Radio-Hacken — Datenreisen durch den Äther

Spionage mit dem Kurzwellenradio

Gedämpftes Licht überall. Ein Mann mit Kopfhörer sitzt vor einem Computer, daneben ein Radio. Seltsames Quietschen und Pfeifen ist vernehmbar. Plötzlich — rhythmisches Piepsen übertönt alles. Der Mann drückt ein paar Tasten, und seltsame Zeichenfolgen erscheinen auf dem Bildschirm. Je länger der Text wird, desto klarer der Inhalt: Der Computer entschlüsselt eine Fahndungsmeldung.

Das ist keine Zukunftsmusik, sondern eine von fast jedem Amateurfunker und Computer-Freak durchführbare Szene. Und sie ist vor einiger Zeit ähnlich passiert. Der Vorfall ging eine Weile durch die Presse. Auch empfing ein Amateurfunker geheime Sendungen von Interpol. Wie ist so etwas möglich?

Im Zeitalter der Datenfernübertragung über Telefon und Glasfaser

Streng geheime Botschaften, neueste Nachrichten, Wetterkarten — all das wird über Kurzwelle gesendet. Wußten Sie, daß Sie Ihren Computer zur Entschlüsselung dieser Signale einsetzen können?

ist eine Art der Kommunikation fast schon in Vergessenheit geraten — der Funk. Jahrzehntelang war der einzige Weg, mit weit entfernten Ländern, Schiffen oder Flugzeugen Verbindung aufzunehmen, das Morsen. Auch heute noch werden Nachrichten und Daten mit Hilfe von Morsezeichen rund um den Erdball verschickt. Natürlich übernimmt der Computer die Aufgabe des Morsens. Was liegt also näher, als diese Signale wieder mit dem Computer sichtbar zu machen?

Dazu brauchen Sie keine große Ausrüstung. Die Grundausstattung besteht aus einem Heimcomputer (sehr gut eignet sich der C 64), einem Radio mit SSB-Teil (Einseitenband) oder einem BFO (Beat Frequency Oscillator, das sind spezielle Sende- und Empfangstechniken. In der Bedienungsanleitung steht, ob Ihr Radio diese Funktionen besitzt.) sowie einer guten Antenne. Aber auch Omas altes Dampfradio eignet sich als Empfänger, Hauptsache, er besitzt ein Kurzwellenempfangsteil. Am wichtigsten ist eine gute Antenne, denn der Computer erzeugt einen so hohen Störpegel, daß ein Empfang mit der eingebauten Antenne selten oder nicht möglich ist. Aber schon ein langer Draht (quer durchs Zimmer gespannt) bringt gute Ergebnisse. Nachts ist der Empfang am besten.

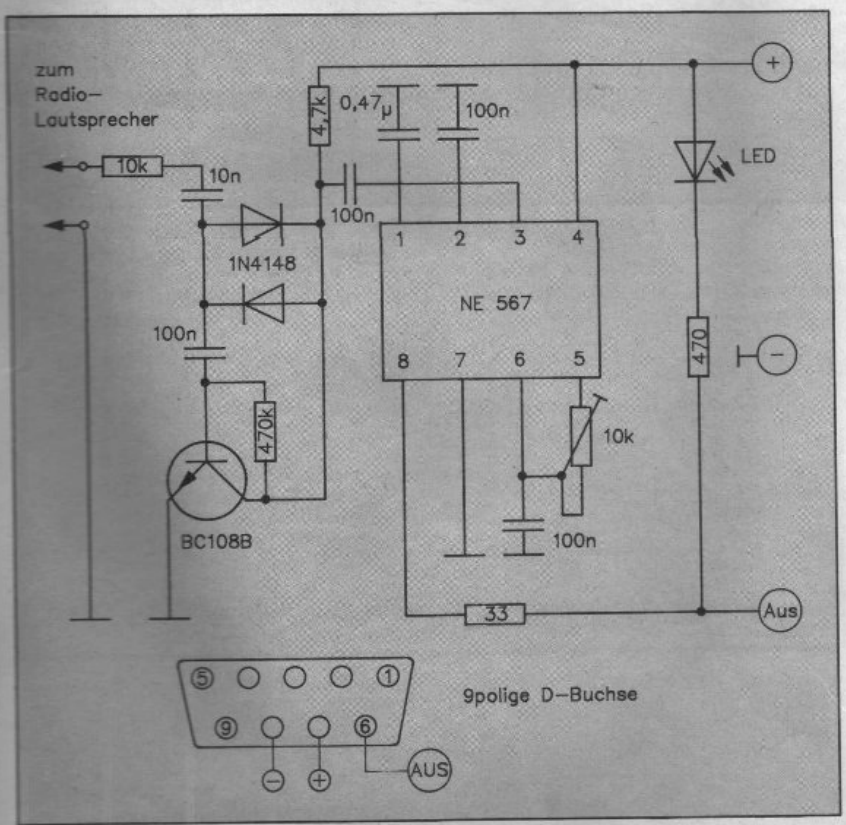
Was jetzt noch fehlt, ist ein Decoder, der die empfangenen Signale für den Computer umsetzt. Wir bieten Ihnen in diesem Beitrag eine Bauanleitung für einen solchen Decoder. Die Schaltung und das Programm ist für den C 64 ausgelegt. Prinzipiell kann diese Schaltung an jeden Computer mit Joystick-Port angeschlossen werden. Das Basic-Programm ist so allgemein gehalten, daß lediglich zwei Programmzeilen für den Einsatz auf einem anderen Computer geändert werden müssen. Dazu aber später mehr.

