This is still the first official version.
I am hoping to make it much longer if I can get submissions.
Too many test to revise it now. will later when get more info. hurry
up and submit, bastard shit.

Archive-name: mac-hack-faq
Last-Modified: 11/22/1994
Version: 0.5

```
---=====++++++++++++++++++++++++=====---
   --===+    Mac Hack FAQ:   +===--
      -=+ Defeating Security +=-
        ++++++++++++++++++++
```


Compiled
by
AX1P
an149689@anon.penet.fi
with extra-special thanks to:
Bubba "Anderson" Sanchez, III esq.
SwordSlinger(an146315@anon.penet.fi)
The Psychedelic Sloth
MacHacker
Chaos
Imbellis
Numerous anonymous contributors...

xxxxxxxxxxxxxxxxx-==**< THE MACINTOSH HACK FAQ INDEX >**==-xxxxxxxxxxxxxxxxx

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
x

A. NOTES

This FAQ deals primarily with defeating security programs for the Macintosh, but there is a lot of room for expansion. If you have any hacks for Mac security programs, ideas for extending the scope of the FAQ or any other feedback, send mail to the faq-maintainer, AX1P at: an149689@anon.penet.fi. Right now I am interested in steering the FAQ towards defeating password protection for various compression programs and defeating copy protection so send in those submissions. I also would like to thank Bubba "Anderson" Sanchez, III esq. for writing the entire article on bypassing HD driver protection. And thank you to everyone who submitted their hacks and encouragement.

COMMON SENSE DISCLAIMER:
I can not held responsible for any damage that might occur from experimenting with the techniques herein. Some may be completely wrong, others may only work on certain macs and particular versions of software. If you screw something up, it's your ass. Run like hell and/or play computer illiterate. I do not support breaking laws of any race, creed or short-sightedness...

B. WHAT ARE THE GENERAL TECHNIQUES FOR BYPASSING MAC SECURITY MEASURES?

*** Disable System Extensions by holding down the Shift-key during start-up. This is one of the easiest techniques but you would be surprised how often it works! On Classics, try booting up off the ROM disk by holding down Command-Option-x-o during boot-up.
*** Find the Finder. On some "secured" systems, you can gain access to locked folders if you now the name of an unlocked file within. For example, here is a FoolProof hack:
    1) Search for the word 'finder'(a file we know is in the locked system folder).
    2) The locked file opens to display the Finder file. From here, you can now move the FoolProof Preferences and Extensions out of the system folder.
    3) Reboot.
*** Break into the debugger by hitting the programmer's switch or the Command-Power key combo. Then type 'G FINDER', or 'G F'. You can also get to the debugger by holding down the control-command-power key combo and restarting.
*** Crash the system! In some older security programs, you can get to the finder by repeatedly opening applications until all the RAM is consumed. Older versions of At Ease will open a dialogue box that asks if you would like to quit At Ease to free up RAM. Click yes!
*** Boot from a floppy. Even if your sysadmin has floppy startup disabled, you should be able to force it by holding down the command-option-shift-delete key combo to boot the floppy. This key combo won't let the internal hard drive mount
*** Plug an external hard drive into the SCSI port. Even if your sysadmin has disabled floppy access and starting up without extensions you
can copy any programs on the drive if you know any of the passwords.
*** Social engineering is almost too obvious (and cliche) to mention, but it seems to work. Remember to act computer stupid and/or get really pissy.

C. WHAT DO I DO AFTER I GET TO THE FINDER?

So you have finally found the finder...now what? Now you can run any programs you want, but why not make things easier on yourself for your next trip to the finder. If you know that your sysadmin keeps logs:

1) Copy the system folder to the hard drive.
2) Rename the original system folder.
3) Reboot without At Ease.
4) 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. The logs have been bypassed but you really don't care to be rebooting over and over while the lab monitor glares at you. It would be much better to have the system supervisor's password so you can switch back and forth between At Ease and the finder at will. The easiest way is to install a keygrabber, which is a system extension that logs and captures all the keystrokes on the computer. Oasis is a good keygrabber for the mac that can be found on the internet or alt.2600. Unfortunately it has no documentation. To use it:

1) Get into the Finder and copy Oasis into the folder:
   System Folder:Extensions
2) Wait a few days.
3) Look for the logfiles in:
   System Folder:Preferences:~Temporary Folder.

Another keygrabber that is easier to find is MacLifeInsurance. You will have to weed through several hundred pages of inane poetry, reports and e-mail to Grandma but eventually one will have the password. If there are large number of users, you may be able to add your own account and password with the supervisor's password. Use your discretion. And look for those keygrabbers on local boards and ftp sites.

