the protection. If you want to polish the hack (cover your tracks, find passwords, etc.) here's some advanced steps you can take:

* If you know that your sysadmin keeps logs Copy the system folder to the hard drive. Rename the original system folder. Reboot without At Ease. When you are done, put the real system folder back and delete the second one.

* If you aren't concerned about logs, just move the At Ease Preferences out of the System Folder: Extensions folder and reboot. Remember to put them back when you are done.

* Install one of the aforementioned Keystroke recorders. Wait a few days and check the logs from the recorder. You should have the administrator password!

Crashing the System--Another Hack for At Ease lies in Crashing the system it's running on. Just keep opening applications until all the RAM is consumed. On older versions of At Ease, a dialogue box will appear that asking you if you would like to quit At Ease to free up RAM. Click yes!

Null Password--Open the file System Folder:At Ease:At Ease Preferences with MSWord or any ther text editor. Look for the string "MFDR\ ]". Delete everything between "\" and "]". Save the changes and you have a null password. Now you can go to At Ease Setup and change the password to whatever you want!

OEM Hack---The following directions are excerpted from the At Ease Administration Manual from the Section: 'What do I do if I forget my Administrator Password?'

If you forget the At Ease administrator's password, follow the directions below instead of those in the manual. If your startup disk is locked, you'll first need to run the Unlock application on the AT Ease 2.0 Utilities disk to unlock the start-up disk. Consult the manual for information about the Unlock application.

1. Start up your computer from another startup disk.
2. Open the System Folder of your usual startup disk.
3. Open the At Ease Items folder inside your System Folder.
4. Drag the At Ease Preferences file into the trash.
5. Hold down the Option key while you choose Empty Trash from the Special menu.
6. Restart from your usual startup disk.
7. Open the At Ease Setup for Workgroups application.

Note: If you are using an AppleShare server volume as the At Ease disk, your setups may not appear until you reset the At Ease disk to this server volume.

8. Reconnect to the server volume and use the At Ease Disk command to reselect the volume.

Note: Make sure you use the information on the server instead of

replacing it with the information on the startup disk.

9. Add a new password and clue.
10. Make sure the following options set correctly:

    * Allow Remote Administration checkbox
    * Lock Startup Volume checkbox

11. Turn At Ease back on.
12. Quit At Ease Setup for Workgroups."

09. How can I use DisEase to Hack At Ease?

DisEase is a fairly powerful utility for Hacking At Ease. It allows you to manipulate At Ease, break out of At Ease, decode passwords, any number of things that would render At Ease useless. The only problem is on most At Ease protected system you are prevented from finder or floppy disk access, thereby preventing you the ability to run DisEase in the first place. In these situations, follow the above steps for breaking into the Finder, you can then access DisEase and use it to decode the Administrator password.

10. Where can I find DisEase?

DisEase 1.0.....ftp://ftp.eskimo.com/u/a/adrenal/mac/DisEase.hqx
DisEase 3.0.....http://www.tyrell.net/~ibs/Hackr/Cracking/DisEase3.0.sit.hqx

Also you can contact the Author. macpants@aol.com

11. How can I Hack FoolProof?

FoolProof is Macintosh security scheme that uses driver level and Systems Folder protection to prevent against bypassing. Driver Level protection is protection written to the Driver Level of the Hard Disk. At this level, the drive can not be mounted without envoking the protection. This condition will continue to exist as long as the Driver remains intact. Here are some methods of defeating it.:

IMPORTANT NOTE--The FoolProof extension, among other things, intercepts the Restart & Shutdown calls from the System and makes sure to disable any external boot device whenever a Restart or Shutdown is called. To defeat this, when you Restart YOU HAVE TO DO HARD RESTARTS (ctrl-opt-del). When you do hard Restarts no calls are made to the System, and the System is restarted without locking or protecting anything. So be sure to do HARD RESTARTS when hacking FoolProof.