Bevor es ans Basteln geht, wollen wir einmal die verschiedenen Betriebsarten, die es in der Funkerei gibt, näher betrachten. In den Klammern finden Sie die gängigen Abkürzungen für die Betriebsarten.

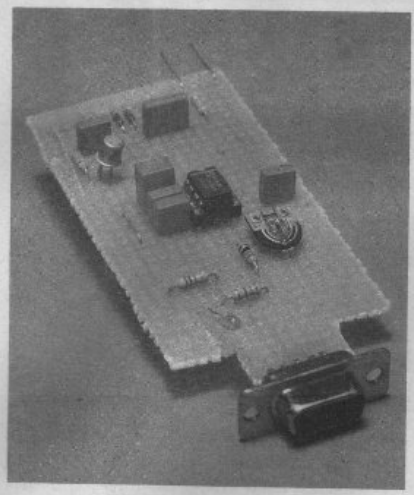
Morsen (CW): Morsen ist nach Sprechfunk immer noch die häufigste Betriebsart und auch völlig unkompliziert zu decodieren. In unserer Bastelanleitung beschränken wir uns auf den Empfang solcher Sendungen.

Funkfernschreiben (RTTY): Die interessantesten Funkdienste arbeiten in RTTY (Botschaften, Militär, Polizei, Presse).

Faksimile (FAX): FAX wird zur Bildübertragung benutzt, beispielsweise Pressebilder und Wetterkarten.



Mit dieser Schaltung bauen Sie einen Decoder, der die Morsezeichen für den Computer umsetzt. Beim C 64 ist keine Batterie notwendig.



Fertig aufgebaut und verdrahtet sieht die Schaltung etwa so aus

Schmalbandfernsehen (SSTV): Das ist eine speziell für den Amateurfunkdienst entwickelte Betriebsart, um Bilder zu übertragen. Es gibt noch einige aufwendigere (und damit übertragungssichere) Betriebsarten, die bei der Übertragung von Fernschreiben Verwendung finden.

Wenn Sie jetzt noch eine gute Frequenzliste besitzen (aus Fachbüchern, beispielsweise die KW-Spezial-Frequenzliste 87/88 vom Siebel Verlag oder von Amateurfunkern), so ist der Erfolg vorprogrammiert.

Mit geeigneten Programmen können Sie die Texte von Nachrichten-

```
CQ CQ CQ DE DDH47 147. KHZ DDH9 11039 KHZ
CQ CQ C* DE DDH47 147. KHZ DDH9 11039 KHZ
NW* BAWJADE-WESERMUENDUNG. LOTSE. RSETZ
DIENST ZEITWEILIG BEI LEUCHTTONNE 17. WES
ER. 221600 UTC DEC. 86 NAVIGATIONAL WARNI
NG NO.603 JADE-WESER EASTUARY. PILOTAGE T
EMPORAR* IN VICINITY OF LIGHTBOUY 17. WES
ER. 222150 UTC DEC. 86 NAUTISHE WARNNACHR
ICHT NR 604. BAW ELBEMUENDUNG. LOTSENVERS
ETZDIENST ZEITWEILIG BEI LEUCHTTONNE 9. 2
22150 UTC DEC. 86 NAVIGATIONAL WARNING NO
. 604 ESTUARY . PILOTAGE TEMPORARILY IN V
ICINITY OF LIGHTBOUY 9 = 230800 + DDH47/D
DH9 E SK **
```

