==Phrack Inc.==
Volume One, Issue Three, Phile 10 of 10

=-=

Phreak World News II
Compiled by
\\\\\=-{ Knight Lightning }-=/////

Retraction

We at Phrack Inc, respectfully retract all statements made in last issue concerning Stronghold East Elite and the LOD. We are sorry for any inconvenience this may have caused you.

Phreaks Against Geeks

This group was formed as a joke by The W(hack)o Cracko Brothers Inc. on a conference in December of 1985. The charter members were TWCB, taRfruS, Blue Adept, The Clashmaster, and a few others. Since then, Catcher in the Rye and the Slovak have tried to join.

Later that month, Boston Strangler and Micro Man formed PAP, which stands for Phreaks Against Phreaks Against Geeks. Other opposers of PAG include:
Hack Attack, The Detective, Kleptic Wizard and The Overlord 313. It is not known if these others are now in PAP or not.

All of this nonsense was really started on the Dartmouth System and is mainly a local feud of phreaks in the Boston (617 NPA) area.

Brainstorm Gets 10 Megs

Finally, after several months of promises, Brainstorm (ELITE) now has a 10 Meg Hard-drive. As of January 1, 1986 Modern Mutant cleared the userlog of Brainstorm and a membership drive was started. Note: To become a member of Brainstorm, you will have to take a small (and more or less easy) filter.
Some other new features on Brainstorm are online games; Karate, Football, and a hacking simulation.

Anarchy Inc. Disbanded

Anarchy Inc., a once very famous g-phile writing organization, has been disbanded. Basically because most of its membership are now attending college.

Dartmouth Conferences To Be Abolished?

This message was given on January 9, 1986 when a user would try to join a conference.

XCaliber, Fantasie, Spectre, etc are not available until tomorrow. Due to pressure from Kiewit and some users, conferences have been disabled for one day. Hopefully this will remind some people that the conferences are a public service on the part of a few people and are not a "right". Recent abuse of the conferences has made caring for these conferences almost more trouble than they are worth. These abuses have also caused some users to complain to Kiewit. Too many complaints and they might vanish altogether. If everyone will work at keeping the conferences reasonably clean and free of abuse life will be much easier. Thank you for your time and appologies for the lack of conferences.

You are no longer connected to conference "XYZ".

Later, Corwin got pissed off by the password abuse that was going on and killed almost all non-Dartmouth student passwords. It is also rumored that he took down the DUNE bbs, however Apollo Phoebus says that it is a temporary thing and that DUNE will be going back up soon.

MCI Employee Bust

Employees at MCI were creating fake accounts and then running up massive bills. Then later they would either credit the accounts or say that the subscriber reported code abuse. Any employee found doing this was fired.

Another way these employees were cheating the company was by reporting code abuse on their own accounts, however MCI Security using CNA quickly caught these employees.

Note: MCI Security has stated that the only real way that they can catch abusers of the phone company is by calling the numbers that the abusers call and asking them who they know making these calls.

Information has been provided through MCI Security

MCI/IBM Merge

MCI Telecommunications company has merged with IBM and their phone industry SBS. This was an effort to join the two as strong allies against AT&T.

IBM computers Vs. AT&T computers

MCI Telecommunications Vs. AT&T Telecommunications

Changes arising from this merger (if any) are not known, but none are expected for some years.

The Life And Crimes of the W(hack)o Cracko Brothers

The date is somewhere in December of 1984. Peter writes a code hacker for the Hayes and tells Tim NOT to use it on Sprint because they trace. Sometime later that night Tim received a call from Scan Man, sysop of P-80.

Scan Man said he needed TWCB to hack him some Sprint codes cause he didn't have the time or a Hayes. Tim did it for him on the 314-342-8900 Sprint extender.

He left it on all night and the next day while he was in school. Sprint traced him. At 9:00 AM the next morning agents from the FBI, AT&T, Western Union, GTE, and Southwestern Bell, arrived at TWCB's house.

They were let in, bringing with them cameras and tape recorders among other equipment. Upon seeing this Peter blew into an upstairs extension and cancelled the dialing program, but not before the agents made sure it was the right place.

All of TWCB's computer equipment was confiscated and Tim was taken downtown shortly after being picked up at school. Peter was sick and left home. Tim was later released in his mother's custody.

They each received probation and 100 hours of county service.

That was then...

Recently TWCB has come under investigation for the following: Drug use and dealing, burglary, forgery, and fraudulent use of a credit card.

Peter: 8 Class A Felony charges
1 Class A Misdemeanor charge
1 Class B Misdemeanor charge

Tim: 6 Class A Felony charges
2 Class B Misdemeanor charges

Note: Some of these misdemeanors are for not returning library books.

Also it has been said that Tim has been in jail 11 times. Both members of TWCB are now enrolled in a reform school.

The information in this article has been provided by TWCB, directly and/or indirectly.

Blue Adept: Gone For Good

Blue Adept, known for being an all around loser and Dartmouth impersonator, decided to try blue boxing. For some reason he decided to call an out-of-state trunk direct.

