Security on the Mac

or

How Paranoid are You?

Bob van Lier

BackUp, BackUp, BackUp …

- First and foremost defense when something goes wrong
- Macs are reliable and well-built, but internal HDDs are commodity products
- HDDs will FAIL! It is only a matter of when?
- The most complete and practical solution is to use an external HDD
  - Multiple DVDs or CDs can be used for select folder, but no longer practical for today's HDDs
- Time Machine is included with OS10.5 and 10.6
- Carbon Copy Cloner
- SuperDuper!
- Many others

BackUp Strategy

- While Time Machine works well and is a painless option consider cases of fire or theft
- Multiple copies using different software/process
  - Offsite backup
    - Keep a copy at a friend's house, safety deposit box, or hidden fire-proof box
    - Online storage
      - Mozy ($55/year)
      - Dropbox ($600/year for 100Gb)
      - Carbonite ($55/year unlimited)
      - CrashPlan (Free or $55/year to use their servers)

OSX Security Settings

- Use of “standard account” rather than admin account for routine usage
- Deselect automatic login
- Keep software up to date so latest security patches are applied
- Set Screensaver password
- Parental Controls in OS X
- Use Private Browsing when exploring suspect web sites
- FileVault
  - Essentially creates an encrypted sparse image bundle of your user folder

Hazards of Web Browsing

1. IP address which leads to your ISP's location can be cross correlated with other browsing history. IP address and logged in user account are all tied together

    1.1. See https://panopticlick.eff.org/ for how unique you are

2. Browser cookies - personal history plus various technical and social vulnerabilities
3. Probe of sites visited (highlighted links) (http://whattheinternetknowsaboutyou.com/)
4. Flash cookies - Identity and history kept across sessions (plus a 3rd party hosts your permissions, lol.)
5. HTML 5 "local storage"
6. Browser fingerprint - browser agent, headers, plugins, time zone, screen size, system fonts, etc. (if you're on a mac, you're pretty unique)
7. Metadata in uploaded photos and media (date, time, location, etc). Also, user supplied tags attached to photos and media such as facebook photo tags.
8. Camera and microphone access (Schools peeping in on students…)
9. Application phoning home with who knows what data (Little Snitch catches some of these)
10. "Fraudulent sites" checking (safari preferences setting) and google analytics, etc can keep a history of your browsing tied to your IP address, browser cookie, browser fingerprint, etc.
11. more?