Für Süddeutsche sicher geheimnisvoll: Beispiel einer Morse-Meldung

agenturen (beispielsweise TASS aus der Sowjetunion) in RTTY (also Funkfernschreiben) mitlesen, die Wetterkarten (FAX) des Deutschen Wetterdienstes analysieren oder den Wetterbericht für die Nordsee (CW) im Klartext lesen. Vielleicht gelingt es auch einmal, Bilder (SSTV) einer Amateurfunkstation aus den USA zu sehen (natürlich nur, wenn Sie über geeignete Programme verfügen).

Immer mehr Funkdienste verschlüsseln ihre Aussendungen. Einige Schlüssel sind zugänglich, wie SYNOP oder METAR bei den Wetterfröschen. Ein weiteres Problem sind russische oder arabische Stationen. Hier empfängt man leider nur unverständliches Kauderwelsch, denn die Software ist nur für den ASCII-Code ausgelegt.

Beim Empfang können die Störungen des Computers die Decodierung erschweren oder gar unmöglich machen. In solch einem Fall nehmen Sie die Signale auf einer Kassette auf. So können Sie dann die Signale ohne Störgeräusche des Computers einlesen. Vergessen Sie danach nicht, die Kassette zu löschen. Es könnte ja sein, daß Sie Signale aufgezeichnet haben, die nicht für die Öffentlichkeit gedacht sind.

Diejenigen, die jetzt schon anfangen möchten, Radio zu hacken, geben das kurze Basic-Programm ein. Die Zeilen 10 und 300 passen Sie an Ihren Computer an (Zeile 10 löscht den Bildschirm und Zeile 300 ist die Abfrage des Feuerknopfes).

Morsezeichen für Neugierige

Nach dem Starten des Programms wird das Betätigen der Feuertaste als Morsen interpretiert und auf dem Bildschirm ausgegeben. Aber erst mit der Schaltung (PLL-Tondecoder) und einer starken Station wird es richtig interessant. Wunder dürfen Sie sich allerdings von so wenig Aufwand nicht erhoffen. Aber das Programm kann sauber gegebene Morsezeichen bis etwa 90 Buchstaben pro Minute mitschreiben. Mit der Variablen P kann die Geschwindigkeit geändert werden.

```
10 PRINT "□":REM BOB'88
20 P=2:B=2*P:W=4*B:C=1
30 C$=" ETIANMSURWDKGOHVF£L£PJBXCYZQ£££54£3£££2ÉÈ+££££16=/'£££££7£££8£90"
40 I=0:N=0
50 GOSUB300:IF A$="" THEN N=N+1
60 IF N>B THEN 140
70 GOSUB300:IF A$="" THEN 50
80 GOSUB300:IF A$<>"" THEN I=I+1
90 IF I=0 THEN 80
100 GOSUB300:IF A$<>"" THEN 80
110 C=C+C
120 IF I>P THEN C=C+1
130 GOTO 40
140 IF C>63 THEN PRINT "£";:GOTO 160
150 PRINT MID$ (C$,C,1);
160 C=1:I=0
170 GOSUB300:IF A$="" THEN N=N+1
180 IF N>W THEN PRINT " ";:GOTO 80
190 GOSUB300:IF A$<>"" THEN 80
200 GOTO 170
300 A$="":IF PEEK(56320)=111THENA$=" "
310 RETURN
```

Dieses kurze Basic-Programm übernimmt die Decodierung auf dem C 64

Nun zur Hardware. Ein spezieller Baustein setzt die Signale, die aus dem Radio kommen, in für den Computer verständliche Werte um. Die Schaltung findet auf einer kleinen Lochrasterplatine Platz. Die Verdrahtung der Bauteile erfolgt mit etwas Schaltdraht nach dem Schaltplan. Die Stromversorgung übernimmt der C 64. Bei anderen Computern übernimmt eine 4,5-Volt-Taschenlampenbatterie diese Aufgabe. Der Decoder wird mit dem Radio (Lautsprecher- oder Kopfhörerausgang) verbunden. Nachdem Sie einen starken Sender eingestellt haben, verdrehen Sie den Trimmer auf der Platine so lange, bis die Leuchtdiode im Takt der Morsesignale leuchtet.