D. HOW DO I BYPASS HARD DISK DRIVER PROTECTION (for example: FileGuard's Volume Protection)?

Hard disk protection lies in a hard disk's driver code, at a very low level on the disk. This protection is provided by most third party hard disk formatting software or elaborate security software(like FileGuard). Here's a quick guide to permanently removing this protection:

1) Get a high density disk. Install some startup software for the machine in question. Install some disk formatting software that lets you install new drivers (like Gold Triangle; maybe even 'Apple HD SC Setup').
2) Reboot machine. Quickly insert the floppy disk and then hold down command-option-shift-delete. This prevents the SCSI Bus from trying to mount the internal hard disk.
3) When the finder loads, run disk formatting software. If you want to trash the contents of the hard disk, just re-format the disk. If you want to get at the contents, install a new driver over the old driver (consult your software manual).

If you need to diasable additional security at the hard disk, go to 4). Else, go to 5).

4) Reboot machine; boot from floppy again. This time, let the hard disk mount. If all went well, no password will be prompted for here. When finder loads, remove the security inits/cdevs/programs.
5) Reboot machine; boot from hard disk. No password should be prompted for, and life should go on as usual.

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.

This has been tested with FileGuard protection using Golden Triangler. The tester backed up the source code he was working on, and then continued using the machine(llsi). The machine crashed within an hour.

E. MISCELLANEOUS HACKS AND INFO

Q: HOW DO I COPY A READ-ONLY FILE?
A: Many utilities allow you to copy read-only files, including StuffIt, Compact Pro, etc.

Q: HOW DO I ACCESS THE CHOOSER WHEN IT IS PROTECTED ON FOOLPROOF?
A: First try the default password 'foolproof'; Yes, some sysadmins are that dumb. If it doesn't work, try this:

1) Make a copy of the chooser.
2) Use ResEdit or another resource editor to change the creator code from 'dfil chzr' 'dfil keyc'.
3) The default password is reset to 'foolproof'.
4) Swap the original chooser with the modified copy. Remember to cover your tracks and replace the original chooser when you are done.

NOTE: Make sure you work on copies when using ResEdit, especially when you are using someone else's computer.

Q: HOW DO I DEFEAT FILEGUARD'S ENCRYPTION?
A: 1) Use FileGuard to encrypt or copyguard a file with the password 'test', for example.
2) Use ResEdit to copy the resource 'high' from that file.
3) Paste it into the file that contains the unknown password.
4) Save changes and quit.
5) Decrypt the modified file with FileGuard using the password 'test'.

Q: WHERE CAN I GET THE LATEST VERSION OF MACPGP AND THE SOURCE CODE?
A: Telnet to net-dist.mit.edu and login as 'getpgp'. You will have to answer four short questions to get the name of the file it is in(the name changes every half hour). Then ftp there and go to the specified directory. The current version is MACPGP2.6.2. You should also get the README files as the interface barely follows the Macintosh Interface Guidelines.

Q: HOW DO I SET A NULL PASSWORD FOR AT EASE(not all versions)?
A: 1) Open the file System Folder:At Ease:At Ease Preferences with MSWord or any other text editor.
2) Look for the string "MFDR\ ]".
3) Delete everything between "\" and "]".
4) 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!

Q: WHAT DO I DO IF I FORGET THE ADMINISTRATOR'S PASSWORD[in At Ease]?
A:

"IF YOU FORGET THE ADMINISTRATOR'S 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.
[...BS...]
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 aplication.

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.

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."

>> Where do you get the Unlock application? Beats the hell out of me.

F. RELATED ANONYMOUS FTP SITES
==========

There seems to be a serious lack of accessible FTP sites that carry Macintosh hacking utensils, etc. I have hardly found any that I can post. If you have a site to add to this list or you are interested in creating a Mac Hack FTP site, please contact an149689@anon.penet.fi

* SITE: net-dist.mit.edu
* PATH: ?
* FILES: MacPGP2.6, MacPGP2.6 source code
To get the path, you must telnet to net-dist.mit.edu and login as 'getpgp'. You will have to answer four short questions to get the name of the directory it is in(the name changes every half hour). You

should get the README file as the interface barely follows the
Macintosh Interface Guidelines.

* SITE: ftp.netcom.com
* PATH: /pub/bradleym
* FILES: MacRedBox, VirtualQuarter, ...
Not much in the way of a Mac ftp site but it has four or five phreak
utilities.

* SITE: sekurity.com
* PATH: /pub/incoming
* FILES: unknown
Sometimes they have mac stuff. They used to have Oasis... Just look
for the familiar .hqx or .sit suffixes.

*   S E N D   M O R E   F T P   S I T E S ! ! !
* Sorry, that's all I can post now! Keep an eye out for MAQ HAQ FAQ
* update which I hope will come out after my mailbox is flooded with
* your voluminous submissions. I thank everyone who has already
* contributed or sent their feedback and I hope you find the above
information
* useful.

EOT