Later that month Blue Adept and his parents received a phone bill with a charge around $386.00. This led to his being restricted from using the phone.

Sometime after this incident Blue Adept received an invitation to join on a conference. He wasn't home but his parents decided to stay on and listen in.

Blue Adept is not allowed on conferences anymore and all calls to him are now screened.

Overlord 313 Busted: Step dad turns him in

Overlord's step-dad always would be checking his computer to see what was on it and what was nearby. Last week he noticed the credits in Overlord's file on Wiretapping, which can be seen in this issue of Phrack.

He reported his findings to Overlord's mom. She had a talk with him and he promised to stop his evil ways. His step-dad didn't believe him for a second.

1/11/86

Step-dad goes on business trip, where he meets Ma Bell executive Don Mitchell. Step-dad asks all sorts of different questions regarding use of MCI dialups and Alliance Teleconferencing, and talks about how his step-son does all these things and more. Don strongly suggests that he reports this to the phone company...

1-13-86

HE DOES

No legal action against Overlord has taken place as of now.

Information Provided by The Overlord of 313

Maelstrom 305 Busted

While I am not at liberty to revel all the information concerning this bust I will mention the bare facts.

Maelstrom hacked into the Southern Bell Data Network (SBDN). This system happened to be local to him so he did not bother to use an extender. Unfortunately this system also had ANI (Automatic Number Identification). His computer and other equipment as well as all his files were confiscated as evidence.

Information provided by the Maelstrom of 305

Whackoland BBS

This bbs is now up and running strong. Its sysops are of course...TWCB Inc. 300/1200 Baud, and 40 Megs. It has unique features and great mods as well as Elite Sections. Call today... 314-256-8220. Note: Only 100 users will be kept so if you are just a beginner please don't bother to call.

R.I.P. Broadway Show

The Broadway Show BBS in New York is now down, and Broadway Hacker will soon be in Washington DC. This C-64 run bbs, was one of the best in its time, but later it became a hangout for rodents.

>From its ashes rises a new bbs, however its name has not been released as of this writing. Broadway Hacker will sysop this bbs for about a week and then turn it over to the new sysop. His name is not yet know, probably since he hasn't a handle yet.

Although this new bbs will appear legal and have some legal sections it is indeed a phreak bbs, and should be checked out.

718-615-0580

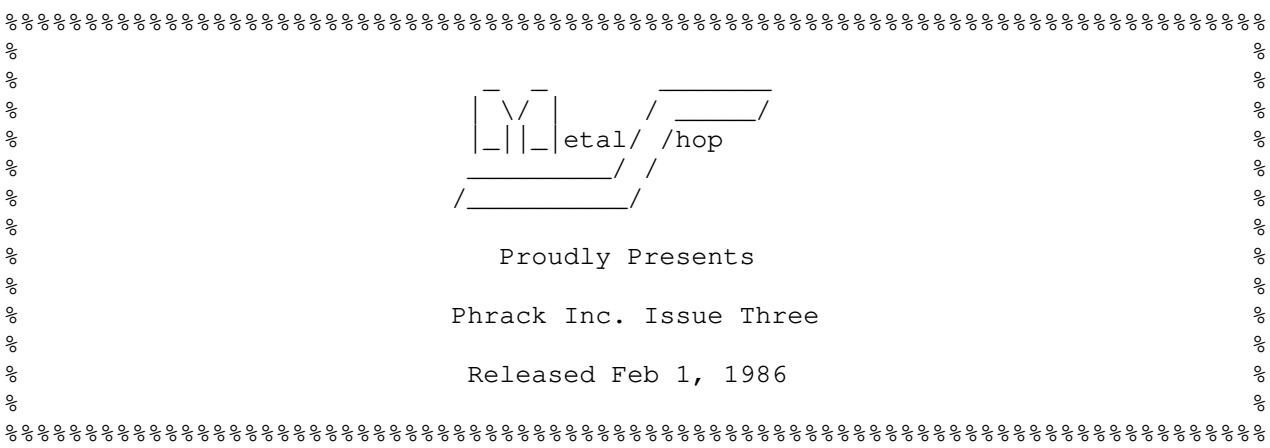
Speed Demon Elite Down?

This bbs sysoped by Radical Rocker has suddenly disappeared leaving the caller with a message of the line being disconnected. No other information is available.

Well that's all for this issue's Phreak World News. If you have anything of news

Knight Lightning/Taran King/Cheap Shades

==Phrack Inc.==
Volume One, Issue Three, Phile 1 of 10

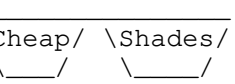


The files contained in this issue of Phrack Inc. are as follows:

1: Index written by Cheap Shades
2: Rolm systems written by Monty Python
3: Making shell bombs written by Man-Tooth
4: Signalling systems around the world by Data Line
5: Private audience written by Overlord
6: Fortell systems written by Phantom Phreaker
7: Eavesdropping written by Circle Lord
8: Building a Shock Rod written by Circle Lord
9: Introduction to PBX's written by Knight Lightning
10: Phreak World News II written by Knight Lightning

If you have an original file that you would like published in a future issue of Phrack Inc. Leave E-Mail to Taran King, Knight Lightning, or Myself on any system that we are on. If you cannot find us try and contact some member of Metal Shop to get into touch with us.