Floppy Boot--As detailed in the beginning of this section, Boot from a floppy with command-option-shift-delete held down. This will prevent the Protected Driver from loading. Once the System is loaded you may need to use a Disk mounting utility to Mount the Hard Drive. Once the drive is mounted, Move the FoolProof Extensions and Prefs out of the System folder and Restart. FoolProof should be disabled.

exit_to_shell--Restart and hit the interrupt switch while the INITs are loading and call an exit_to_shell (see MacsBug section), then Move the

FoolProof Extensions and Prefs out of the System folder and Restart. FoolProof should be disabled.

Find File Hack--If you're started up onto a FoolProof protected system, you'll notice that you probably don't have access to the System Folder. If you did you could drag the FoolProof Extension and Prefs out of the System Folder and Restart without FoolProof protection. Well, believe it or not, the Finder itself provide circumvention around this protection.

1. From the Finder, go up to Find in the Filemenu. Search for 'Finder'

2. Find is nice enough to find Finder for us in the Extension Folder, AND open the Extension Folder for our access. By NO sheer coincedence, the FoolProof extensions just happen to be in the same folder.

3. Drag the FoolProof extensions out of the System Folder and Restart. FoolProof should be disabled.

Note--When you're done with all of the above methods, drag the FoolProof extensions and prefs back into the System Folder and restart. Noone will ever know you were there.

12. How do I access the Chooser when it is protected on Foolproof?

First try the default password 'foolproof'. If that doesn't work, Make a copy of the Chooser and use ResEdit to change the Chooser Creator type from 'dfil chzr' to 'dfil keyc'. This will reset the Password to the default: 'foolproof'. Swap (don't delete) the original Chooser with the modified copy. Now you access the Chooser with the default password. When you're done, cover your tracks by putting back the Original Chooser.

13. How can I defeat Passworded Control Panels?

The single most fundamental way to defeat a passworded Control Panel is to Delete it's preferences. The preferences for any particular program is in the Preferences folder in the System folder. In some cases it may be somewhere else or in other cases the preferences may be invisible. A good program to use to look for a Preferences file (or any file for that matter) is Norton Disk Editor. This program allows you to search for a file by any number of criteria, including attributes (thereby allowing you to search for Invsible files). Once you've found the prefs for the Control Panel you're trying to defeat, delete them (the prefs.) If you can't delete them write over them using a file wiper (see Part #07, File Wipers) Restart. In most cases, whatever Control Panel you were trying to get into will be void of it's password protection. This methods works good for: Screen savers, Virus Programs, some security programs, and Network Managers.

14. How can I defeat the DeskTracy Control Panel (at Kinko's)?

Take a floppy with a File Wiper on it (see Part #07, File Wipers) to Kinko's. Open -> System Folder: Extensions: Desk Tracy Folder Drag the files 'DTPreferences' and 'UData' onto the file wiper. Go up to the Menubar, you should see your Login name up there, drag down to 'Configuration'. Don't change anything, just click the Close Box and it will ask you if you want to

Save. Click 'Yes' Now go up to the Apple Option Menu and Select 'About Desk Tracy'. It should beep at you, and then show you the Desk Tracy 'About' Window. By this process, you have just Returned Desk Tray to it's Virgin Installation State. All accounting is Off, and Desk Tracy is like it was when it was First installed, BEFORE it was configured

15. What is EtherNet or Packet Sniffing?

Ethernet sniffing is listening (with software) to the raw ethernet device for packets that interest you. When your software sees a packet that fits certain criteria, it logs it to a file. The most common criteria for an interesting packet is one that contains words like "login" or "password."

here are a couple of EtherNet sniffers:

Watch 1.7.1.....http://vsl.cnet.com Search: 'sniffer'
EtherPeek Demo...ftp://ftp.aggroup.com/Public/demos

16. How can I EtherNet Sniff on the Mac?

(original by spooty , mods by filbert 4 the machaq faq)
This article will explain how to get someone's password for their unix account etc., from the packets transmitted over a localtalk or ethernet network. I will not bother to explain the difficulties (or impossibilities) of cracking THE password file, or worse yet, shadowed passwords. If you want to learn about these, go read alt.2600 and look at all the lamers asking how to hack the password file in one easy step. What I will give you is the simplest and most powerful way to acquire passwords. Sniffing packets may or may not be punishable where you are. It may be shady behavior, or potentially legitimate. Using someone else's password is obviously a no-no in the eyes of admins, and the law, but then again, if you gave a shit, you wouldn't be reading this. Ready?

