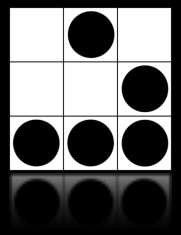


Mac OS hacX

Things you need to know about your Mac

Alessio L.R. Pennasilico

mayhem@alba.st

Pescara, 22 Agosto 2008

$ whois mayhem

Security Evangelist @ 

Member / Board of Directors:

AIP, AIPSI/ISSA, CLUSIT, Italian Linux Society, IT-ISAC, LUGVR, OPSI, Metro Olografix, No1984.org, OpenBeer, Sikurezza.org, Spippolatori, VoIPSA.

CrISTAL, Hacker's Profiling Project, Recursiva.org

Credits

These slides are possible thanks to the help of some Italian hackers that always love to share information:

Andrea Ghirardini, pila@pilasecurity.com

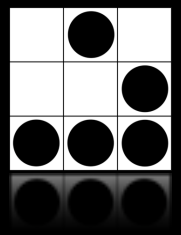
Guido Bolognesi, zen@kill-9.it

Matteo G.P. Flora, lk@lastknight.com

“Those who don't understand UNIX are condemned to reinvent it, poorly."

Henry Spencer

Apple MAC AD



How to obtain a more secure environment using MacOSX?

Screensaver

Alessio L.R. Pennasilico

Autologon

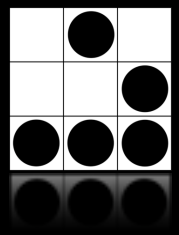
Alessio L.R. Pennasilico

Pair remote control

Alessio L.R. Pennasilico

Malware

Alessio L.R. Pennasilico



Library Randomization

How security is changing?

From buffer overflow to application flaws…

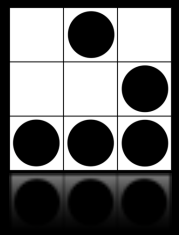
"… and nowadays a ssh remote root is a dead dream..."

anonymous

Apple solution to BO

Library Randomization randomly distributes those commands throughout memory every time the operating system loads.

Thus, even if an attacker finds a buffer overflow vulnerability and pushes his commands onto your system, it's extremely difficult for him to turn that into a working exploit.



SandBoxes

SandBoxing

Think about isolating a baby

in a place where he can play

Do the same with an application!

Web Malware

Malware can compromise my browser

But my browser must not access

all my system resources

Policy

We can create some rules:

the browser will only access

authorized resources

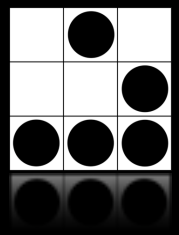
It is native on MacOSX:

```
coniglio:~ mayhem$ man sandbox-exec

coniglio:~ mayhem$ cd /usr/share/sandbox/

bsd.sb                portmap.sb    named.sb
mDNSResponder.sb      ntpd.sb       syslogd.sb
```

and simple to use

```
$ sandbox-exec  -f profile-file applicazione
```

```
$ cat /usr/share/sandbox/named.sb
(allow network*)
(allow file-write* file-read-data file-read-
metadata
  (regex "^(/private)?/var/run/named\\.pid$"
         "^/Library/Logs/named\\.log$"))
```



Access Control List

File system

The file system is HFS+

Provides journaling

access-list and extended attributes

/bin/ls -l

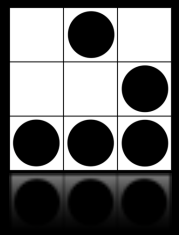
```
coniglio:~ mayhem$ /bin/ls -l
total 24
drwx------+  8 mayhem  mayhem   272 May 13 18:45 Desktop
-rw-r--r--@  1 root    mayhem  1024 Dec 10 10:41 Desktop DB
-rw-r--r--@  1 root    mayhem     2 Dec  9 23:11 Desktop DF
drwx------+ 35 mayhem  mayhem  1190 May  8 19:40 Documents
```

/bin/ls -el

```
coniglio:~ mayhem$ /bin/ls -le
total 24
drwx------+  8 mayhem  mayhem   272 May 13 18:45 Desktop
 0: group:everyone deny delete
-rw-r--r--@  1 root    mayhem  1024 Dec 10 10:41 Desktop DB
-rw-r--r--@  1 root    mayhem     2 Dec  9 23:11 Desktop DF
drwx------+ 35 mayhem  mayhem  1190 May  8 19:40 Documents
 0: group:everyone deny delete
```

/bin/chmod

```
# chmod +a "admin allow write" file1

# chmod +a "guest deny read" file1

# ls -le

-rw-r--r--+ 1 juser  wheel  0 Apr 28 14:06 file1

  owner: juser

  1: guest deny read

  2: admin allow write
```



Monitor

Why monitoring?

It's always important to know

what a binary program tries to do

both from a security point of view

and from a performance point of view

It is important to know

which file are created / accessed / deleted

how much CPU / memory is used

lookup thread / child processes

network activities

dtruss

Used to run strace on your PC?

Did you find an unknown binary?