Later,



==Phrack Inc.==
Volume One, Issue Three, Phile 2 of 10

The purpose of this file is to tell you what you would be dealing with if you stumble across this system, or if you know of a company that is using this system. It doesn't go into incredible detail, and is lacking in areas. It is not a guide to hacking into it, just letting you know what you would be dealing with. This is to pique your interest in the system.

So What the Hell is ROLM?

ROLM is a "Business Communications System" bought by IBM a few months ago, in an effort to compete effectively with AT&T, and get a larger share of the market, in a grand master plan to become "Big Daddy Blue" as opposed to "Ma Bell". It is a very complex system, with features such as PhoneMail, A Super-PBX, Local Area Networks, Public and Private Data Networks, Desktop Communications, and Call Management.

The heart of the system is the Controller, called the CBX <Computerized Business Exchange>. This controls the entire network accessible through ROLM. Since 1983, the CBX was redesigned and upgraded to the CBX II. It is a PBX with much much more <See 'Introduction to PBX's' available on your local bbs> to offer, and that is ROLM's claim to fame. It is light years ahead of the regular PBX system.

The CBX II

The CBX II is the core of the ROLM network. It is computer driven and expandable from one node, with 165 channels, to 15 nodes providing 11,5200 2-way channels. The smaller business could have a model with a 16 user maximum limit, but it can go up to 10,000 users, though this would be quite rare <and quite God Damn expensive!>. It can be accessed from outside lines <like you> as well as HardWired units, with a switching system to prevent busy signals on a port. Speed depends on the system in place, either the newer, faster ROLMbus 295, or the older standard ROLMbus 74. <see Service manuals for exact details> The larger the system, the faster as well. It is adjustable to accept different bandwidths for the various components, such as Telex, Voice, Data, Mainframe, LAN, Video <ta-da! Picturefones in reality!>, and anything hooked up to the system. Similar tasks can be bunched onto one channel as well, at high or low speeds. If multiplexing is used <above>, the maximum speed is 192,000 bps, and if using a single interface, the top possible rate is a mindboggling 37,000,000 bps, which if you ask me, if just fluff and not too practical, so they are usually multiplexed. <Now, what a difference that is from 300 baud!>. Using the CBX II network, you might find just about any kind of mainframe, from HP, to DEC, to VAX, to the IBM 327 series.

Note : There is a smaller version of this called the VSCBX.

Phone Mail

This is one of the little beauties of the system, something truly fun to fuck with. I called ROLM Headquarters in California to ask specific questions about ROLM, posing as a researcher, and I got the big runaround, transferred from department to department. Maybe you can get further than I. Their is 408-986-1000. The to PhoneMail from the outside is 800-345-7355. A nice computer-generated voice comes on asking you to enter your Extension number <which each employee has>, and then enter the "" sign. Then enter your password. If you make around 3 or 4 bad attempts at an Extension of Password, it will automatically ring another number, assistance I assume, to find out why there has been an unsuccessful entry attempt. I haven't played around with this that much, so leave mail to Monty Python with whatever you find. Once entering an authorization with correct password, you will be presented with more options, leave messages to other people, and whatnot. You can hear your messages, forward them to another person, leave the same message to more than one person, change your welcome message, etcetera. The service is for those business-type pigs who never sit still for one minute, like they are permanently on speed.

A Phone Mail Scenario

Let's say if Mr. Greed goes out to meet his secretary at a motel, but definitely has to get that important message from Mr. Rasta, who's bringing in $3 mil in Flake, and can't trust it to the person who would handle it <ie: the person filling in for his sec with the tremendous tits who is getting balled by the dirty old fat man>. Mr. Greed would have given Mr. Rasta his phone and he would be forwarded to the Phone Mail network, where he would hear a message left my Mr. Greed, to anyone who would call. Mr. Rasta would leave his message and hang up. Then Mr. Greed could call up the 800-345-7355 , punch in his extension authorization number, and password. Or, if he was back at the office, he could get it there through DeskTop communications. Messages can be delivered without error, in the person's own voice, without other people knowing about it. Therefore, someone with enough knowledge could use an unused account and use it as his own service, without the knowledge of others.

