....[Umleiten von ausgehenden Anrufen]
CHROME Box.....[Manipulierung des Trunks über eine Fernbedienung]
CHARTREUSE Box.[Stromes der Telefonleitung nutzen]
BROWN Box.....[Partytelefonieren über zwei Leitungen Konferenzschaltg.]
BLACK Box.....[Der Anrufer bezahlt nix, *in BRD nicht mgl. da digitale VST.]*
BEIGE Box.....[Anzapfen einer Leitung mit nem Umbautelefon]
BLUE Box.....[Simuliert einen 2600Hz Ton um VST zu kontorlieren US]
Funktioniert nirgends mehr
BLAST Box.....[Mikrofonverstärker für die Sprechmuschel]
COLOR Box.....[aktives Aufnehmen der Telefongespräche]
DARK Box.....[Umleiten An- und Abgehender Rufe auf ein anderes Telefon]
DAYGLO Box.....[Anzapfen eines zweiten Telefons]
DLOC Box.....[Konferenzschaltung über zwei Telefonleitungen]
GREEN Box.....[Simulieren eines Geldeinwurfs, Geldrückgabe .. US]
Auch schon längst antiquiert

JACK Box.....[DTMF Telefonumbau]
RAINBOW Box....[VST Zerstören mit 220/120V auf der Leitung]
PARTY Box.....[Konferenzschaltung über 2 Leitungen]
PEARL Box.....[Ton Generator]
RED Box.....[Kostenlos aus einer Telefonzelle telefonieren mit Tönen US]
Schön wärs, funktioniert aber nicht mehr
ROCK Box.....[Musik auf der Telefonleitung übertragen]
LUNCH Box.....[Ein AM-Funksender für Empfangen und Senden]
WHITE Box.....[Transportabler DTMF Geber]
OLIVE.....[Eine externe Klingel]
BUSY Box.....[Sperrt die Wähltöne und der Anrufer hört ein Besetztzeichen]
BUD Box.....[Anonymes Telefonieren durch anzapfen der Line (BeigeBox)]
AQUA Box.....[Schutz gegen Rückerverfolgung, Selber Rückverfolgen US]
Naiv, funktioniert heute längst nicht mehr
NOISE Box.....[Erzeugen eines Leitungsgeräusches]
MAUVE Box.....[Anzapfen einer Leitung durch auftrennen einer Leitung]
TRON Box.....[Umdrehen der Phasen im Hausanschluss - Zeiger dreht langsam]
Lächerlich….
TAN Box.....[Telefongespräche aufzeichnen]
URINE Box.....[kapazitive Störung der Telfonleitung beim Läuten ..]
YELLOW Box.....[Zufügen eines weiteren Telefons]
STATIC Box.....[Hochhalten der Leitungsspannung]
MAGENTA Box....[Verbinden einer entfernten Leitung mit einer anderen US]
VIOLET Box.....[Auflegen über die Telfonzelle]
CHEESE Box.....[Verbindung zweier Telefone um eine Umleitung zu schaffen]
TBUSTA Box.....[nach Anruf von Nummer wieder ein Freizeichen über BeigeBox]
NEON Box.....[Externes Mikrofon am Telefon]

Mythen, Horaxes, Unfug

1. Die verschiedenen Farbboxen, mit denen man umsonst telefonieren könne soll, funktionieren in Deutschland des 21. Jahrhunderts nicht mehr!!!

2. Wenn man die +4911 vor einer Rufnummer mit Ortsvorwahl wählt, kann man höchstens umsonst mit dem Bullen reden. Kostenlose Gespräche vom Handy aus sind damit unmöglich.
   Denn statt 0049-**11-0**30-4567496 kann man auch direkt 110 wählen.

3. Wenn man vergisst den Telefonhörer aufzulegen, kommt niemand mehr von der Post vorbei und man bekommt auch beim notorischsten Nicht-Auflegen keine Strafe aufgebrummt. Das war zu Zeiten der analogen Vermittlungstechnik bis zu den 1990er Jahren so. Heute ist das sowohl der Vermittlungsstelle als auch der Telefongesellschaft egal, was ihr mit eurem Hörer macht.