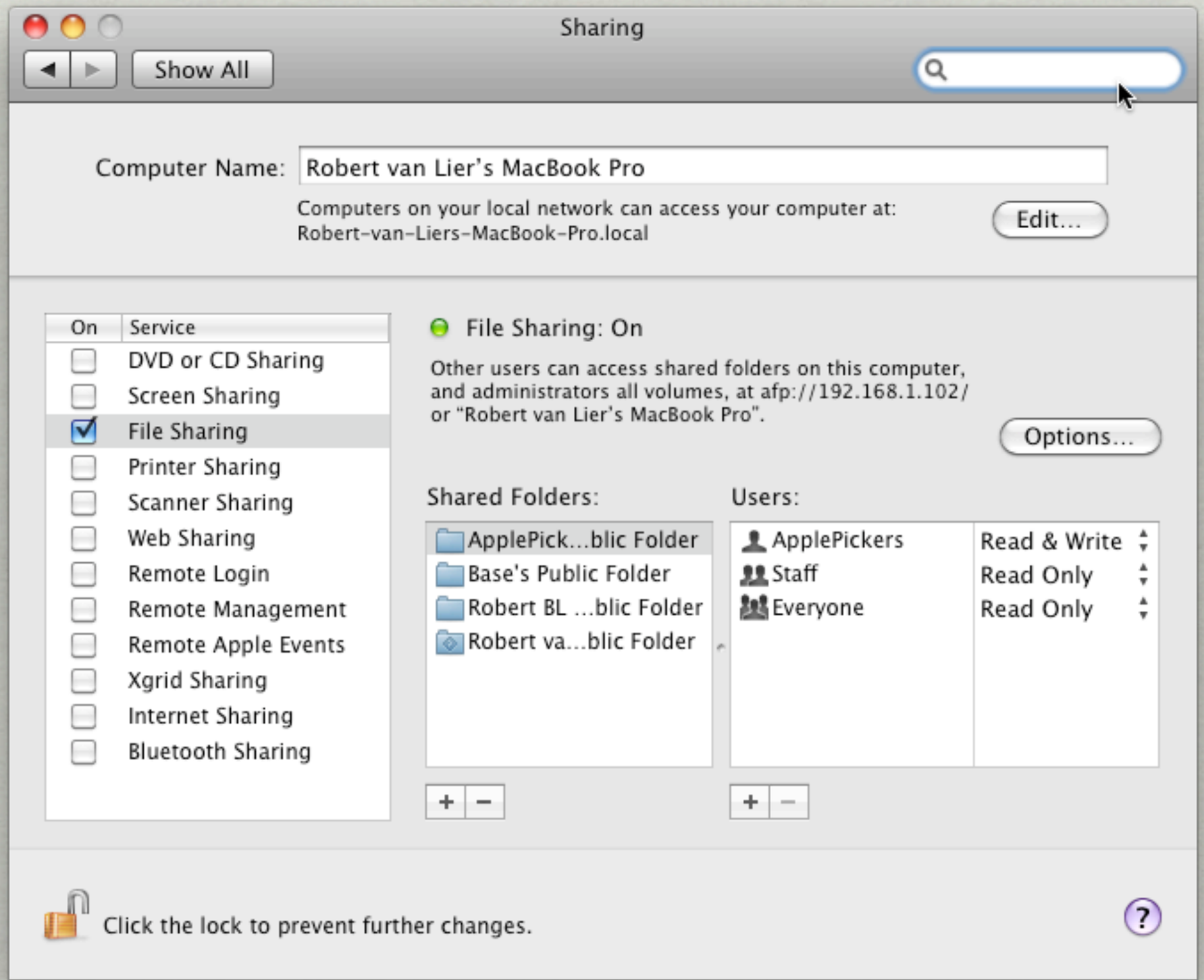
Passwords

- Don’t use the same password for all your stuff
- Don’t use an easily found word like child’s or pet’s name
- Mac OSX has built-in password storage: Keychain
  - Keychain can generate random passwords and store them
- Consider password manager:
  - 1Password ($39.95)
    - Solid, well respected in Mac community
  - SplashID ($29.95)
    - Better cross-platform support
  - PasswordVault (versions from free to $45.00)
  - LastPassword (free)
    - Cross platform
    - Versions for iPhone, Android and other phones ($1/month)