First of all, you need a packet sniffer. Just about any sniffer will do. Since this article is aimed primarily at Mac users, I will use Watch 1.7.1, available at the Phruwt ftp site. This app will do nicely. Now, all you need is a Mac and a network, both of which you will have to find yourself.

Any computer at a cluster at any company or university will probably be tied into their network, at least for a local bridge. For older, smaller, or just plain dumber networks, you will be able to access the entire LAN from any computer connected to it. Otherwise you are limited to the particular zone to which your computer is assigned. It shouldn't be too hard to find a good, accessible zone, however. If there is a main computing center at a school, for example, it will probably be both the site of accessible computers AND the same zone that sysadmins use.

Alrighty. Time to get to work. Fire up your sniffer. The default settings on Watch 1.7.1 are fine. Under the "Filter" menu, only "LAP ctrl capture" should be checked. Click "start." Now you will see "packets" and "errors" begin to add up. For the first time, let 50 or more packets pile up before you hit stop. Now look at the packets. They will all have names like AFP, ATP, etc, that will confuse the hell out of your newbie ass if you don't know what they are. Don't worry about them. What you're looking for are the ones which are

labeled by either TCP or Telnet.

Anyone using Telnet to log into an account will have to enter both a userid and a password. This is where your knowledge of terminals comes in. When you're telnetting, or using any terminal-based software, every keystroke you hit is sent to the server, and then the server responds somehow to your screen in the terminal. For example, say you are typing a letter to someone using pine or some other unix mailer. If you type "k", a "k" will be sent to the server, and then a "k" will be sent back to appear on your screen. On the other hand, if you're hitting space bar to advance a page or something, a space will be sent, but the server will not return a space, but rather the next page of text. Got it?

So what you're looking for is the userid/password interaction between the client and server. By watching the packets (and you'll see this quickly), you'll soon find some sucker firing up his account. The first sign will be the server's prompt for the userid, which should be as plain as day. Then the unwitting fool will start typing in his userid, and the server will be displaying it on his screen like this (these are only the last few columns you will see in Watch. For more detail, you can double click on any of the packets):

(In this example, 25 is the server and 69 is the user's computer)

```
lap dst 69 lap src 25 Telnet: 'login:'
lap dst 25 lap src 69 Telnet: 'l'
lap dst 69 lap src 25 Telnet: 'l'
lap dst 25 lap src 69 Telnet: 'o'
lap dst 69 lap src 25 Telnet: 'o'
lap dst 25 lap src 69 Telnet: 's'
lap dst 69 lap src 25 Telnet: 's'
lap dst 25 lap src 69 Telnet: 'e'
lap dst 69 lap src 25 Telnet: 'e'
lap dst 25 lap src 69 Telnet: 'r'
lap dst 69 lap src 25 Telnet: 'r'
```

Of course anyone typing any words will look like this, so you have to be sure this punk is logging in and not just blabbing about himself to his fat girlfriend back home. So make sure he has received the login prompt before this, by paying attention to the source and destinations of each packet (dst and src). Also, all the packets may not be together like this. A lot of other shit might be mixed in, so once again, lay off the crack and make sure the packets you're looking at are all going to and from the same places (note: the number for the server will just about always be the same and the varying clients' addresses will differ).