4. Fast leere Telefonkarten lassen sich nicht in der Mirkowelle wieder aufladen. Dabei geht mindestens die Karte kaputt, wenn nicht sogar Muttis Mirkowellenofen.

Hotlines

Bei der Telekom
www.telekom.de

Technische Hotline (Störungsannahme)	0800-33302000
Kaufmännische Hotline (Beratung & Verkauf)	0800-33301000
Garantie-Hotline	0180-51990
IT-Service-Line	0800-3308300

Bei Arcor
www.arcor.de

Privatkunden Hotline	0181-070010
Privatkunden Fax	0181-070011
Geschäftskunden Hotline	0800-2726775
Technische Hotline für Internet By Call und PIA-Dienste	0900-1070200

Bei Alice (HanseNet)
www.hansenet.de

Info-Hotline	0800 – 4110411

Bei Versatel

www.versatel.de

Privatkunden	0800 – 888 888 3
Geschäftskunden	0800 – 80 40 200
Internet Support	01805 - 66 10 44 (12 ct./ Min.)
Rechnungsfragen	01805 - 777 447 8 (12 ct./ Min.)
Support Allgemein	01805 - 040 40 30 (12 ct./ Min.))
Entstörung	
Berlin:	0800 - 70 500 700
Schleswig-Holstein:	0800 - 90 90 099
Nordrhein-Westfalen:	0800 - 88 88 88 4
Baden-Württemberg:	0800 - 823 0 823

TROPOLYS Hotlines

(Carrier, die von Versatel aufgekauft wurden)

chemtel

0371 489 40 00	PK-Kunden-Hotline ChemTel
01805 999019	Internet-Hotline ChemTel
0371 489 11 11	Störungs-Hotline ChemTel

citykom

01805 227805	PK-Hotline citykom
01805 227705	GK-Beratung citykom
0251 9874172	GK-Störungs-Hotline citycom

cne

01805 227803	PK-Hotline cne / meocom
01805 227703	GK-Beratung cne / meocom
0201 1855855	GK-Störungs-Hotline cne

ddkom

0351 48229 99	PK-Kunden-Hotline ddkom
01805 99039	Internet-Hotline ddkom
0351 48226 26	Störungs-Hotline ddkom

jetz

03641 505 505	PK-Kunden-Hotline jetz
01805 3894453	Internet-Hotline jetz
03641 505 555	Störungs-Hotline jetz

maineotk

01805 227807	PK-Hotline maineotk
01805 227707	GK-Beratung maineotk
069 25493 777	GK-Störungs-Hotline maineotk

mainzkom

01805 227808	PK-Hotline mainzkom
01805 227708	GK-Beratung mainzkom

meocom

01805 227803	PK-Hotline cne / meocom
01805 227703	GK-Beratung cne /meocom
0208 9409090	GK-Störungs-Hotline meocom

pulsaar

01805 227 802	PK-Hotline pulsaar
01805 227702	GK-Beratung pulsaar
069 21789 254	GK-Störungs-Hotline pulsaar

telebel

01805 227801	PK-Hotline telebel / telelev
01805 227701	GK-Beratung telebel / telelev
0202 9798000	GK-Störungs-Hotline telebel

telelev

01805 227801	PK-Hotline telebel / telelev
01805 227701	GK-Beratung telebel / telelev
0214 3103232	GK-Störungs-Hotline telelev

tnp

0331 62 00 866	PK-Kunden-Hotline tnp
01805 999029	Internet-Hotline tnp
0331 62 00 888	Störungs-Hotline tnp

Supermarktfinder
Keine Tiefkühlpizza und Cola mehr??

