MA BELL IS A CHEAP MOTHER

TAP

TAP
Room 603
147 W. 42 St.
New York 10036

NOVEMBER 1982 No. 79

Fred Steinbeck Issue

Blue Box Equipment And Usage
by
Fred Steinbeck

For all you blue box fans out there, here are a number of parts and part sources for your little devices that you may be interested in. Also in this article are some comments on Nick Haflinger and Ted Vail's blue (green) box in issue number 68, and the use of blue boxes in the Bay Area.

Speakers

Many phreaks are fond of using telephone earpieces as speakers for their boxes. This has some advantages, as the high resistance (~100 ohms) causes less power to be drawn. However, getting the little SOB's out of pay phones is close to impossible.

Fortunately, **Trinetics, Inc.** (55807 Currant Road / Mishawaka, Indiana 46544 / (219) 259-8535 (yes, they accept phoned COD orders)) makes what they call the PC-48 inductive coupler. This is a thing which fits around the earpiece of your phone, and with a four foot cord to an 1/8" phono plug, gets hooked up to your box. Tones are then played into the phone with little or no fuss or muss. The PC-48 can also be used to record calls, and costs $10.00. As some of you may remember, this was first mentioned in an earlier issue of TAP.

There is, however, a problem with the inductive coupler. In order for it to be loud enough to be heard, you need a great deal of power. This is probably just because inductive couplers are not as efficient as speakers.

Keyboards

For me, finding a good 4x4 matrix keypad was a bit of a problem. However, **Advanced Computer Products, Inc.** (P.O. Box 17329 / Irvine, CA / (800) 854-8230 or (714) 558-8813 inside CA (No COD orders)) has solved my problems, if only temporarily. They offer, for $10.00, a FlexSwitch 4x4 keypad (black with white unmarked keys) which is only 0.03 inches thick! Unfortunately, the beastie measures 4" on a side. Too large, in my opinion.

Another solution may be on the horizon, however. **Grayhill, Inc.** (569 Hillgrove Ave. / La Grange, Illinois, 60525 / (312) 354-1040) manufactures a number of 4x4 (and other) keyboards which are only 2" on a side. A vast improvement. I don't know if Grayhill sells directly, as I haven't talked with them yet, but I am sure they would be happy to tell you who you could buy their products from.

The Green Box in #68

In issue number 68, Nick and Ted's article on the green box was printed, along with a set of schematics for such a creature. There are a few comments I would like to make on this schematic.

The LM 747 Output Pin

In the schematic, one of the outputs of the LM 747 op-amp is not numbered on the diagram (i.e., there is no pin number going with that output). Just to set the record straight, it should be pin number 12. If you have issue #68, you might want to make the correction now, to save time later.

Op-amps In General

For my version of the the green box, I'm using an LM386 op-amp. This produces 400 miliwatts, which is more than the LM747 can produce. The LM386, however, has a problem when it comes to biasing correctly. Why, I don't know.

Parts For It

I have had trouble finding 40103's around here. Again, **Advanced Computer Products** (address above) saved my neck. They carry 40103's, they just don't advertise them. They cost $4.25 each. If someone could find a better (pronounced "cheaper") place, please let us all know.

I managed to get a couple 27C16 CMOS PROM's from National Semiconductor. I think these might be the only PROM's that would take a small enough amount of current to make the project practical. My fully assembled green box takes 42 ma standby current, and 47 ma when producing tones.

For those of you who don't like wiring crystals (me - I **hate** buying capacitors), **Jameco Electronics** (1355 Shoreway Road / Belmont, CA 94002 / (415) 592-8097 (COD's accepted)) makes a little package which has four pins, but fits in a 14 pin socket. Give it +5 VDC on one pin, ground on another, and a third will produce a 1 MHz square wave. It costs $9.95, part number OSC 1.000. The only problem with this device is that it draws 20 ma typical. So use the conventional circuit and you just about halve the current consumption.

Plea For Parts

The places I have mentioned above are relatively expensive...I know that there are cheaper places out there. However, having more money than brains, I'm too lazy to find them. If someone else would, it might make a good article.

Boxing From The Bay

In using a blue box around here (East Bay), WATS numbers and information don't seem to work too well. Or more accurately, at all. So, the method I have been using is this: call a long distance number, one that you **know** can be bleeped off. Then, as the phone on the other end starts to ring, bleep off. Unfortunately, if the number you call supes, your money will be gobbled at the end of the call.