DeskTop communications

ROLM has developed a Computer/Telephone integrated device for use with the Desktop communications. It is linked with the CBX II through fone lines, thus accessible by you and me from the outside. It is not hardwired, though it can approach hardwired speed. If you could get your hands on one of these computer/fones then I think you would have found something very useful at home, in your general life. But you could access the network without the special features of the fone, like one touch dialing, which is designed for the stupid lazy businessman. You can access company databases through the network, mainframes, other people, just about anything as if you were right there and told your secretary to do it for you. There is special software used by the computers or computer/fone but it can be improvised and is just an aid. It uses a special protocol <Don't know what, try to get your hands on one by trashing a sales office>. What is great is that everything is tied together through telefone lines, and not RS-232C! Thus, there is an access port....somewhere. Scan the 's around the office using ROLM. How do you know if it is using ROLM one way or the other. Compile a list of local businesses, call them up saying "This is ROLM Customer Support. We have a report of a complaint in your CBX II network, let me speak to your supervisor please." If they say "ROLM? CBX II? We don't use that" then just apologize and go elsewhere. Or say that you are from ROLM corp and would like to know if the company is interested in using it to network its system. Like, if they have it already, they would say that they had it. And if they didn't, you would just give them a fake <or if you're nice the for the local sales office obtainable in the list below>.

But you know what's REALLY Great? They have made the network link in mind for the person with a Computer IQ of about 0. Commands are in plain English. Here is a demonstration screen as seen in their brochure:

```
CALL, DISPLAY or MODIFY

Display groups

ACCESSIBLE GROUPS:
  [00] PAYROLL       [01] MODEM       [02] IBMHOST
  [03] DOWJONES      [04] DECSYSTM    [05] MIS-SYSTM
  [06] DALLAS        [07] SALES

CALL, DISPLAY OR MODIFY?
Call Payroll

CALLING 7717  <which would be the ID code for the PAYROLL file>
CALL COMPLETE

**PAYROLL SYSTEM** <or whatever they want to call it>
 ENTER ACCOUNT CODE:
```

See, nothing is confusing, everything pretty self-explanatory. There may be more than one person wanting to do the same thing you are, so if there is, you would be put on a queue for the task. It seems that those with an IBM would be best suited for ROLM hacking, because ROLM is owned by IBM, and the PC's used by the network are IBM. A person with a simpler fone/Terminal couldn't access

something like their DEC mainframe, or something like that. By calling in, you could not run an application, unless you had a special interface, but you could access the database, which any dumb terminal could do.

However, there are security levels. Thus one with a privileged account could access more things than one without it. Like Joe Schmoe in Sales couldn't get to Payroll . It seems that for non-IBM's to access some of the parts of the network, you would need an interface to become the same thing as a RolmPhone.

Excessive 's of bad logon attempts, which would be construed as a linking error would notify the network manager, And if they saw that there was no hardware error, eventually, they would think of if they were somewhat experienced, you guessed it, hackers.

The PBX

ROLM has something called Integrated Call Management <from here on known as ICM>. Now, when designing ICM, they must have taken into account the abuse possible in plain ol' PBX's. So they put in something called Call Screening. This will enable the company to restrict calls to certain 's and prefixes. Calls to non-business 's or certain areas can be screened out <"No personal calls on my time, Johnson!">, with the exception of 1 specific that you want.\024

There is a choice of having a codeless, screened PBX, or a PBX where accounts are assigned to each employee, and the 's they call get recorded to that account. There can be privileged accounts where a large volume of calls would go relatively un-noticed. But I don't think that large-scale abuse of this system would be easy or practical. Calls are routed AUTOMATICALLY through the service where the rates are cheaper to the location dialed, which is pretty fucking cool. And, the PBX is accessible from the outside, using Direct Inward System Access, making it AB-useable.\024

But what about if there is Equal Access in that area? It doesn't matter, the CBX will automatically access the service without you having to worry about it <hell, this is totally unnecessary for a hack/phreak, cause we ain't paying for the damn call anyhow!>

BUT!: There is a use of Call Detail Recording, where information on all ingoing and outgoing calls are recorded.

Conclusion

Not a lot of research went into this file, but it did take a little while to type up, and all of the information is correct, to my knowledge. Anyone is free to expand on this file into a Part II. It was written to enlighten people about this system, and I hope this has helped a little bit.

Sysops: You are free to put this file up as long as NONE of the credits are changed! <this means the Phrack, Inc. AND Personal credits>. Please give us a chance.

Coming soon, to a telephone near you: The Return of The Flying Circus. Look for it.

--Later On
Monty Python <01/11/86>

==Phrack Inc.==
Volume One, Issue Three, Phile 3 of 10

"SHOTGUN SHELL BOMBS" from The Poor Man's James Bond by Kurt Saxon

typed in by --] Man-Tooth [--

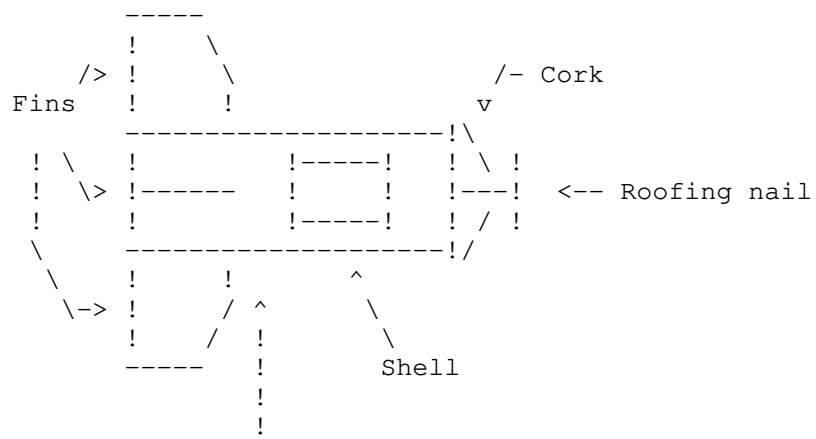
These little goodies are affectionately known as "nut busters." They are simply shotgun shells enclosed in cardboard rolls with cardboard fins put on. On the primer end of the shell is glued a small cork with a hole drilled through it. A roofing nail fits in the hole snugly enough to stay in, but loose enough to plunge into the primer upon impact.