Now when it's time for the password:

```
lap dst 25 lap src 69 Telnet: 's'
lap dst 69 lap src 25 Telnet: ' '
lap dst 25 lap src 69 Telnet: 'm'
lap dst 69 lap src 25 Telnet: ' '
lap dst 25 lap src 69 Telnet: 'e'
lap dst 69 lap src 25 Telnet: ' '
lap dst 25 lap src 69 Telnet: 'g'
```

lap dst 69 lap src 25 Telnet: ' '
lap dst 25 lap src 69 Telnet: 'm'
lap dst 69 lap src 25 Telnet: ' '
lap dst 25 lap src 69 Telnet: 'a'
lap dst 69 lap src 25 Telnet: ' '

Where, you ask, are the missing letters? They don't show up, because the server doesn't reveal them on the user's screen, so the ol' peeking over the shoulder technique won't work, unless you can follow someone's typing fingers, which is hella difficult.

Okey dokey. You've got your userid and password. Go have fun now.

Unless, of course you want to hear about the other fun you can have with a sniffer. Say for example, you're trolling around and see someone is reading PORNO stories on usenet. One time I found this kid reading stories about some little boy getting off by being spanked by his mom. What a fucking weirdo! Anyway, you can pinpoint who is doing what pretty easily. Use another program, like Trawl or Interpoll, and you'll be able to see what every locally networked computers' addresses are. Usually you can get the owner name too. Also, you can set Watch to filter out everything except the traffic between two addresses. This is particularly useful, because most of the time there will be so much fucking trash flying back and forth, that it will be difficult to wade through it all.

This method is sort of a bitch to use, because you may have to just wait and be lucky to get the password. You can be sneaky though like this:

Call some bastard up whose password you want. Be at a computer, if necessary in his/her zone.

You: "Hey Jerky, didja get that kewl mail I sentya? Them: "Uh, let me check..."
(Fire up your sniffer and do it quick!)
Them: "Hold on..."
(click, click, click, as they type away) Them: "All it says is 'hi.'"
You: "Oh whoops, I'll have to send it again. Bye."

Hang up, stop the packet collection and you've got paydirt.

If someone uses a desktop based mailing program, like Eudora, the collecting account passwords is even easier. The packets will be marked "TCP" instead of "Telnet" and in the text of the packet (you'll have to check the full details of the packet for this) you'll find the whole text of the userid's and passwords inside.

Sniffers are good for a lot of other shit too, so play around with them and see what you get. Unfortunately, Apple Fileserver (AFS) passwords are a bear to get, since they are usually two-way scrambled (sys 7.1 and higher, I believe). I'm trying to figure out the encryption, but it's not really my department. In any event, someone's account password will very often be their server password too.

Although some systems are switching over to Kerberos protected transmission

of all packets across their LANs, most are still wide open. Doing something butt-stupid, like changing someone's password on them, will only result in them getting back into their account in a matter of hours, so be creative. It's pretty fun just to watch (hence the name) the dark sides of all the people you know. Then go up to them and say shit like, "Spank much lately?" Have fun with this, and don't get caught.

17. How can I defeat a FileGuard protected system?

FileGuard is a powerful and versatile security system for the Mac that uses Driver Level protection, Encryption and Owned Finder Resources to provide controlled access to Protected system. In defeating FileGuard completely you'll need to be able to eliminate the protection, and decrypt protected filed.

Basic FileGuard Hack--FileGuard protection can be somewhat confusing. The install process requires installing FileGuard onto a HardDisk, and then installing the Driver Level protection of FileGuard after the initial install has been performed. Because of this, and because of the way FileGuard acts after the initial install, someone unfamiliar with FileGuard can easily be left with the impression that his or her system is protected, when in fact the Driver Level of FileGuard's protection has not beeen installed. Without the Driver Level protection the FileGuard can be defeated by disabling extensions. So to start, ry Restarting with the Shift-Key held down. If the Driver Level protection of the system has not been installed, then you will have unprotected access to the system.

FileGuard 2.7.x Hack--If the Driver Level of FileGuards protection has been installed on the system, the only way to defeat the protection is to Hack the password or to remove the Driver altogether. Password hacking is discussed in more depth in the section on FileGuard 2.9.x. It is discussed their ecause it is much more viable for that version of FileGuard. For this version (2.7.x), the most viable way to defeat the security is to remove the Driver altogether.