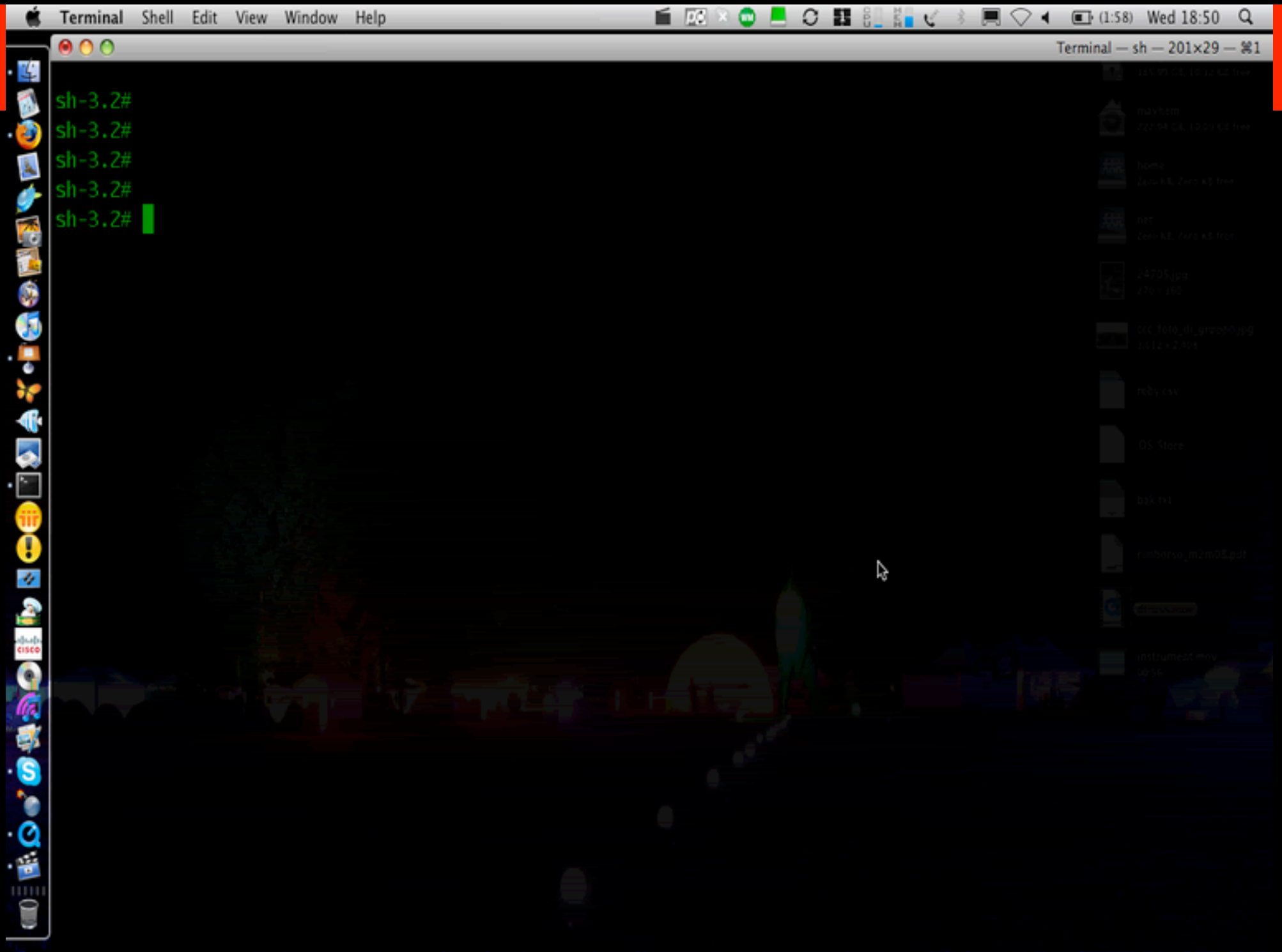
```
root@coniglio# dtruss /bin/ls
```

Running processes

It is possible to attach dtruss to

already running processes

to monitor syscalls


Terminal Shell Edit View Window Help
(1:58) Wed 18:50
Terminal — sh — 201×29 — ⌘1
sh-3.2#
sh-3.2#
sh-3.2#
sh-3.2#
sh-3.2#

dtrace

It is useful to create profiles

of system wide parameters to monitor

Pre-compiled libraries can be found:

http://www.solarisinternals.com/si/dtrace/

Instruments

It is the GUI provided by Developer Tools

It analyzes any activity of running

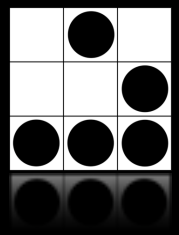
or new launched applications

Instruments screencast

Default processes

It is important to know what are the default system services. A comprehensive and updated document can be found at:

http://www.westwind.com/reference/OS-X/background-processes.html



Firewall

Tiger or 10.4

Traffic based firewall

BSD IPFW product

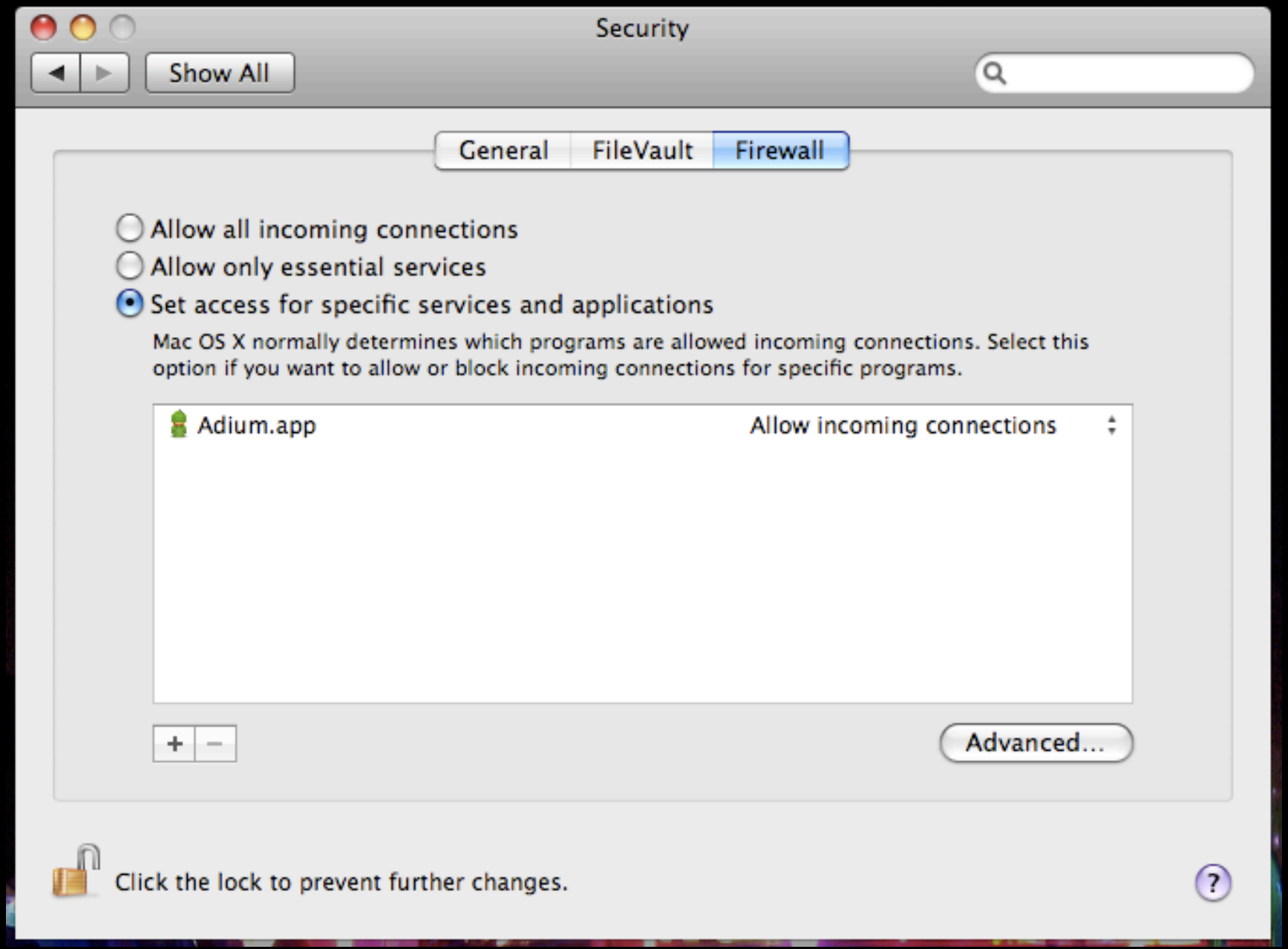
Powerful and flexible

Complex syntax for a *normal* user

Leopard or 10.5

Application based firewall

Configuring a firewall?



Application Firewall

It puts a signature file inside the application

Some applications check their integrity

Some applications stop working

From AppFW to IPFW

Thanks God: IPFW is still present

You can use it from command line

IPFW

```
root@coniglio# ipfw -h

ipfw syntax summary (but please do read the ipfw(8) manpage):

ipfw [-acdeftTnNpqS] <command> where <command> is one of:

add [num] [set N] [prob x] RULE-BODY

{pipe|queue} N config PIPE-BODY

[pipe|queue] {zero|delete|show} [N{,N}]

set [disable N... enable N...] | move [rule] X to Y | swap X Y | show
```