Since the shell is not confined in the chamber of the gun, it will naturally not cause the same amount of damage. But if it goes off between a fellow's legs he can look forward to becoming a soprano.

These bombs are thrown singly or by the handful into the air over milling crowds. The weight of the shell and stabilization by the fins causes the nut buster to head straight downward.

It has tremendous effect as its presence is usually a suprise. The threat of more coming is guaranteed to route any mob.

Not only does it go off on the pavement but it will also explode on contact with a person's head or shoulder. At night it is impossible to trace its point of origin.



Close fitting 3-1/2 inch Aluminum Tubing Glued on Shell.

SHOTGUN SHELL BOMB

A clever use for a plain shotgun shell is as a muffler bomb. The shell is simply shoved up a car's exhaust pipe with a length of stiff wire until it drops into the muffler. After a few minutes on the road the shell explodes, totalling out the muffler and treating the driver to a sick kind of panic.

==Phrack Inc.==
Volume One, Issue Three, Phile 4 of 10

Signalling Systems Around the World

For those of you who have the desire to make international calls, this info may be of interest. Thanks to TAP and Nick Haflinger.

CCITT 1. An old international system, now deceased. Used a 500 Hz tone interrupted at 20 Hz (Ring) for 1-way line signals.

CCITT 2. Proposed "International Standard" that never caught on much. Used 600 Hz interrupted by 750 Hz. Still used in Australia, New Zealand and South Africa.

CCITT 3. An early in-band system that uses 2280 for both line and register (!!). Used in France, Austria, Poland and Hungary.

CCITT 4 A variation of 3, but uses 2040 and 2400 for end to end Tx of line and register. Used for international Traffic in Europe, but cannot be used with TASI (AKA Multiplex or "that dammed clipping").

CCITT 5 This is the most popular, and the one used in the US. 2400 and the infamous 2600 are used for link to link (not merely end to end line signals. Registers are handled via DTMF (Touchtones). Anyone know what 2400 does??

CCITT 5 bis. Just like above, but a 1850 Hz tone is used for TASI locking and transmission of line signals.

CCITT 6 The newest and worst for phreaks. It uses digital data sent out-of-band to control the connection. In other words, the connection is made and billing started BEFORE you can get control.

CCITT 5R1 A regional system like 5, but doesn't use the mysterious 2400 and can't use the multiplexer.

CCITT 5R2 Probably the interface to AUTOVON, as it uses 120 Hz spaced tones for DTMF instead of 200. Also 3825 Hz is the blow-off tone instead of 2600.

The "Extra" tones

1700 + 700 = Inward Operator
1700 + 900 = Delay operator, also, in TSPS,STP (a "Zero Plus" call from a coin phone)
1700 + 1100= KP1 (Start recognition of special tones)
1300 + 1700= KP2 (End recognition of special tones)

12-85 Data Line. CIS 72767,3207: TWX 650-240-6356

==Phrack Inc.==
Volume One, Issue Three, Phile 5 of 10

* PRIVATE AUDIENCE *

(A BASIC LESSON IN THE ART OF LISTENING IN)

BROUGHT TO YOU BY

-[THE OVERLORD]-

-=-

PART I: THE LAW

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 transmission of a wire communication to intercept or disclose intercepted communication."

What all this legal bullshit is saying is that if you don't work for a phone company then you can't go around tapping people's lines. If you decide to anyway, and get caught, it could cost you up to 5 years of your life and $10,000. This, you are all assuming, means that if you tap someone else's line, you will be punished....wrong! You can't tap your own line either. The punishment for this is probably no more than a slap on the hand, that is if they actually catch you, but it's a good thing to know.............now on to the fun.....

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 is 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 that 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!