Also, I boxed off of a 415 number the other day, but when I played my tones, **every** time I got a 120 ipm reorder signal. Does anyone know if the 415 NPA use automatic equipment? I know the tones are correct (i.e., it works from other area codes).

Another possibility is boxing from terminal boxes. Park your car next to one, open it, and use your handset (you do have a lineman's handset, don't you?) to find a working pair. Then use about 20' of wire (which the terminal box may have - MS boxes have a big spool of wire inside) to bring the line to your car. Hook up the handset and box away! This brings up the point of "Why box when I can just dial with my handset now?" In my opinion, putting 'em through yourself is more phun, that's why!

Comments, suggestions, bitches, ideas, etc., should be sent to Fred Steinbeck, c/o TAP.

Cheats won't ring Bell any more

The telephone company is cracking down on cheaters who make long-distance calls from pay phones and bill them to someone else's number.

Operators in some parts of the nation are now required to verify any numbers given for billing by calling the referred-to phone number and confirming with whomever answers that the caller lives or works there.

If no one answers at the number to be billed, or if someone answers and says the person calling is unknown to them, the call is rejected.

Tricksters using the confidence game cost American Telephone & Telegraph Co. more than $44 million last year, the company said.

The ARPANET
(Part I: An Introduction)

by Fred Steinbeck

What It Is

The ARPANET, also referred to as the ArpaNet, is one of the largest governmental computer networks in existence. It was established in the late 1960's purely as an experimental network. It was so successful, however, that more and more computers were added to it, and now it is the main government computer network. It was originally sponsored by the Defense Advanced Research Projects Agency (DARPA - the people who brought you the M16 rifle), but now it is run and sponsored by the Department Of Defense (DOD) and the Defense Communications Agency (DCA - Note that their military counterpart, the Defense Communications Command, or DCC, are the folks who brought you AUTOVON and AUTODIN).

Access to the ARPANET is given only to people who "need" access. That is, if a person has a government project which would require use of the net, they would be granted access. As it is now, many institutions have access to the network via computers known as TAC's and TIP's. Most (if not all) TAC's and TIP's have dialup ports (without passwords, I might add). Because of this, Joe Nobody can get onto the network - all it takes is a little know how.

What It's Good For

There are basically two things you can do with the network. First, if you have access to a computer connected to the ARPANET, you can probably send electronic mail over the network. This is fun, but not truly anything to get overheated about.

The second thing you can do with the ARPANET is use it to connect with remote computers, called **hosts**. This is much like Telenet (see Paul Montgomery's article in issue 74). Once you can connect to the remote computer through your dialup, you can attempt to login (not that you'd ever do that, of course...)

There are two basic ways of getting access to the network. The first method is to find the dialup number of a TIP or TAC in your area. Then call the number and use it to connect to the computer that your interested in (I realize that's not very specific. Parts II and III of this series will cover doing just that...)

The second method is just as good, but it works only if you already have access to a computer connected to the ARPANET. If you do, look for a program called, curiously enough, "tip". This is a program which allows your computer to simulate a TIP. Because the program "TIP" is different on almost every machine, I can't explain exactly how to use it - you'll have to look up the information in the computer's manual.

Getting A TIP Or TAC Number

Most major universities and colleges are connected to the ARPANET. Also, large corporations or companies doing business with the government may be connected. Here are some specific places that have TIP's or TAC's:

Gunter Air Force Station, AL; Hanscom Air Force Base, CO; Andrews Air Force Base, Washington; Kirtland Air Force Base, NM; Army Communications Electronics Command, Fort Monmouth, NJ; Bolt, Beranek and Newman, Inc., Cambridge, MA; Massachusetts Institute Of Technology, MA; MITRE Corp., VA; Moffett Field, CA; National Bureau Of Standards, Washington; Rockwell Intl., Richardson, TX; SRI International (our favorite!), Menlo Park, CA; Stanford University, CA; The Rand Corp, Santa Monica, CA; University Of Southern California; and the University Of Utah.

My, all those Air Force Bases. While you're there, perhaps you could ask about AUTOVON, too! In any case, as far as getting TIP/TAC numbers, use common sense and bullshitting techniques. First, ask computer science students at the university or college in question - they'll probably know, and won't mind giving them out. As far as government places (i.e., Air Bases), well, just have a good story. I saw the other day at a National Guard Armory a notice about how a guy posed as a military intelligence officer and walked into the Arms room of the armory and took an M16A1 rifle. The military isn't all that tough...