IPFW GUI

Simpler interface = fewer errors

Simple interface = more users

WaterRoof

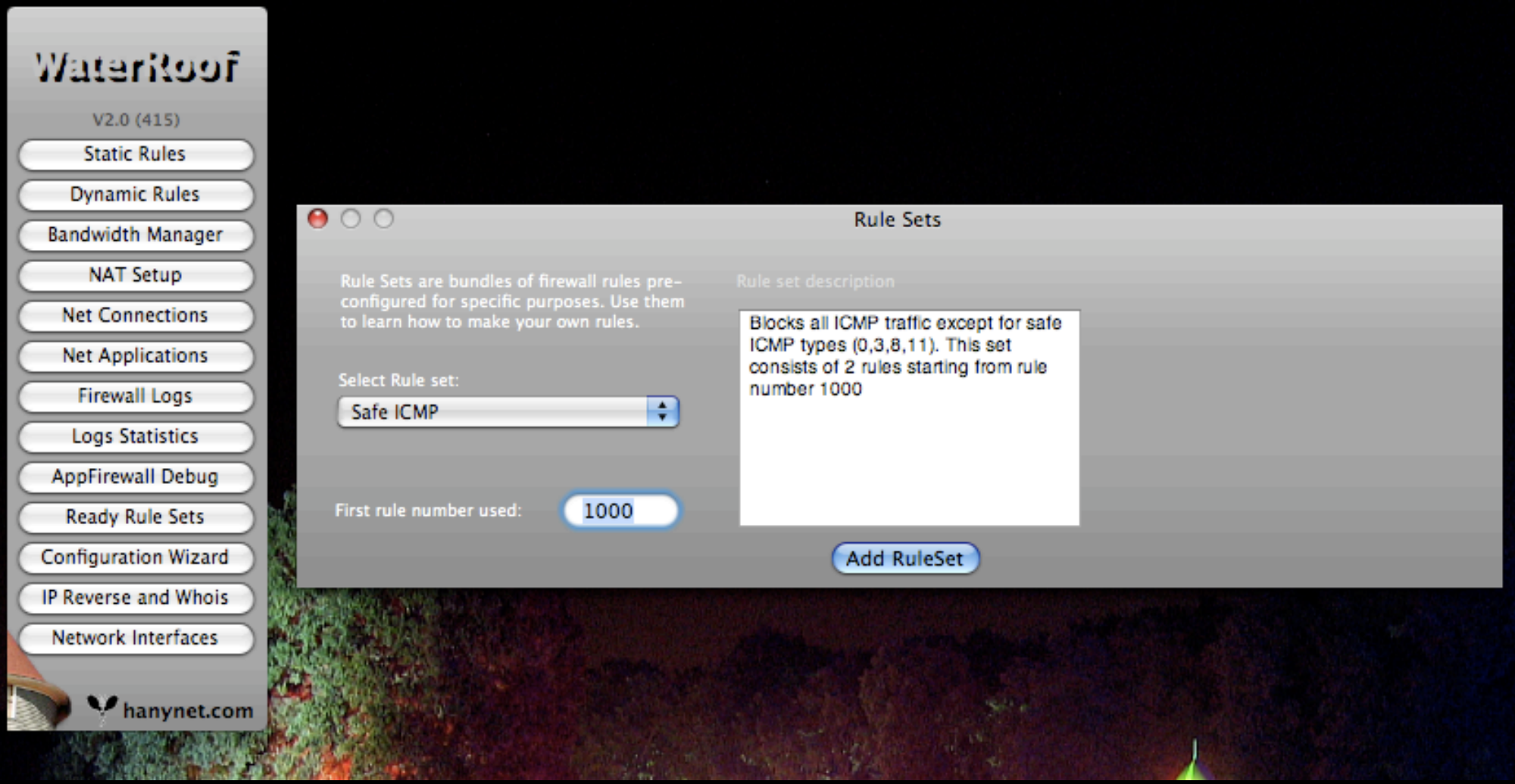
This Italian project is an

IPFW firewall frontend for Mac OS X 10.5

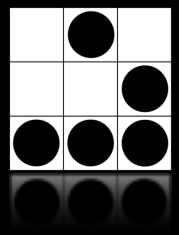
with an easy interface and many options.

Features include dynamic rules, bandwidth management, NAT configuration and port redirection, pre-defined rule sets and a wizard for easy configuration. You can also watch logs and graphic statistics.

WaterRoof



http://www.hanynet.com/waterroof/index.html



Bonjour

Bonjour

Also known as zero-configuration networking, enables automatic discovery of computers, devices, and services on IP networks.

Bonjour uses industry standard IP protocols to allow devices to automatically discover each other without the need to enter IP addresses or configure DNS servers. In order to provide a true zero-configuration experience, Bonjour requires that devices implement three essential things.