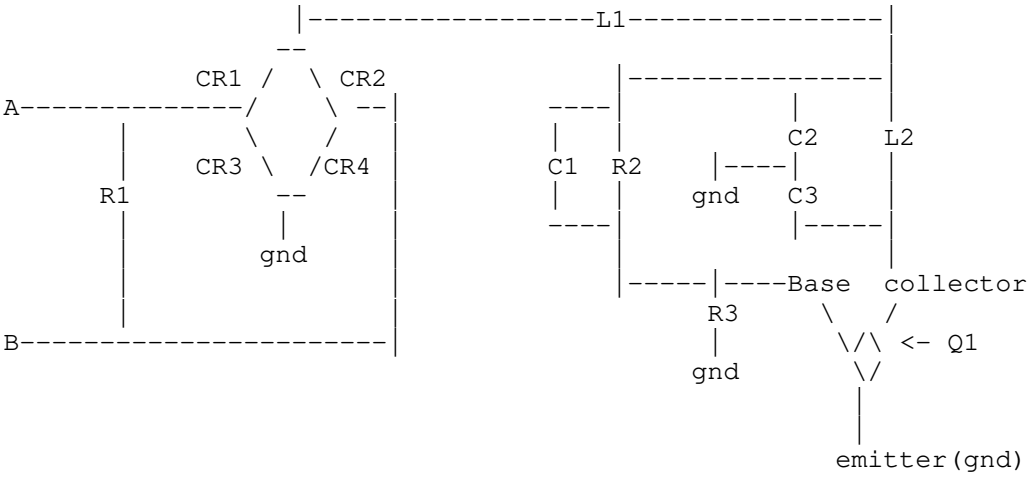
PART IV: WIRELESS TRANSMITTER PLANZ

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....

PARTS 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

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.

-[OVERLORD]-

THANKS TO:

The CircleLord
TARAN KING
Knight Lightning
The Forest Ranger
P-80 systems

Watch for more advanced tapping, how they catch you, and verification in the near future.

==Phrack Inc.==
Volume One, Issue Three, Phile 6 of 10

Fortell Systems

Written by Phantom Phreaker

Call The Alliance at 618-667-3825

Fortell systems seem to be a system to monitor lines. They can only be used to monitor lines within their own NPA.
A Fortell system is at 716-955-7750. Whene you call, you will hear:

'Hello. This is the Taradyne Fortell system. Please enter ID code'

The ID for this system is 722877*. After you type that in (DTMF) it will ask 'please enter line number' where you then type the PRE+SUFF of the number you wish to check within the NPA of the Fortell.
After you enter a number, it will repeat the number you entered. Now it will ask you to 'please enter mode'.

The modes are:

1-Calling on other line
2-Calling on test line
3-Line test results

If you enter mode 1, you will have these commands available:

1-Fault location
2-Other testing
7-Test ok, Monitor
8-Hang up
9-Enter next line number

If you enter 7 here, it will repeat what you selected, and ask for an ID code which can be any 6 digit number followed by a *.

Now it will dial and tell you:
'Subscriber busy-busy-monitor test in progress conversation on line-short on line'

2-Monitor test
3-Overide and test
4-Wait for idle

If you enter 2, (Monitor Test) it will tell you the busy status again.

If you enter 3, it will override, or tell you 'Not available in this CO'.

If you enter 4, (Wait for idle) it will wait until the line is idle.

If you enter 1 (Fault Location) at the main list you will get these options:

1-Open location
3-Short location
4-Cross location
5-Ground location
8-Hang up

If you enter 2 (Other testing) here, you will have these commands:

2-Loop Ground OHMS
3-Dial tone test
5-Pair ID
8-Hang up

If you enter Mode 2, you will have these options:(Other testing)

2-Other testing

7-Test ok, Monitor
8-Hang up
9-Enter next line number

It will repeat what you selected. If you select 2 here, you will now have these commands:

2-Loop Ground Omhs
8-Hang up

If you select 7 at the main list after mode 2, it will ask for an ID which is any 6 digit number followed by a *. Now it will dial and check the number. If the number is busy, it will say 'Subcriber busy-monitor-test in progress-conversation on line-short on line-please hang up-waiting for idle' Now you can just type * to go back to the main list of commands.

If you enter MODE 3, if you have done a test before, it will give you the results of the test. If you haven't done a test, it will tell you so with 'No test results available'

You can abort back to the main commands list by typing a *.

By typing a 9 at several places you will be taken back to the beginning where it asks you to 'enter line number'

PP-01/06/86

==Phrack Inc.==
Volume One, Issue Three, Phile 7 of 10

Electronic Eavesdropper

by

Circle Lord

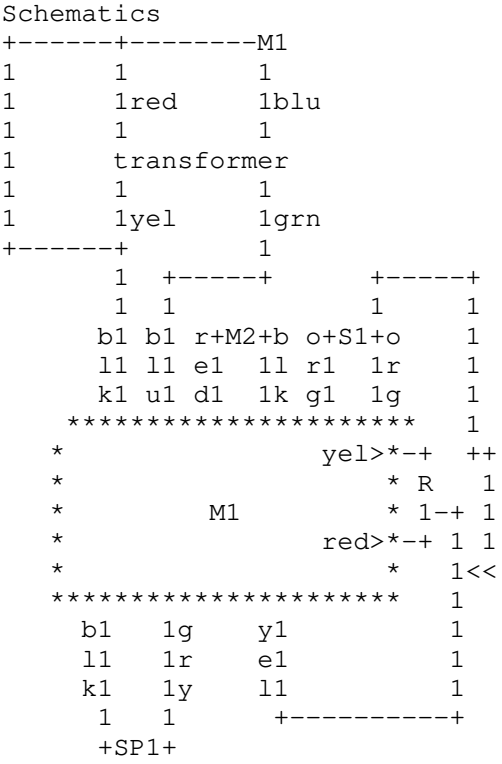
Have you ever considered buying one of those hi powered microphones often seen in eletronics magazines, but thought it was to much to buy and to small to card? The circuit shown in this file will provide you with the information to build one for a lot less money.

