Chapter 2- The Tools of Cracking

As I mentioned earlier you will need certain programs to help you along in the deprotection process.

MacsBug: Is a full-featured debugger that allows you to set traps in programs and then trace through instruction by instruction. This is an immeasurably useful program. It has loads of commands, but I only use these commands for cracking:

atb [trap] ; lets you set a trap that which will break you into MacsBug if the program tries to exectute it. Mac Traps are from A000-AFFF and do many different things like _Eject & _ExitToShell and stuff like that.
atc ; this will clear all of the traps t hat you set with atb
es ; quit current application and exit to shell
ea ; quit current application then launch it again
G ; go. Continue the application as normal. Turn off MacsBug.
GT [addr] ; lets you GO from a selected address.
il [addr] n ; lists from selected address "n"= number of lines
? ; This displays the online help file, very useful

These are the commands I use most of the time. There are other commands which are more complicated and do some special things but there is no need to explain them here. I will do that in a future issue.

FEdit 3.21: This is a very good sector/file editor with good search functions for finding certain code and changing it. This is very much like any other editor so there is no need to explain its functions.

DisAsm 3.1: This is a disassembler, the only one I have seen on the Mac so far and it works pretty good. All functions are operated from the Menus, but the main ones I use are the Search functions. Like finding certain traps, are certain addresses. I don't really use this much but if needed it is good to have a disassembler around. Sometimes MacsBug won't quite work if a program steals memory away from it and DisAsm must be used as a last resort.

Programmer's Key: This is a nifty little INIT that lets you invoke MacsBug from the keyboard. Basically you hit the Command-Reset keys and it dumps you into MacsBug, you can also hit Control-Command-Reset to restart your computer. Which is kind of neat. I recommend using this instead of the hardware interupt switch on the machine itself, mostly because its a pain to keep reaching in back of your machine to do it.