To remove the Driver you'll need to make an HD floppy Start up disk that has a SCSI Driver utility on it. This is easy task given the amount of information you need to cram on to a single 1.44mb Floppy. To aid you in making this special floppy, I suggest you go by LaCie's home page and check out how they suggest you do it.

LaCie.......http://www.teleport.com/~lacie/makestarter.html

This page can provide you insight on how to make a SCSI Driver Install disk for use in FileGuard and other driver level protection hacking.

Try the following as a LAST RESORT:

1. Get a high density disk. Install some startup software for the machine in question. Install some disk formatting software that ets you install new drivers (like Gold Triangle, Apple HD SC Setup, or Silver Lining).

2. Restart, holding down command-option-shift-delete. This prevents the SCSI Bus from trying to mount the internal hard disk.

3. Run disk formatting software and install a new driver over the old driver.

4. Restart. No password should be prompted for.

NOTE--This process will probably cause the hard disk to crash severely in the future!!! Only do this if there is something you really need on the disk. After you copy the needed files to a different place, you should REFORMAT THE HARD DISK.

FileGuard 2.9.x Hack--In the 'FileGuard 2.9 addendum' which highlights changes in the latest release of FileGuard, it states:

'FileGuard now allows you to customize the message that appears whenever the volume password is requested.'

. . . . . .

'Unless you checked the option 'Ask volume password at startup' (see below), the volume password is only requested when the FileGuard extension is not active (for example, if someone tries to boot with extensions off to bypass FileGuard). Since the volume's password is not regularly requested, you may also wish to customize this message to include some kind of reference which will trigger your memory in case you forget the volume password. Be sure not to type in an obvious reference that could let others easily guess the password.'

What a give away. Heres how this hack would (potentially) work:

Normally, if a system is FULLY protected by FileGuard, when you Start up a dialog will appear requesting a NAME and an ACCESS KEY. You're given three opportunities to get it right or the System Restarts and you go through the same thing again.

Now, if you try and Restart with the Shift-Key held down, the system will load WITHOUT Extensions and without the FileGuard Control Panel. But even without the Control panel, the System is still protected by the Driver Level portion of FileGuard's Protection (provided Volume Protection has been installed). But the Driver Level portion of Fileguard's protection is less secure and for two reasons:

1. The Driver Level protection puts up a message (as stated in the above mentioned 'addendum') which may, in and of itself, contain the password.

2. The Driver Level protection doesn't ask for a NAME, only a VOLUME PASSWORD, thereby eliminating part of the guess work.

So, boot up a FileGuard system with the Shift-Key held down, read what the FileGuard says, and start using the words within the dialog as potential Passwords to the Volume. If that doesn't work, try possible single word passwords (remember, you only have to enter one word). With a little effort you might just exploit a vulnerability.

FileGuard Encrypted Files--Use FileGuard to encrypt a file with the password

'test', for example. Use ResEdit to copy the resource 'high' from that file. Paste it into the file that contains the unknown password. Save changes and quit. Decrypt the modified file with FileGuard using the password 'test'.

SECTION III: SYSTEMS HACKING

18. How Can I hack FirstClass?

FirstClass Defaults--Theirs only one FirstClass default I know of and it's a doosie. Every FirstClass system comes with the Administrators account:

USER: admin
PASS: admin

The FirstClass Administration Manual very clearly states that the first thing you are REQUIRED to do after Installing your FirstClass server is CHANGE this password. But because of the way FirstClass is designed, it is often overlooked. When you've installed your Server and loaded up the FC Client Admin settings that come with the server, you never have to enter a password. Its already saved into the Settings. So all you do is click Login and you're in. And when first configuring a FirstClass system there are ALOT of things to address and an inexpereinced Admin (as most Admins setting up an FC system are) will often overlook changing this default account.