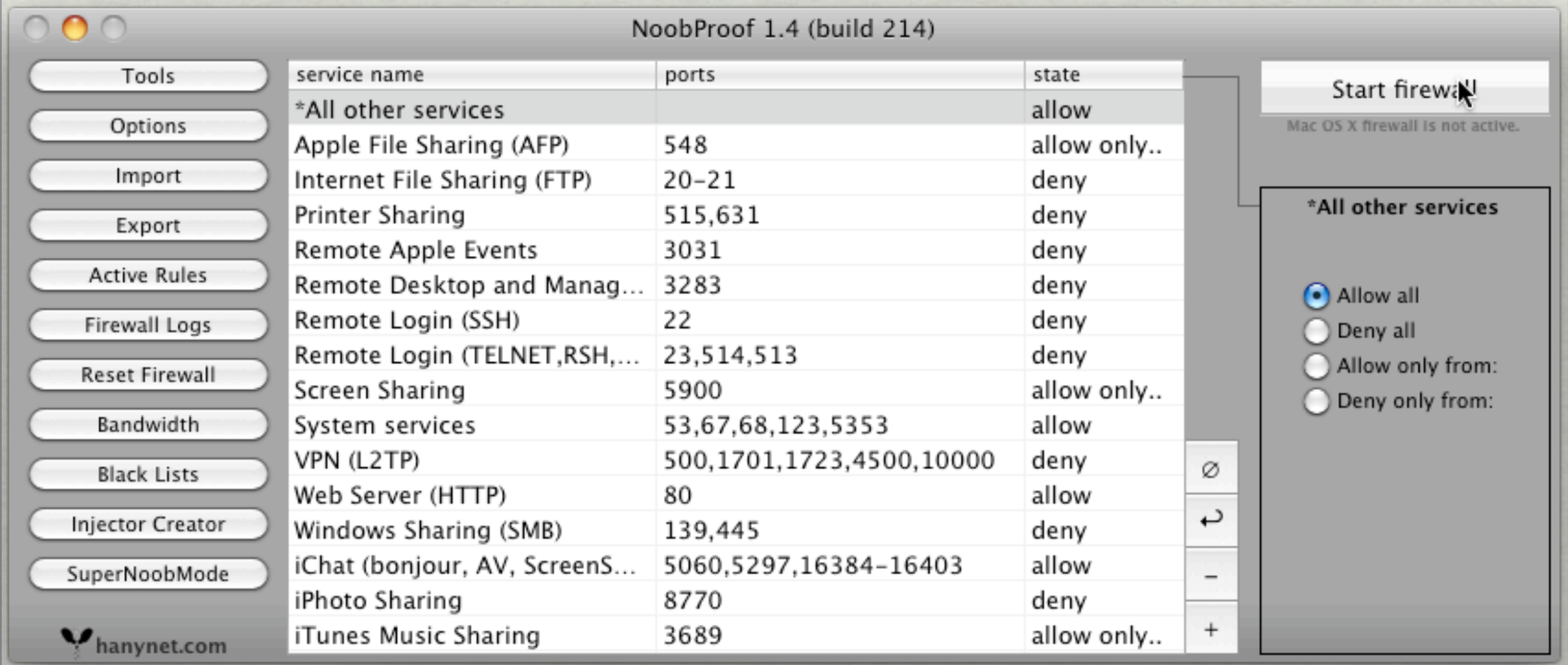
Firewalls

- OSX has a Built-in Firewall that be easily modified to open common ports for services
  - System Prefs ⇒ Sharing
- NAT firewall built into most routers
  - See settings to block ports
- NoobProof