real,-	www.real.de	0800-7358350
extra	www.extra.de	0800-3987262

R-Gespräche
Unter R-Gespräch wird allgemein "ein Telefongespräch, bei dem der angerufene Teilnehmer das Entgelt übernimmt" verstanden. R-Gespräche sind in Deutschland grundsätzlich zulässig. Insbesondere aus telekommunikationsrechtlichen Vorgaben ergibt sich kein Verbot dieser Dienstleistung. R-Gespräche werden von mehreren Unternehmen angeboten

0800 0800 108	-	T-Com
0800 4411 333	-	R-Talk

Telefonauskunft

Rufnummern für Telefonauskunftsdienste (Stand: 20.06.2006) wurden wie folgt vergeben:

Unternehmen	Rufnummern für Auslandsauskunft	Rufnummer für Inlandsauskunft
01030 Telecom GmbH Leopoldstraße 16, 40211 Düsseldorf		**11897**
01058 Telecom GmbH, Leopoldstraße 16, 40211 Düsseldorf		**11858** **11894**
01051 Telecom GmbH Robert-Bosch-Straße 1, 52525 Heinsberg		**11827** **11828** **11856**
1-2-3 Multimedia GmbH Graf-Adolf-Straße 73, 40210 Düsseldorf		**11876**
1 18 18 Auskunft GmbH Schleefstraße 2d, 44287 Dortmund		**11818**
11840 Voice-Commerce GmbH Isaac-Fulda-Allee 5, 55124 Mainz		**11840** **11838**
11844 Auskunftsdienste GmbH Crusestraße 8, 47441 Moers		**11844**
11883 Telecom GmbH, Girmes-Kreuz-Straße 55, 41564 Kaarst	**11831**	**11883** **11893**
11899 Auskunft Service GmbH, Mexikoring 33, 22297 Hamburg		**11899**
A.Ahlers Ltd. & Co.KG Friedrich-Ude-Str. 7, 65812 Bad-Soden		**11865**
AOL Deutschland GmbH & Co.KG Beim Strohhause 25, 20097 Hamburg		**11842**
Arcor AG & Co.KG Alfred-Herrhausen-Allee 1, 65760 Eschborn		**11870** **11888**
Auskunft 24 AG Eckdrift 107, 19061 Schwerin		**11824** **11850** **11851**
BeDe Werbeagentur GmbH Brandsende 2-4, 20095 Hamburg		**11846**

Beate Uhse new media GmbH Am Pferdewasser 10, 24937 Flensburg		**11816**
CNS 24 AG Leipziger Straße 42, 04860 Torgau		**11825**
DB Dialog Telefonservice GmbH Solmsstraße 71, 60486 Frankfurt		**11861**
der heiße Draht Verlagsgesellschaft mbH & Co.KG Drostestraße 14-16, 30161 Hannover		**11852** **11866** **11868**
Deutsche Telekom AG, In der Ruste 20 - 22, 53113 Bonn	**11834**	**11833** **11836** **11837** **11864**
dtms Deutsche Telefon- und Marketing Services AG Isaac-Fulda-Allee 5, 55124 Mainz		**11814** **11821** **11839** **11841** **11853**
Eura Tel GmbH Georgiring 1-3, 04103 Leipzig		**11832**
First Early Bird GmbH, Zeughausgasse1, CH-630 Zug	**11813**	
FRED 11811 Services GmbH & Co KG Beim Strohhause 31, 20097 Hamburg		**11811**
info-portal GmbH Gützower Landstraße 36-40, 17489 Greifswald	**11882**	**11849** **11881** **11889**
IN-telegence GmbH & Co.KG Oskar-Jäger-Straße 125, 50825 Köln		**11847** **11862** **11863**
KielNet GmbH Preußer Straße 1-9, 24105 Kiel		**11843**
klickTel AG Martin-Luther-Str.1, 46284 Dorsten		**11815** **11898**
Mega Satellitenfernsehen GmbH, Rüsselsheimer Str. 22, 60326 Frankfurt		**11867** **11871** **11873**
mobilcom Communikationstechnik GmbH Tiergartenweg 1, 24837 Schleswig	**11829**	**11819**
mobile live GmbH Zollhof 17, 40221 Düsseldorf		**11857**