So, for now, you mission is (if Jim Phelps will allow me to borrow his line) to find out the TIP and TAC numbers in your area. Later issues will have parts II and III, which cover actually using the net. Stay cool 'till then.

The ARPANET
(Part II: Use Of The Net)

by Fred Steinbeck

Dialing The Net

Ok, now you've got a TIP or TAC number and you're just waiting to find out how to screw with the ARPANET, right? Well, first thing is to call the TIP/TAC number. It will give an answer tone, so your modem (presumably 300 baud) should be set for originate.

Nothing happens! Nothing is printed on the screen! Fantastic. The TIP or TAC is waiting for a **hunt character**, a character which will tell it what speed you are running at.

If you have the dialup for a TAC, type a control-Q. You should then get the message...

```
<Sitename> TAC <version #> <port #>
```

If you don't, or if the message is garbled, hit the break key (for people without "break" keys, try hitting the "#" sign button on a touch-tone phone) and then type another control-Q. If this doesn't work, let me know by mail, and I'll see if I can't figure something out for you.

TIP's are another story entirely. They are a general pain in the ass to work with. The hunt characters for TIP's vary depending on the baud rate and the device that you are using to connect to the TIP.

If you are ASCII 110, 150, or 300 baud, the hunt character is "E" (upper-case). If you transmit ASCII 300 baud, but receive at 1200 baud, the character is "D". ASCII 1200 baud doesn't need a hunt character. Assuming you get the hunt character to TIP ok, you should see the TIP signon message, which is like the TAC signon. Note that ASCII 1200 baud people don't get a signon message.

Using The Net

There are two commands we are concerned with. The first is "@o host/imp", which tells the TIP/TAC to open a connection to the specified host and imp address. The second command is "@c" which stands for "close", and is used for (surprise!) closing the connection. The "o" and "c" do not necessarily have to be in lower-case.

A host/imp address specifies the computer that you wish to connect with. The computer you will most probably want to connect with first is the Network Information Center at SRI International. The host/imp address for this is "0/73", so the command to connect to it is:

```
@o 0/73
```

The Network Information Center (SRI-NIC) will require an account - when it types "@", type either "NICGUEST" or "NIC" and hit return.

The NIC system is pretty straightforward, but obnoxious to use. It allows you to get information on other computers on the net, how to order (by U.S. Mail) manuals from SRI, internet protocols, etc. In short, after screwing with it for a while, you will learn enough about the net to go off on your merry way.

Oh, when you get tired of a connection, simply type "@c" and hit return. This will close the connection and bring you back to the TIP/TAC command mode.

This is really a bare-bones course on the ARPANET, but it should be enough to get you out there, nethacking to your heart's content. Next month will be part III, general netnotes. If, in the meanwhile, you have questions or comments, send them to Fred Steinbeck, c/o TAP.

Gibberish
by
Fred Steinbeck

This column of mine will cover many topics, some of which I have dealt with before - in short, it's a potpourri of various things...or, gibberish.

Books to get: An excellent book I have just finished looking over is **Signalling In Telecommunications Networks** by Samuel Welch. This book, although rather technical, covers SF signalling, MF interoffice signalling, CCIS (common channel interoffice signalling, also known as plain ol' common channel signalling, CCS), and many other topics. Highly recommended.

Books I'd like to get: In issue number 68, The Magician wrote about the Bell book **Notes On Distance Dialing**, mentioning that it used to cost $12.95. He also said to send a SASE for more info on getting it. Would it not be easier to tell how in TAP? Or is it one of those things that is better left to a limited readership?

Along the same lines, how does one get a copy of the CCITT Green book, or the Bell **100 Series Test Codes**? I'd like to get these, but I have not been successful yet...perhaps somebody will take pity and send some info in, huh?

Articles: The July **Penthouse** magazine has an article on computer crime. Believe it or not, this article mentions our good friend Donn Parker, as well as Susan Thunder, the 8BBS, and the COSMOS computer system...worth reading, perhaps.

Sprint: In the last issue, number 76, there was a list of Sprint dialups across the nation. However, one I used to use in Oakland, (415) 832-5015, was omitted. While I appreciate the effort that went into compiling such a list, is it possible there are more additions?

Garbage: Garbage can provide an excellent source of information...dialups, passwords, computer logins, etc. Try going through your local ESS dumpster late at night and see what's there. Or perhaps a stock market place. Or bank (be careful, though). I think you'll be surprised at what you'll get (besides fleas and the plague)!