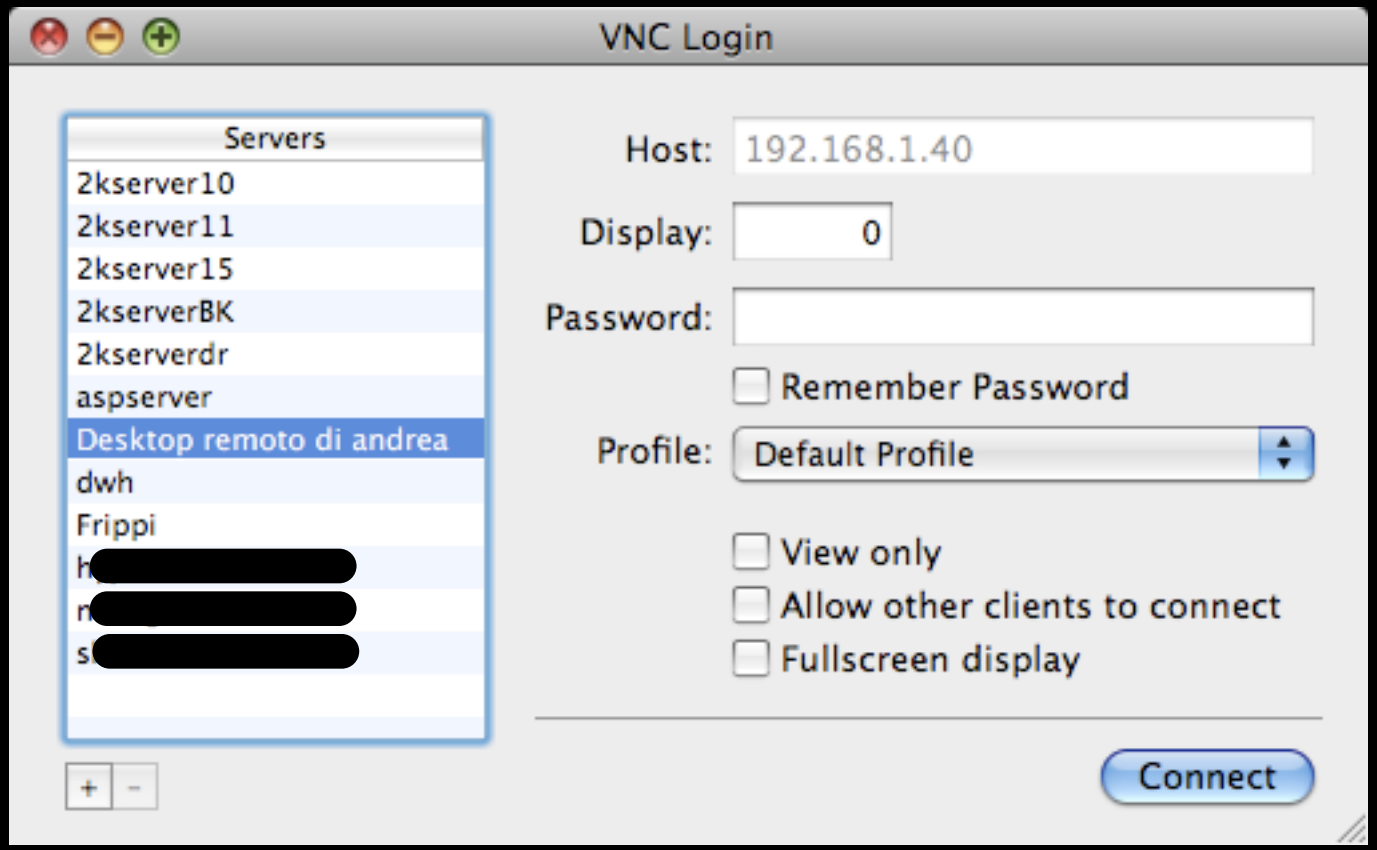
Requirements

- Allocate IP addresses without a DHCP server.
- Translate between names and addresses without a DNS server.
- Locate or advertise services without using a directory server.

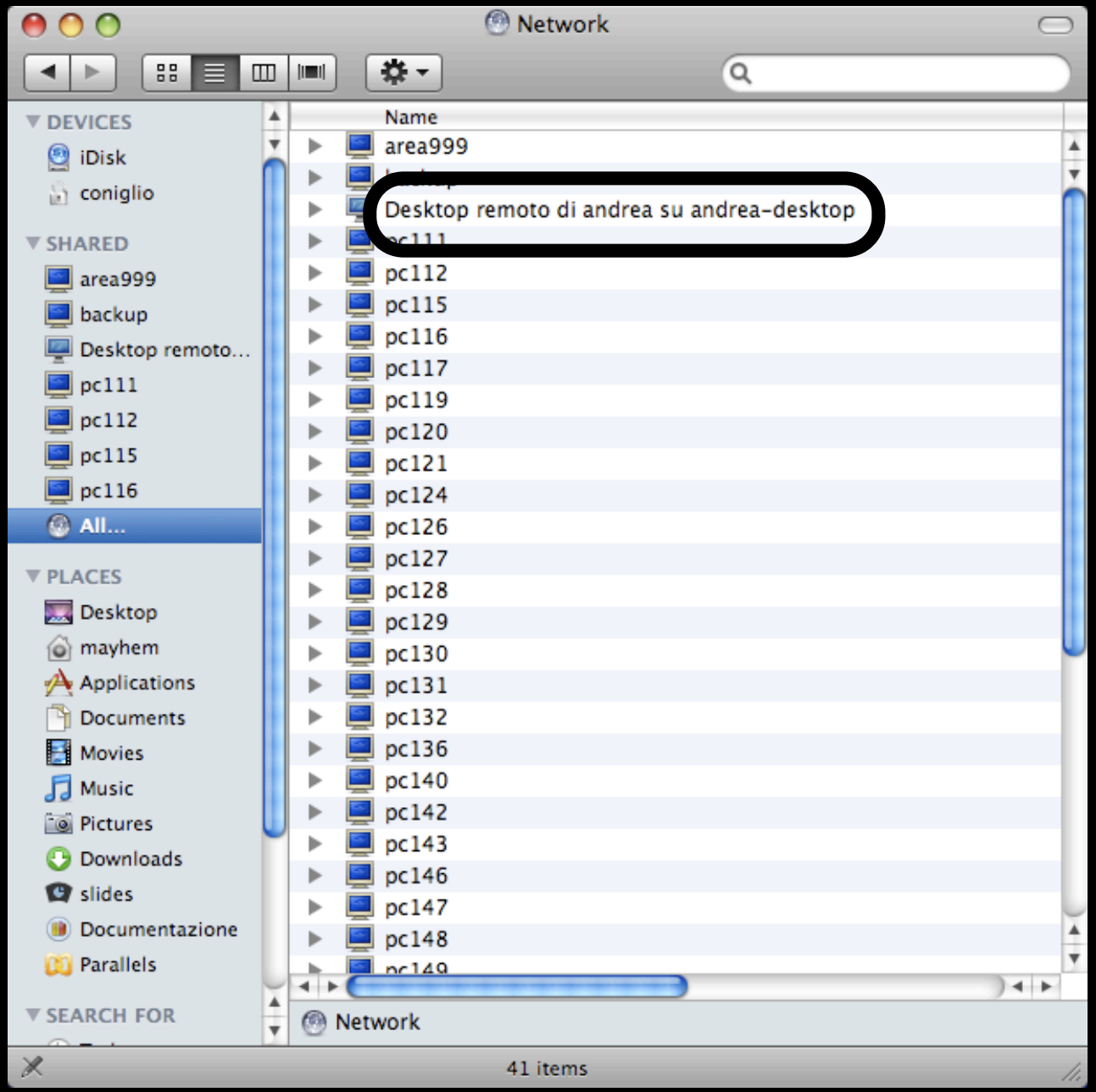
Useful for...