MR.NET services GmbH & Co. KG Fördeprommenade 16, 24944 Flensburg		**11879**
NEXT ID GmbH Willi-Brandt-Allee 20, 53113 Bonn		**11826** **11848** **11891** **11895**
Orion Versand GmbH & Co. KG Schäferweg 14, 24941 Flensburg		**11854**
SNT Multiconnect GmbH & Co. KG Wilhelm-Hale-Straße 50, 80639 München	**11878** **11820**	**11835**
Telegate AG, Fraunhofer Str.12a, 82152 Martinsried b. München	**11890**	**11877** **11880** **11887**
telomax GmbH Robert-Koch-Straße 37, 55129 Mainz		**11859**
TELIX AG, Landsbergerstr. 110, 80339 München		**11810** **11884** **11886**
TellVis Service GmbH Beckumer Straße 34, 59229 Ahlen		**11860**
T.L.I.n.v. Burgemeester Kenisstraat 1, 2910 Essen in Belgien		**11892**
Translease International Ltd. Dublin		**11896**
Twentyfourseven GmbH, Kruppstraße 92-100, 45145 Essen		**11845**
Ventelo GmbH, Matthias-Brüggen-Straße 55, 50829 Köln	**11823**	**11822**
Vodafone D2 GmbH, Am Seestern 1, 40547 Düsseldorf		**11872**
VoiceWebOne AG Kurfürstenanlage 36, 69115 Heidelberg		**11885**
Yellow Access Operating Services AG, Mürtschenstraße 25, CH-8048 Zürich		**11855**

Abkürzungen

AB	Anrufbeantworter
ADM	Außendienstmitarbeiter
APL	Abschlusspunkt Linientechnik
AsB	Anschlussbereich
AWD	Anrufweiterschaltung
CLIP	Caller's Line Identification Presentation (Rufnummernanzeige)
CLIR	Caller's Line Identification Restriction (Rufnummernuntedrückung)
CLNS	ConnectionLess Network System
CONS	Connection Orientated Network System
DA	Doppel-Ader
DECT	Digital Enhanced Cordless Telecommunications (Digitale, verbesserte schnurlose Telekommunikation; bis 1995 *Digital European Cordless Telecommunications*
DSL	Digital Subscriber Line (digitale Teilnehmeranschlussleitung)
DSLAM	DSL Accesss Multiplexer
DTAG	Deutsche Telekom AG
DTMF	Dual Tone Multi Frequenz
EG	Endgerät
ERNA	Elektronische RufnummNummern Ansage
EVN	EinzelVerbindungsNachweis
EVz	Endverzweiger
GAP	Generic Access Profile
HVt	Hauptverteiler
IAE	ISDN-AbschlussEinheit
IP	Internet Protokoll
ISDN	Integrated Services Digital Network (integrierte Dienste im digitalen Netz)
KVz	Kabelverzweiger
LM	Leistungsmerkmal
MSN	Multisubscriber Number
PIN	Persönliche Identifikations- Nummer
PUMA	Prüfen Und Messen im Außendienst
SEPT	System Externe Prüf-Technik
TAE	Telekommunikations-AnschlussEinheit
TAL	Teilnehmer-Anschluss-Leitung
UAE	Universal-AnschlussEinheit
ÜVt	Übergabeverteiler
YIPL	Youth International Party Line

Links

http://www.phreak.de/infos/german/index.html
Viele Phreaking-Tutorials, aber oftmals veraltet

http://www.trust-us.ch/ccc2/index.php
Hacker und Phreaker Archiv

daraus
http://www.trust-us.ch/isdn_dipl/index.html
Oliver Ferreau - Sicherheit im ISDN (Diplomarbeit April - Oktober 1997)

http://www.informatik.fh-kl.de/~zitt/telefon.htm
Hubert Zitt im Internet- Das kleine Telefon-Werkbuch

Wissensquellen sind
www.google.de
www.wikipedia.de