Radio-Hacken und die Post

Wie sollte es anders sein — auch hier hat die Post etwas zu sagen. Nach dem Fernmeldeanlagengesetz (FAG) dürfen Sie nicht einfach irgendwelche Funkdienste abhören, auswerten oder etwa aufs Tonband aufnehmen. Als Normalbürger dürfen Sie nur die Rundfunksender und den Amateurfunkdienst empfangen. Besitzen Sie eine Amateurfunklizenz, dürfen Sie zusätzlich noch sogenannte »CQ-Aussendungen« empfangen (meist Wettermeldungen und Zeitzeichen). Deshalb darf man die Empfangsversuche nicht im Geltungsbereich der Deutschen Bundespost machen oder seine Ergebnisse nicht veröffentlichen, das heißt Dritten zugänglich zu machen. Auf gut deutsch heißt das: Hängen Sie solche Versuche nicht an die große Glocke. Denn im Fernmeldeanlagengesetz lautet ein Absatz etwa sinngemäß: Empfängt man »zufällig« Funkdienste, die nicht für die Allgemeinheit freigegeben sind, so darf man sie weder aufzeichnen, ihren Inhalt weitergeben, sie auswerten, noch über ihre Existenz sprechen. Dazu noch eine nette Geschichte: Interpol übermittelte die Anschrift und die Telefonnummer einer verdächtigen Person über Funk an andere Dienststellen,

Hier noch einige interessante und starke Frequenzen:			
4489.0 kHz	Bracknell/England	SYNOP	RTTY 50 BAUD
4785.5 kHz	Köln-Wahn	METAR	RTTY 50 BAUD
147.3 kHz	Quickborn	Wetter	CW
9230.0 kHz	TASS/UdSSR	Presse	RTTY 50 BAUD
14364.0 kHz	XINHUA/China	Presse	RTTY 50 BAUD
4062.0 kHz	Frankreich	Polizei	CW
7504.0 kHz	England	US Navy	CW
+-3735 kHz		Amateurfunk	SSTV
+-14230 kHz		Amateurfunk	SSTV

Amateurfunkbänder:

3500 - 3800 kHz
7000 - 7100 kHz
14000 - 14350 kHz
21000 - 21450 kHz
28000 - 29700 kHz

Im 2-Meter-Band auf 144,675 MHz gibt es eine neue, aber nur von den Amateurfunkern verwendete Betriebsart. Sie heißt Packet Radio. Hier ist ein Verkehr von Computer zu Computer möglich, ähnlich wie bei Modemverkehr über das Telefon. Es sind auch Mailboxen installiert, die über Funk mit 1200 Baud arbeiten. Arbeiten in Packet-Radio setzt aber eine Amateurfunklizenz voraus. Interessenten wenden sich am besten an:
Deutscher Amateur Radio Club
Postfach 11 55
3507 Baunatal 1

Diese Bauteile brauchen Sie für den PLL-Decoder:

1 IC NE567
1 Sockel DIL8
1 Transistor BC108B
2 Dioden 1N4148
1 Leuchtdiode
1 Widerstand 33 Ω
1 Widerstand 220 Ω
1 Widerstand 4,7 KΩ
1 Widerstand 10 KΩ
1 Trimmer 10 KΩ
1 Widerstand 470 KΩ
4 Kondensatoren 100 nf
1 Kondensator 10 nf
1 Kondensator 0,47 µf
1 Sub-D-Buchse 9polig
ein Stück Lochrasterplatine
etwas Draht zum Verdrahten
Lötkolben und Lötzinn

um weitere Informationen aus anderen Ländern zu erhalten. Ein Radio-Hacker, der diese Sendung »zufällig« empfing, wollte es nun genau wissen. Er rief kurzerhand unter dieser Nummer an, mit dem Erfolg, daß sich die Ehefrau des Verdächtigen meldete.

So weit sollten Sie es nicht treiben, Sie geraten bei solchen Aktionen sehr leicht in Konflikt mit dem Gesetzgeber. Betreibt man Radio-Hacken im gesetzlichen Rahmen, so dürften Sie keinen Ärger bekommen. Vorteilhaft ist auch, daß Sie keine Kosten für ein Telefon zahlen müssen, das Radio ist ja (hoffentlich) angemeldet. (Bob Langer/rz)