Password Dig--Theres a utility called FirstClass Digger 1.x which will dig passwords out of the FirstClass server. This utility is available at via SoftArc Online. For more info on SAOL goto the SoftArc home page: http://www.softarc.com

Admin Password Dig--There is one way to hack FirstClass if you have physical access to the server. To do this, you first open the root level of the hard drive and then open the folder named "FirstClass Post Office". The locate the foldernamed "UserDir" and open that. From there, open the folder named "admin.". Then copy the file named .ENProf onto a disk. When you have the time, open it up with Microsoft Word. To do this, you must change the "Show" pull-down menu from "Readable Files" to "All Files" and THEN locate the .ENProf. You will see the admin's password around the fourth or fifth line. If the admin. is using a shorter password than he used to, then you will see his password, followed by the correspoding characters of his old password. I.E., if someone changed their password from "systemadmin" to "admin." it would look like "adminmadmin". If you do not get on with the whole string listed, try passwords by taking the last letter away until you get it. You can now give yourself Administrator privs. From there, you can do everything the real admin. can do, EXCEPT open the Admins desktop, and grant other users admin. privs.

Admin Accounted Settings--Another one I've seen, is when a FirstClass Admin is setting up a new Server, one of the things they can do to add to the look of their System is make custom Settings file. Well this Custom setting file is usually just the Admin settings file modified. They modify it a ittle bit at a time, and then to check to see how it looks they'll login to their system. For the sake of ease they'll go ahead and have the Username and Password saved so all they have to do to test the setings after a modification is click Login (cuts down on the time required to enter the name

and password). Well after a few hours or days of making the perfect settings file, they're tired, and happy and releived and whole bunch of other things that lead to distractions. They think they're done, and they Stuff their settings file and distribute it on BBSs or the Internet so people can use the settings to access their FC system. What did they forget to do? They forgot to delete the Admin username and password from the settings file. By the time they've found out, someone has already logged in with the uAdmin account (all they had to do was click Login), accessed the Hard drive, found their way to the DTP or Acconting folder, and stolen confidential or personal files.

FC Time Limit Hack--Next time you're logged into a FirstClass system be sure to go upto view and select Session Status. Keep track of your time. When you're time is almost up, go up to the menu bar and hold a menu open. The System won't log you off under these this ondition. Wait for about 30 seconds past the time you're supposed to be logged off. Let go of the menu and you'll still be logged on and can stay logged on indefinitley.

19. What is UNIX Password Hacking?

Traditionally stated, the purpose of hacking a UNIX is: to "get to ROOT." This refers to the ROOT account that every UNIX system has as part of it's Operating system. The ROOT is a 'Trusted User' account, THE most powerful account on a UNIX. If you can hack a ROOT you can utilize or exploit every function a UNIX is capable of. But to get to "ROOT" you have to have somewhere to start. one of the most common places to start is with the 'passwd' file.

'passwd' is the common name of the file in which user account information is stored on a UNIX system. You might consider it a comprehensive users list. The file contains the information for an accounts USERNAME, PASSWORD, USER NUMBER, GROUP, GECOS, HOME DIRECTORY, and SHELL. A single entry of a passwd file entry might look like this:

```
                 PASSWORD        GROUP NUMBER    HOME DIRECTORY
                /               /               /
               /               /               /
  kbahadur:8d34jSjs73hsb:2162:15:Ken Bahadur:/usr/users/kbahadur:/usr/bin/ksh
   \                      \             \                            \
    \                      \             \                            \
     USERNAME               USER NUMBER   GECOS INFORMATION           SHELL
```

Now then, if you can see this:

```
           encrypted equivalent of pasword
             /
kbahadur:8d34jSjs73hsb:2162:15:Ken Bahadur:/usr/users/kbahadur:/usr/bin/ksh
```

...you can use a passwd' file crackers to "guess" the password to this account entry. Once you've guessed an accounts password you can use that account to try and hack root. Try theses common commands on a UNIX to attempt to steal the 'passwd' file.

```
UNIX 4.x.................cat /etc/passwd
AiX......................cat /etc/security/passwd
yp/NIS (yellow pages)....ypcat passwd
```

20. How Can I do it on the Mac?

'passwd' File Crackers--Hacking UNIX can be done on any machine, the only place where it can become localized (like on your Mac) is in the process of hacking 'passwd' files. To hack a 'passwd' file on a Mac, you need a password file cracker FOR the Mac. A few such programs are:

MacKrak 2.0b1.....ftp://ftp.armory.com/pub/user/swallow/
MacCrac v.01a.....http://iti2.net/k0p/mac_u-g/MacCrac%20FAT%200.1A.sit.bin
Killer Cracker 8.0....http://www.tyrell.net/~ibs/Hackr/Hacking

Word Lists--To use the above listed 'passwd' file crackers you need Dictionary or Word List files. MacCrac comes with a fairly large Dictionary (2meg), but for the other programs you need to find your own. Paul Leyland runs Word List f*ckin' central. Hes got hundreds of Word Lists for dozens of nationalities and criteria, for example: Star Trek, Swahili, American, French, Names, Dog Names, just a shit load. check him out:

Word Lists.....ftp://ftp.ox.ac.uk/pub/wordlists/

Word List utilities--You can combine several different word lists to make custom Dictionaries for special (hacking) occassions. A utility that can bring considerable ease ease to this task is Word List Maker. Word List Maker is a 'drag&drop' utility to create sorted lists of words from arbitrary text files. You can drop several text files and/or custom MS-Word dictionaries on to the WordListMaker icon to create a single word-list. You can also exclude arbitrary words from the output file. It will combine 2 or more Word Lists, alphabetize them and delete the duplicates.

WordListMaker v1.6....ftp://mirror.apple.com/mirrors/Info-Mac.Archive/text

SECTION IV: PHREAKING
---

21. What is phreaking?

Phreaking is the exploration, use, abuse, and/or defraudment of the telephone system via the manipulation of telephone system circuits, switches or services. Phreaking is commonly performed by generating tones which allow you to utilize various functions of the phone system usually reserved for internal use. The afforementioned tones can be generated by software programs designed to perform this purpose. These warez are commonly referred to as 'phreaking warez'

22. What are some phreaking warez for Macs?

FoneTone Pro v1.0--FoneTone Pro v1.0 is a United Kingdom Blue Boxing program. Blue boxes use a 2600hz tone to size control of telephone switches that use in-band signalling. The caller may then access special switch functions, with the usual purpose of making free long distance phone calls, using the tones provided by the Blue Box. Depending on who you ask, most people will tell you Blue Boxing is no longer possible in the United States. It is, however, still widely performed in Europe.

FoneTone Pro v1.0
http://www.tyrell.net/~ibs/Hackr/Phreaking/FoneToneProv1.0.sit.hqx

MacPhoney--MacPhoney is a RainBow box emulator. That is, it's a box that performs a number of different boxing tones. These tones include Green Box--pay phone tones, Red Box--pay phone toll tones, White Box--AutoVon tones, and TouchTones--standard dialing tones.

MacPhoney
http://www.tyrell.net/~ibs/Hackr/Phreaking/Phoney4Mac.sit.hqx

23. How can I use these programs?

Mac Phreaking programs work by producing tones which when played through phone lines will have the potential of exploiting functions of the phone system. The generated tones are produced through the Mac speaker. For the tones to be effectivley played through the phone line, it is best to have the phone line connected to the Audio Out jack of your Mac or Newton. The best illustration of how this is done comes from Mr. Upsetter in a Submission made to and published in Phrack 38.

AUDIO LINKS
~~~~~~~~~~~
By Mr. Upsetter

It all started with my Macintosh...

Some time ago I had this crazy idea of connecting the output from the audio jack of my Macintosh to the phone line. Since the Macintosh has built in sound generation hardware, I could synthesize any number of useful sounds and play them over the phone. For instance, with a sound editing program like SoundEdit, it is easy to synthesize call progress tones, DTMF and MF tones, red box, green box, and other signalling tones. So I set out to do exactly this. I created a set of synthesized sounds as sound resources using SoundEdit. Then I wrote a HyperCard stack for the purpose of playing these sounds. Now all I needed was a circuit to match the audio signal from the headphone jack of my Mac to the phone line.
~~~~~~~~~~~