- ✓ Easily connect to printers
- ✓ Easily connect to services (i.e. VNC)
- ◉ *Enumerate*
- ◉ *Replicate worms*

Find VNC servers



or RDP server

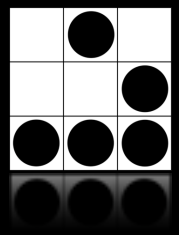


Disable bonjour

```
launchctl unload -w /System/Library/\
LaunchDaemons/com.apple.mDNSResponder.plist
```

To re-enable it:

```
launchctl load -w /System/Library/
\LaunchDaemons/\com.apple.mDNSResponder.plist
```



FileVault

FileVault

Will provide encrypted volumes

Can transparently encrypt the whole home

Can create volumes on CD / USB Key

/Users

FileVault will create a sparse bundle disk image

AES 128 encrypted

Automagically mounted at login

Logged off user

Empty /Users/mayhem

/Users/.mayhem containing the encrypted volume

The password of the volume is always corresponding to the user password

sparse image

It is a unique big file

must be maintained

default until 10.4

preserved when migrating

sparse bundle image

a lot of 8 MB bands (*files*)

easier to maintain

default since 10.5

No deniability

FileVault does not provide any plausible deniability feature.

Any *analyzer* will easily understand if you are using one or more encrypted volumes.

Break in

Is it possible to violate FileVault security?

Past

Mac OS X 10.3

In need to analyze a FileVault volume

Get in touch with a developer

Retrieved the user passord from swap space

After some days Apple published a new patch :)

Present

Mac OS X 10.4

In need to analyze a FileVault volume

Windows shares enabled

This create a NTLM copy of the user password :)

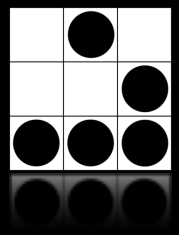
Future

Mac OS X 10.5

In need to analyze a FileVault volume

...

http://citp.princeton.edu/mory/



Gaining root locally

Conditions

No ability to boot from CD

Able to use single user mode

No time / possibility to use John the Ripper

Legacy way

CMD-S

```
# /sbin/mount -wu /
# /sbin/SystemStarter
# nidump passwd .
```

OR

```
# passwd root
```

What to do

```
sh-3.2# rm /var/db/.AppleSetupDone
```

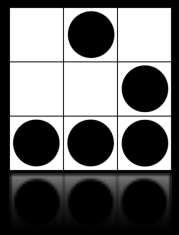
At next reboot setup will start

Then you can create a new administrator

and take any needed privilege / authorization

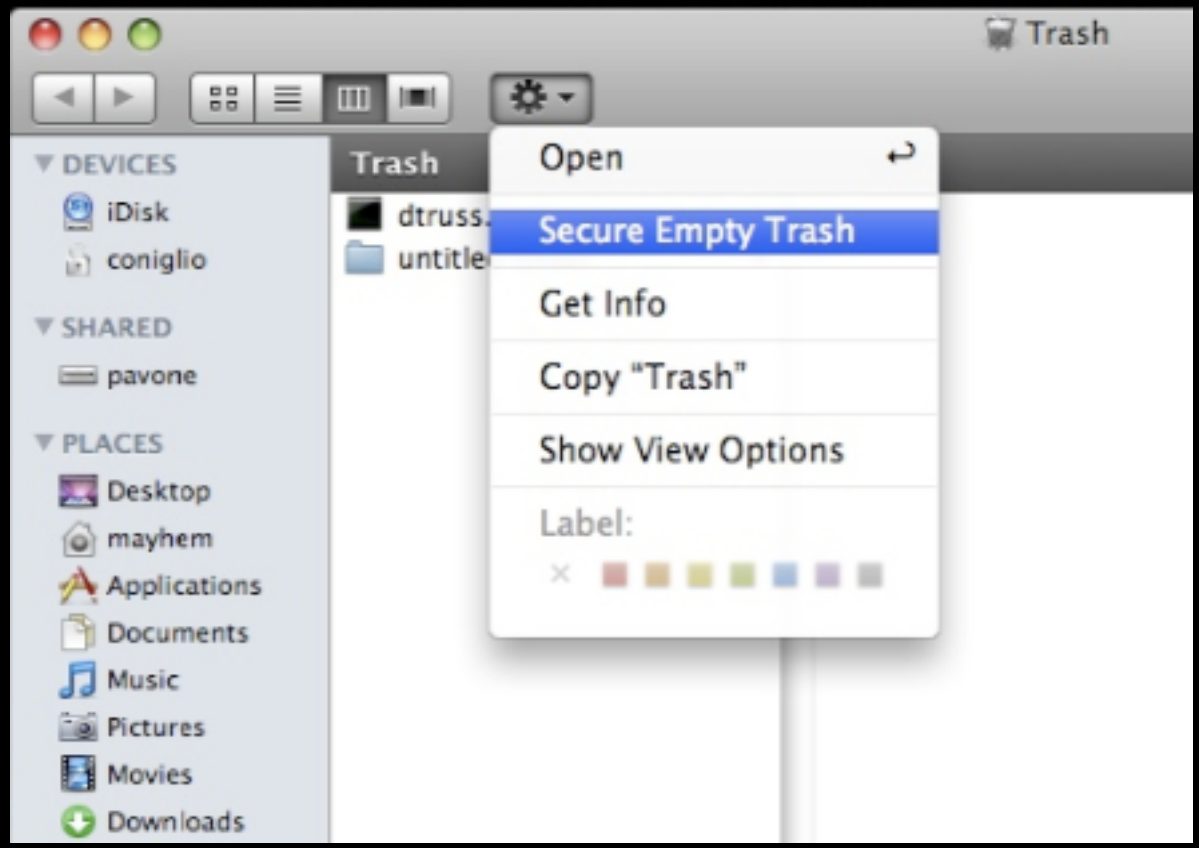
Curious content :)

```
<dict>
    <key>AppleSpam</key>
    <string>NO</string>
    <key>Location</key>
    <string>P</string>
    <key>Occupation</key>
    <string>5</string>
    <key>OthersSpam</key>
    <string>NO</string>
</dict>
```