These audio eavesdropping devices are probably one of the hottest items in the underground due to their ability to pick up voices through thick walls. You can also attach the speaker wires to a tape recorder and save all the conversation. As one can see these are great for blackmailing a teacher, classmate, principal, neighbor, or whoever you seek services from...

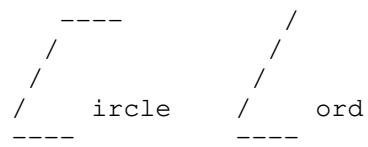
Parts list:

-=EM-------------------------
M1 Amplifier Module. (Lafayette 99C9037 or equiv.)
M2 9-VDC battery.
M3 Microphone
R1 20K poteniometer with spst switch.
S1 Spst switch on R1
SP1 8-ohm speaker
T1 Audio transformer (Radio Crap part 273-1380)

Schematics



S1 here is on the potentiometer
M3 can be an earphone earpiece


ircle
ord

==Phrack Inc.==
Volume One, Issue Three, Phile 8 of 10

Making a Shock Rod

By

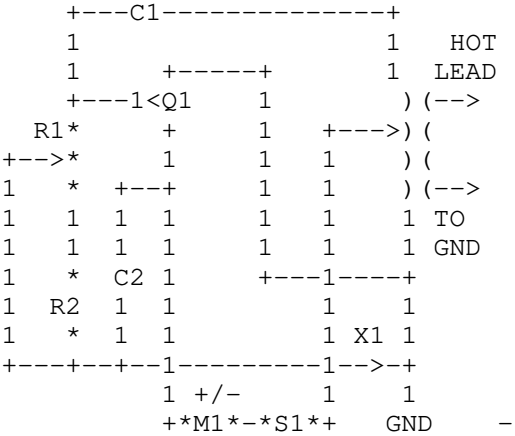
Circle Lord

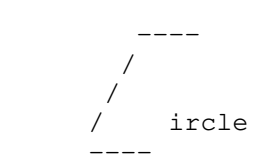
This handy little circuit is the key to generating THOUSANDS of volts of electricity for warding off attackers (notice the plural). It generates it all from a hefty 6-volt source and is easily fit into a tubular casing. Originally used as a fence charger, this circuit can be put to other uses such as: charging a whole row of lockers at school, a row of theater seats, or a metal bleacher set in the gym. More on this later.

To build this, all you need is a GE-3 transistor, a 6.3-volt transformer, and a handful of spare parts from old radios. The ammount of shock you wish to generate is determined by the setting of potentiometer R1, a 15,000 ohm variable resistor. Hint: for maximum shock, set R1 at maximum!

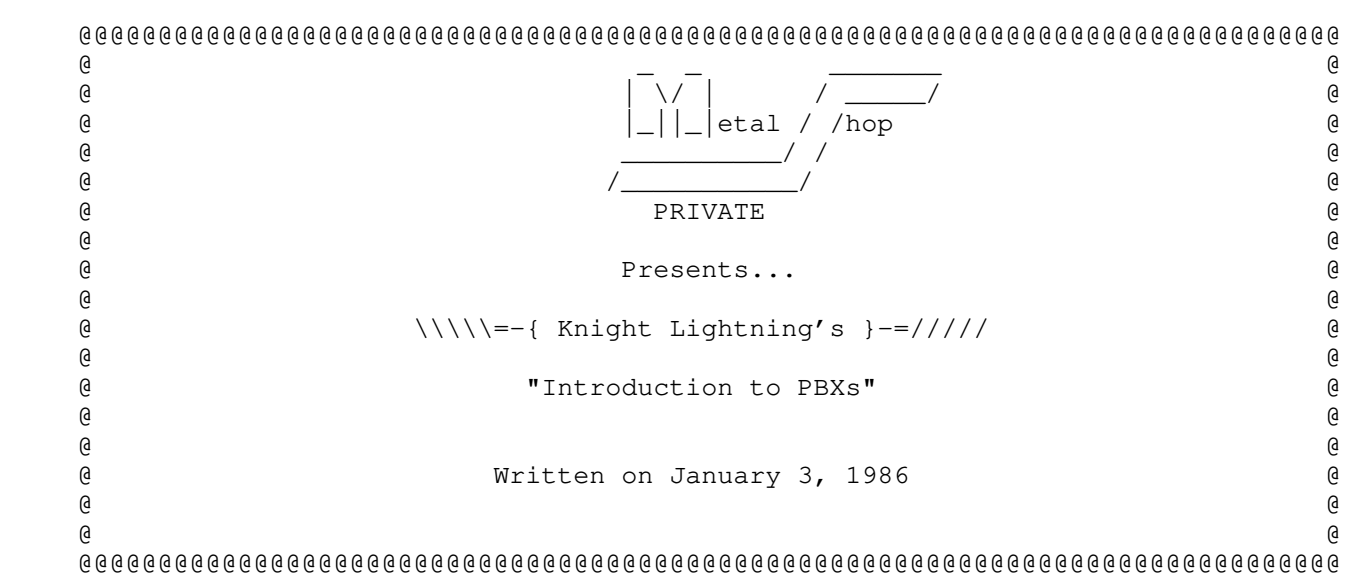
Item	Description
C1	500uF, 10-WVDC electrolytic capacitor
C2	2000uF, 15-WVDC electrolytic capacitor
M1	6-VDC battery
M2,M3	Leads
Q1	GE-3 transistor (2n555 will also do)
R1	15K potentiometer
R2	160-ohm resistor
S1	Spst switch
T1	6.3-VAC filament transformer (Triad F-14x or equiv.)
X1	1N540 diode