Newslines: Here are a couple in the Pac Tel area, from Bell's own newspaper, Update:

(415) 545-8800	San Francisco (or)>-|
(800) 882-1061	(from California)<--|
(408) 491-7777	San Jose
(714) 237-3111	San Diego
(714) 835-5111	Orange-Inland Empire

The San Jose number in issue number 65 is disconnected.

AUTOVON: I talked with another guy, this one an electronics tech with the Navy. I got the following from him.

AUTOVON is sponsored by the Defense Communications Command (DCC). They are the military counterpart of the Defense Communications Agency. The Air Force are the main AUTOVON users, and the Navy uses it a good deal too. There is another service similar to AUTOVON called AUTODIN, which stands for AUTOmatic Digital Information Network. It is used only for connecting computers together.

At any given time, the military controls / uses 3% to 7% of the nation's long distance lines. However, in an emergency, at the press of a button, a computer called SCAN in Omaha will grab onto **90%** of the civilian long distance lines for military use. Could be cute to get the dialup to SCAN!

Last, more and more AUTOVON traffic is being put through government computers called STEAMVALVEs, which are essentially over-grown voice encrypters.

I seem to have run out of things to write about. Comments or questions should be directed to me c/o TAP. Or, like I said, write an article!

Gibberish II
by
Fred Steinbeck

Welcome again to a collection of oddities and bizzareness in the phone phield. Much of this month's material comes straight from the horse's ass, so to speak (i.e., the Bell System).

ESS's

Ah, yes, the infamous ESS, or Electronic Switching System. The very word strikes terror into the heart of a phone phreak. First the bad news, I guess. I was reading a few days ago in the May / June '82 issue of Bell Lab's **Record** magazine, and found that 51% of all switching centers across the U.S. are now ESS's. It took Bell 17 years to get the first half done, and it is expected to take another 10 years to finish the job. 1992, **phriends**. * Sigh *

New Payphones?

In the March '82 issue of **Record**, I saw that Bell is working on a new pay phone. This one is known as the "electronic" model (as opposed to the old one?) In any case, the thing is a little better armored, and is alleged by Bell Labs to produce the 2200 & 1700 Hz more accurately. It's also supposed to detect slugs and foreign coins better. We shall see, as it is supposed to appear in 1983.

Automated Coin Toll Service (ACTS)

Around here (Bay Area), we have a new computer called ACTS. This computer runs under stations which have TSPS, and basically tries to impersonate an operator. ACTS is used with pay phones, for long distance calls. For example, you put in your dime and dial a long distance call. You hear a voice (with an 80 word vocabulary, no less) come on and say, "Thirty five cents please. (2 second pause) Please deposit thirty five cents for the next three minutes." If you talk for more than the three minutes, and then hang up, ACTS will call back and demand your money...

More bad news - ACTS, being a computer, can detect coin toll fraud (i.e., red boxes) better than operators. I would assume it would measure the duration and frequency of the tones. You can flash the switchook, however, or dial "0" and get the operator. Why you'd want to do that, I don't know. She'd probably just turn you over to ACTS again.

If you want a document on ACTS (a promotional / quasi-technical one), or have any questions or comments about this article, send a SASE to Fred Steinbeck, c/o TAP.

UNIX Wizardry
by
Fred Steinbeck

In this column, I shall try to show a few tricks I have picked up while hacking on the UNIX operating system. This is not meant to be a tutorial; I assume you are relatively familiar with UNIX. Enough to know what I'm talking about, in any case.

I use the UNIX systems here at U.C. Berkeley, so a few notes about them: First, they run Version 7 UNIX, and generally run under the C-shell. I think that most systems around use the C-shell today, though, and are version 7, so that shouldn't be any problem.

Directories & Terminals: Some good directories to mess with are /etc, /usr/doc, /usr/spool, and /dev. This last directory, /dev, contains all the devices (peripherals) on the system.

UNIX treats all I/O devices as files, which means that there are some special things you can do with them. First, all terminals hooked into the system have a file associated with them. At UCB, most of the terminals are /dev/dz##, /dev/bx###, or /dev/mx##. The "#" signs are digits.

In any case, the "who" command prints out the names of the terminals people are on. So, let's say that a friend of yours has logged on, using terminal "dz28". Well, the filename which corresponds to terminal "dz28" is /dev/dz28. Following this to it's logical conclusion, if we type

```
     cat /usr/dict/words > /dev/dz28
```

and hit return, we will cause the entire 50,000 word dictionary (in the file "/usr/dict/words") to be printed on his terminal. If he happens to be on a 300 baud dialup, well, so much for him.