Secure Deletion

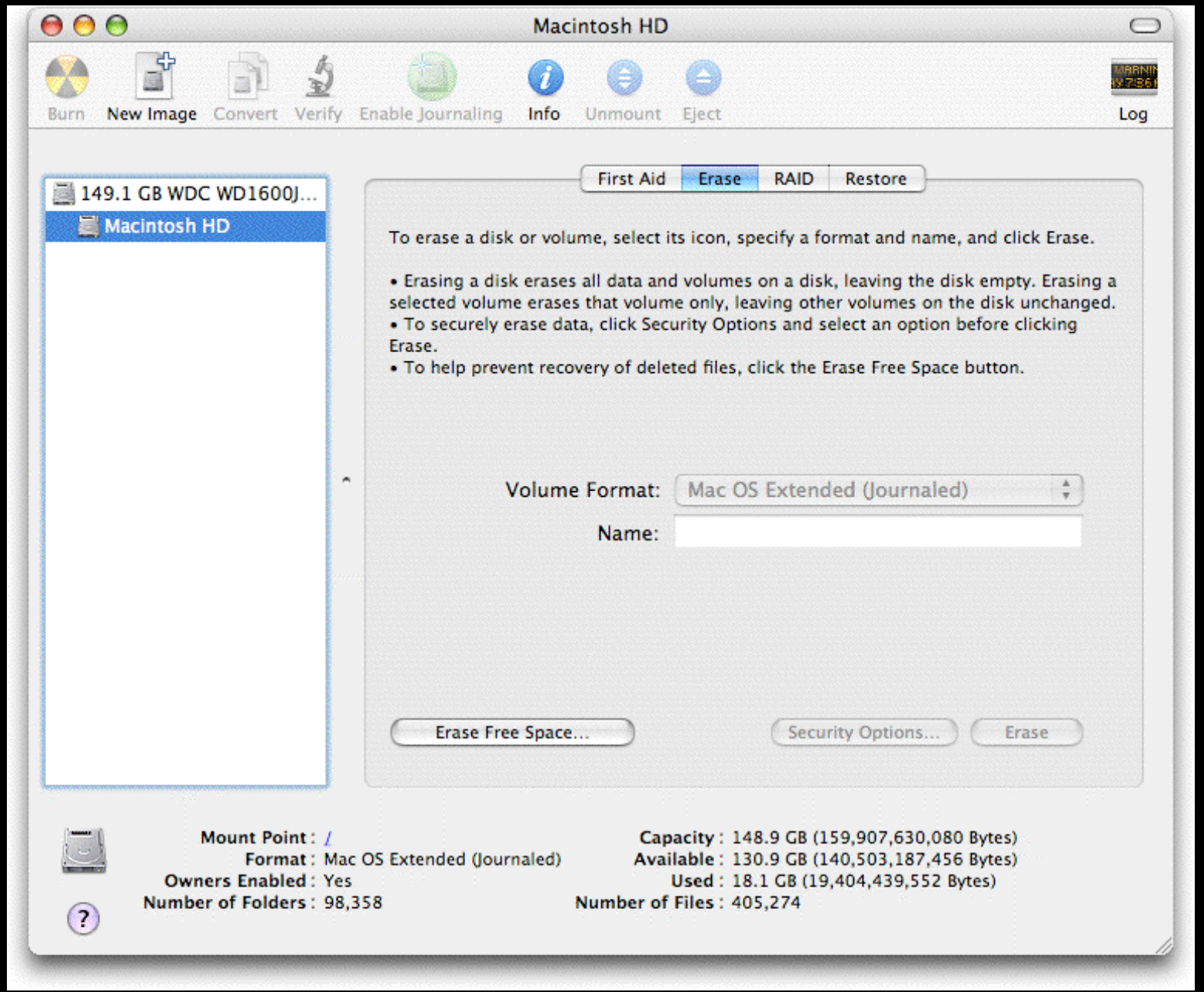
Native feature



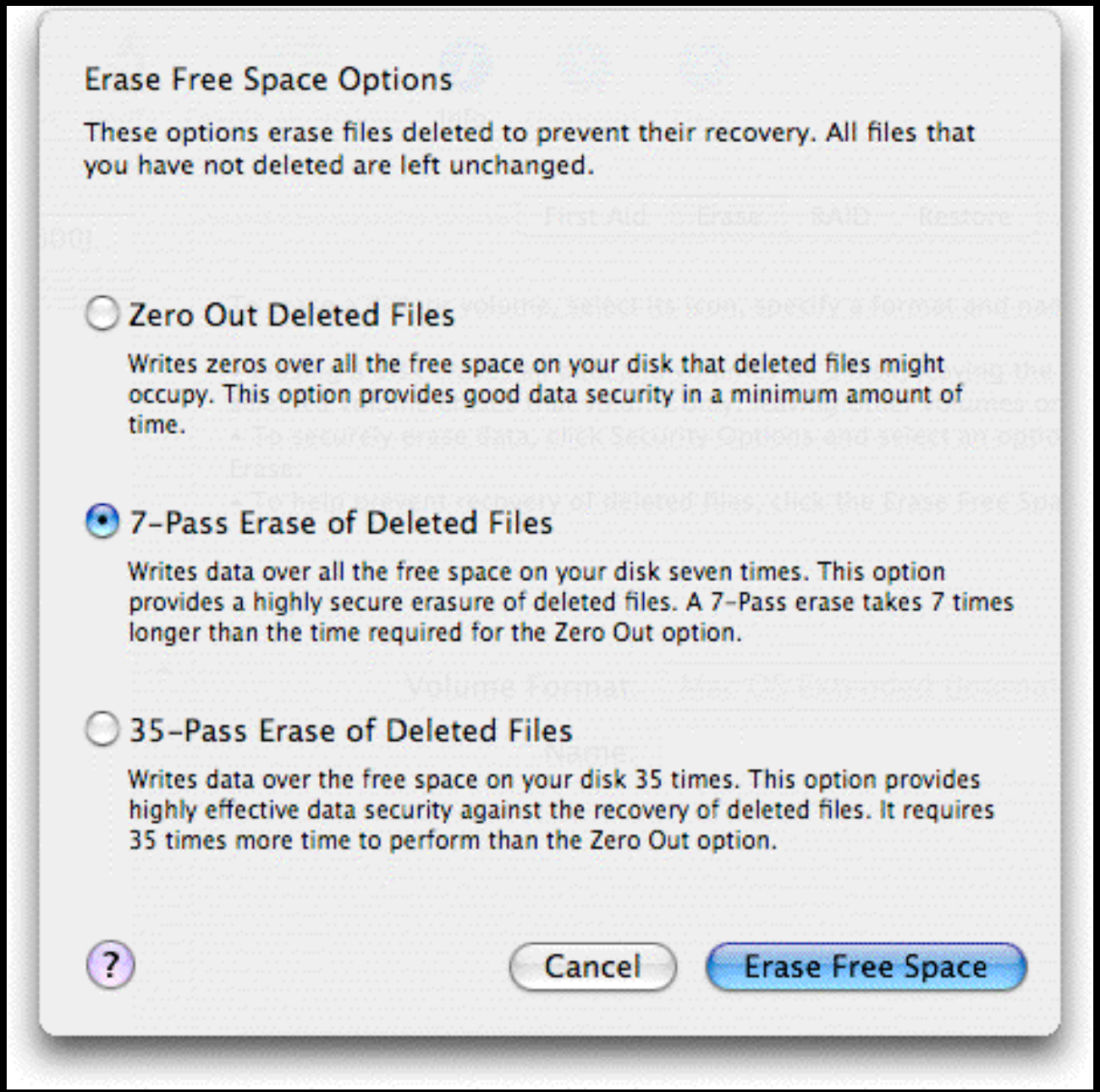
You can do it directly from your trash bin

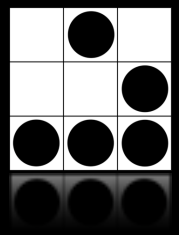
Many 3rd part application exists

Erase free space



Methods used





Harden

Do it easy

There are a lot of things to fix

Many different sintaxes

Mainly command line

It would be useful to have a simple tool

Bastille Unix

The Bastille Hardening program "locks down" an operating system, proactively configuring the system for increased security and decreasing its susceptibility to compromise. Bastille can also assess a system's current state of hardening, granularly reporting on each of the security settings with which it works.

Assess

In its assessment mode, it builds a report intended to teach the user about available security settings as well as inform the user as to which settings have been tightened.

Harden

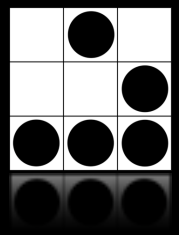
In its default hardening mode, it interactively asks the user questions, explains the topics of those questions, and builds a policy based on the user's answers.

It then applies the policy to the system.

Understand

Being OSS can be useful even only to understand which parameters are evaluated

http://bastille-linux.sourceforge.net/index.html



Nice tools