Schematics:





==Phrack Inc.==
Volume One, Issue Three, Phile 9 of 10



This file is a personal continuation of the PBX entry in the MCI Telecommunications Glossary.

A telephone exchange serving an individual organization and having connections to a public telephone exchange is called a Private Branch Exchange (PBX). The PBX performs a switching function by connecting any extension in the private organization to an outside line. A PBX is actually a private switch that connects a group of telephones within an individual organization. Calls placed outside this individual group are connected to a telephone company's central office switch through trunks. A PBX may be operated by an attendant from the private organization or the switching system may be done automatically. Other terms that are commonly used interchangeably with PBX are: Private Automatic Branch Exchange (PABX), Private Automatic Exchange (PAX), and Computerized Branch Exchange (CBX). Although these terms were originally used to identify specific switch structures, today they are often used as synonyms.

PBXs can use any of three basic switching methods: step-by-step (SxS), Cross-bar (X-bar), and computer controlled, to perform the basic function of switching. However, in addition to detecting calls and establishing a transmission link between two telephones, PBXs can do much more.

The common control, often called a central processing unit (CPU), controls the switching matrix that connects the stations and trunks. The switching matrix of a PBX performs the same job as does an operator at a manual switchboard or a common control central office switch. The CPU, however, gets its instructions from the "stored program", which contains directions for activities, such as detecting calls, sending them over the best available route, and recording billing information. These computerized electronic switches are used to perform routine, as well as unique, functions that simply weren't practical or even possible with electromechanical switches.

Just as in the public switched network, PBX switches make connection between instruments, or "key telephone sets". We're all familiar with key telephone sets, whether we know them by name or not. They're the business telephones that have six push-button keys lined up below the dial--a red button marked "hold" and five buttons or lines with flashing lights.

Systems with PBXs and key sets have a great deal of flexability in planning for their needs because they can set up their codes to accomplish the functions needed in their particular situations. In fact, the PBX can be programmed so that each individual extension within a system can take advantage of features applicable to its own business needs.

Some of the features that are availiable with PBXs and key systems are: call transfer, which allows internal or external calls to be transferred from one telephone to any other phone in the system; automatic push-button signaling,

which indicates the status of all phones in the system with display lights and buttons; one-way voice paging, which can be answered by dialing the operator from the nearest telephone in the system; camp-on, in which a call made to a busy phone automatically waits until the line is idle; and internal and external conference capabilities, which enables outside callers to conference with several inside users.

Some features automatically handle incoming telephone calls. Automatic call waiting not only holds calls made to a busy extension until the extension is free, but also signals the person being called that a call is waiting and informs the caller that he is on hold. Automatic call forwarding will send calls to employees who are temporarily in locations other than their offices, provided they "inform" the PBX where they can be found. Automatic call distribution automatically send an incoming call to the first extension that's not busy--a useful feature for situations in which any one of a group of persons in the organization can adequately respond to incoming calls. Another example is automatic call back, which allows a caller who reaches a busy line to ask the PBX to return his or her call when the line is free.

Still other features provide services such as night telelphone answering, telephone traffic monitoring, and network or hot-line connection. These examples are but a sample from the features possible with computerized PBXs.

===

This is a very brief description of how to use and what to expect on a PBX.

Basically, you call the PBX and you will have to enter a code that can be anywhere from 4 to 6 digits (Note: some PBXs do not require codes). Then you will hear a dial tone. From here you would under normal circumstances dial: 9 + 1 (or 0) + NPA-PRE-SUFF, for long distance dialing or dial 8 for local dialing.

The most common use of the PBX is to call Alliance Teleconferencing, a teleconference service offered by AT&T. To do this dial: 0700-456-1000,1002,1003,2000,2001,2002.

Note: PBX codes are usually very simple and usually 4 digits.
EX: 0000, 1111, 1234, etc

===

Look for a file on Alliance Teleconferencing coming soon...

This has been a Knight Lightning presentation...

@@@