You can probably see the difference between this and the "write" command. "Write" prints "message from so-and-so" (your name where it says "so-and-so") on his screen. Well, "cat"ing into other people's terminals doesn't reveal your identity to them, so it is less likely that they will be able to retaliate.

Another good command, when used in conjunction with terminal filenames, is "stty" (set tty). The command

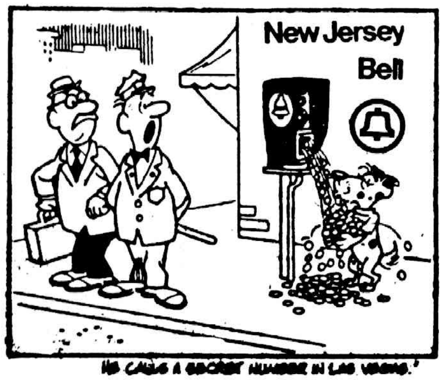
```
     stty 0
```

causes you to be logged off. But, if we specify a terminal to send this command through, it will effect the user of that terminal. Therefore,

```
     stty 0 > /dev/dz28
```

will logout your aforementioned friend (boy, you sure treat your friends rotten, don't you?)

Well, it's 2 in the morning right now, so I'd best leave you to your UNIX wizardry, and me to my sleep. But there's more...soon: anonymous messages in the system bulletin board program.



HE CALLS A SECRET NUMBER IN LAS VEGAS.'

ACTS Update

by Fred Steinbeck

I wish to apologize for some misinformation in a previous column of mine (Gibberish II). In this column, I mention ACTS, the Automated Coin Toll Service computer which is replacing operators for accepting money at pay phones. I gave the impression that ACTS would be hard to use red boxes on, as it, being a computer, would be able to detect timing differences between red boxes and the pay phone.

I have **never** been more wrong. I have witnessed successfully boxed calls using a manual red box - one where the length of the tone is determined by how long the switch is held down. In other words, the button is pressed twice to simulate a dime. ACTS happily accepts this, so I conclude that it doesn't know a milisecond from a hole in the ground.

I should mention another possibility, however. It could be (and I have no proof of this at all) that if ACTS suspects toll fraud, it allows the call to go through, and then notifies an operator. This probably isn't so. Occasionally an operator will come on the line and ask for money, but this only seems to happen when the "money" is deposited too fast.

On a related subject, I have found what seems to be the best way to blue box from the Bay Area. Call a number you know can be blue boxed off of, **from a pay phone**, using your red box. Then disconnect and re-route your call with your blue box. The most it will cost you is a nickel.

I know a girl who did this the other day. A few days later the person she called got a call from Bell Security. They knew the number she called, the number she called **from** (which is why you should use a pay phone), the time of day the call was placed, and the length of the call. So it might be prudent only to do this when scanning for operator codes, etc., unless you **know** the person you are calling won't talk.

Q. *In his fascinating book "Russia," Robert Karser claims that there are no telephone switchboards in Russian hotels. If that is true, how do telephone calls get through?—Mildred Davis, Austin, Tex.*
A. Each hotel room in the newest Moscow hotels has its own phone, its own separate phone number, its own outside lines. In creature comforts the Soviet Union lags 50 years behind the U.S.

Curling up in front of the fire
Book Review
by Cheshire Catalyst

As a Phone Phreak, we are all called upon from time to time to explain to our less technical friends "How it all Works." Now there is a book you can hand them, (or tell them to get) called <u>All About Telephones</u>, by Van Waterford. The book glosses over the history of telephone service in the U. S., and then explains the workings of the insides of the phone. His explanation of the network inside the phone left much to be desired, and he didn't explain fully why there were so many harmonics available from the ringer. Then again, that wasn't what the book was really about.

Most of the book seems to discribe what telephone hardware is out there in the marketplace, and how to hook it up. It goes into modular connectors, cordless telephones, decorator phones, repertory dialers, caculator phones, scramblers, security alarms, facsimile, and mobil radiophones.

It includes a glossary, which is pretty good for the new comer. Most important, it has a list of suppliers, including addresses, of all the companies mentioned in the book.

The blurbs on the back of the book Also mention <u>The Handbook of Telephones & Accessories</u> <u>($9.95 paper, order #997) which I hope to review</u> in a future issue.

<u>All About Telephones</u> (order number 1097) is <u>available for $5.95 from</u> Tab Books, Dept Tap, Blue Ridge Summit PA, 17214.