iAlertu

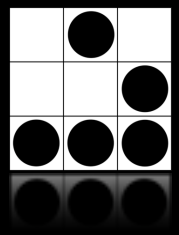
Basically iAlertU is a car alarm for your Apple Mac. iAlertU uses the built in motion to trigger the alarm and the isight to capture the image of the thief.

http://sourceforge.net/projects/ialertu/

Proximity

Proximity monitors the proximity of your mobile phone or other bluetooth device and executes custom AppleScripts when the device goes out of range or comes into range of your computer.

http://www.apple.com/downloads/macosx/system_disk_utilities/proximity.html



Conclusions

Am I the apple or the mouth?

Apple OS is a UNIX

you can harden it and make it secure.

As usual you have to know the mechanisms to adopt and which limits your security has.

Web-o-grafy

http://developer.apple.com/bonjour/

http://www.macosxhints.com/article.php?story=20050707222434355

http://db.tidbits.com/article/9251

http://securosis.com/2007/11/01/investigating-the-leopard-firewall/

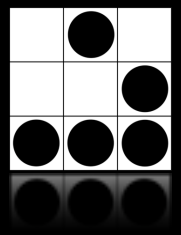
http://www.apple.com/macosx/features/300.html#security

http://db.tidbits.com/article/9294

http://www.matasano.com/log/981/a-roundup-of-leopard-security-features/

http://www.itwire.com/content/view/15143/53/

http://www.scribd.com/doc/40500/New-Admin-Setup-Mac-OS-X-How-to



Questions?

Thank you!

Alessio L.R. Pennasilico

mayhem@alba.st

Pescara, 22 Agosto 2008