OS X Built-in Firewall



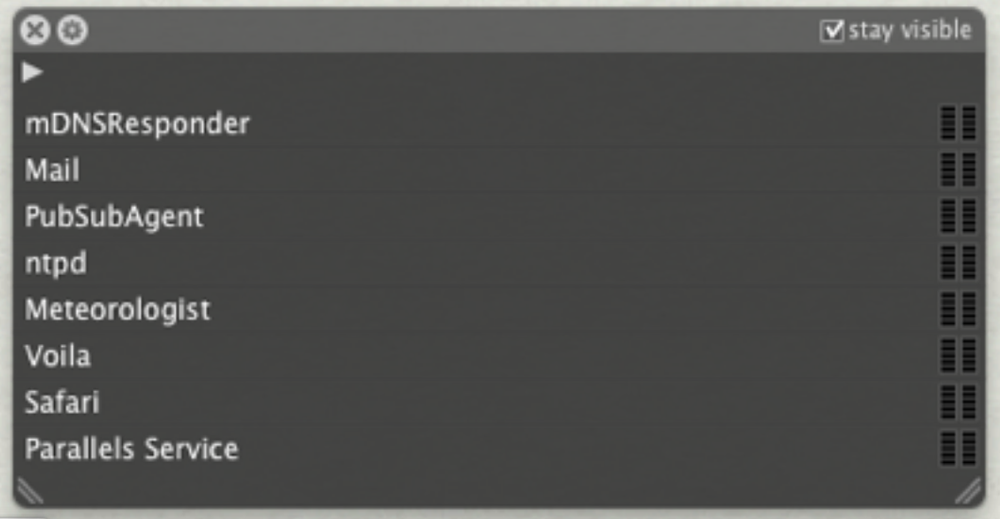
NoobProof

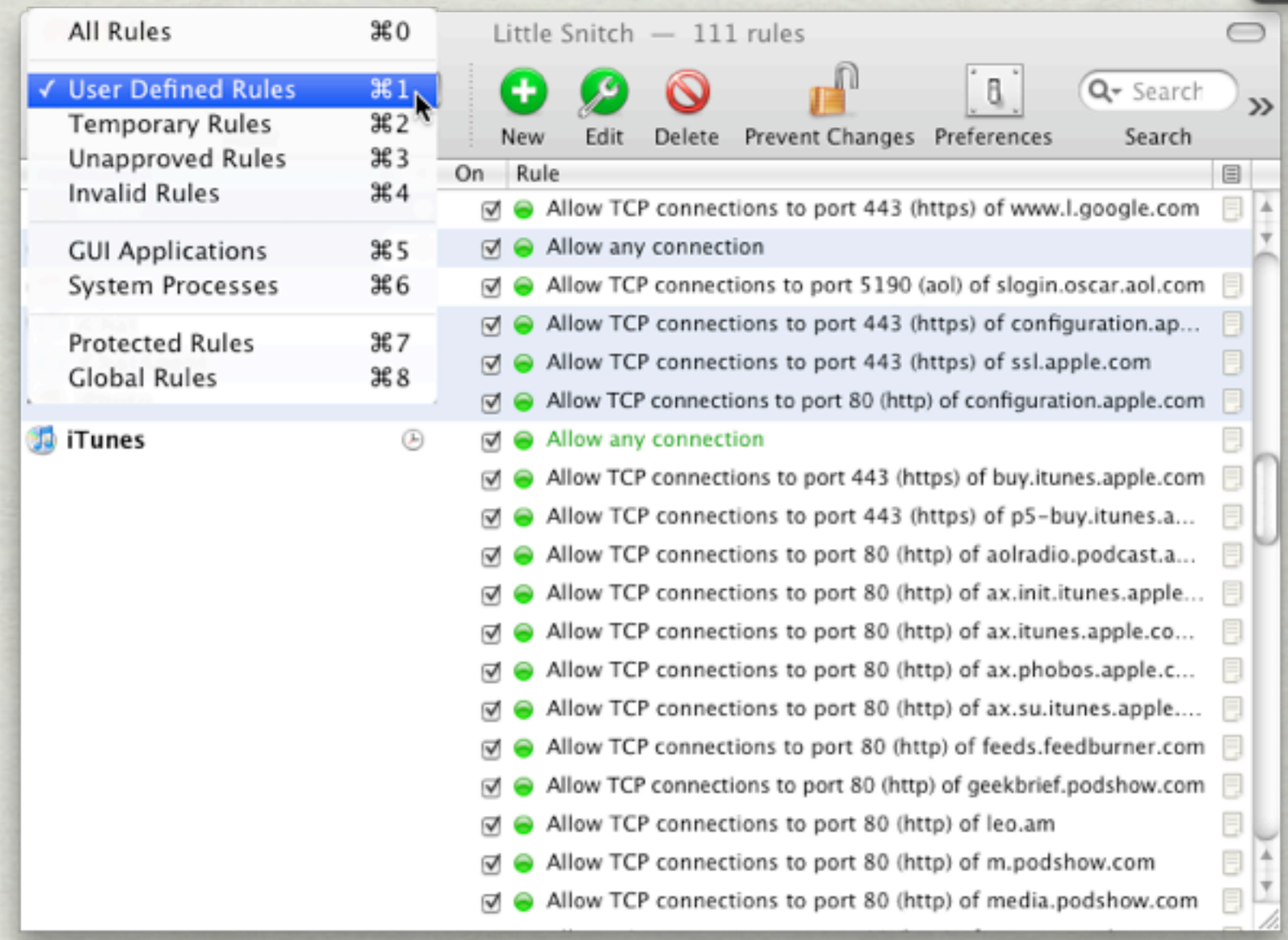

NoobProof 1.4 (build 214)
Tools
Options
Import
Export
Active Rules
Firewall Logs
Reset Firewall
Bandwidth
Black Lists
Injector Creator
SuperNoobMode
hanynet.com
service name
ports
state
*All other services
allow
Apple File Sharing (AFP)
548
allow only..
Internet File Sharing (FTP)
20-21
deny
Printer Sharing
515,631
deny
Remote Apple Events
3031
deny
Remote Desktop and Manag...
3283
deny
Remote Login (SSH)
22
deny
Remote Login (TELNET,RSH,...
23,514,513
deny
Screen Sharing
5900
allow only..
System services
53,67,68,123,5353
allow
VPN (L2TP)
500,1701,1723,4500,10000
deny
Web Server (HTTP)
80
allow
Windows Sharing (SMB)
139,445
deny
iChat (bonjour, AV, ScreenS...
5060,5297,16384-16403
allow
iPhoto Sharing
8770
deny
iTunes Music Sharing
3689
allow only..
Start firewall
Mac OS X firewall is not active.
*All other services
Allow all
Deny all
Allow only from:
Deny only from:

Network Traffic Cops and Anti-virus software

- The Mac environment has not been of much interest to malware authors because of relatively small market
- Little Snitch
  - Watches all incoming and outgoing connections
  - Set up permanent block to unwanted connections
- Change Hosts file to redirect DNS queries back to local machine
  - Read more here
- ClamXav
  - No active viruses targeting Mac OSX, but don't want to pass on viruses to PC using colleagues
- VirusBarrier X6
  - OSX/Opinion Spy debacle
  - Shows that anti-virus software manufacturers over emphasize risk to sell product
- MacScan

Little Snitch

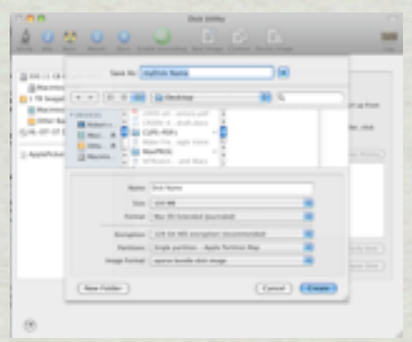




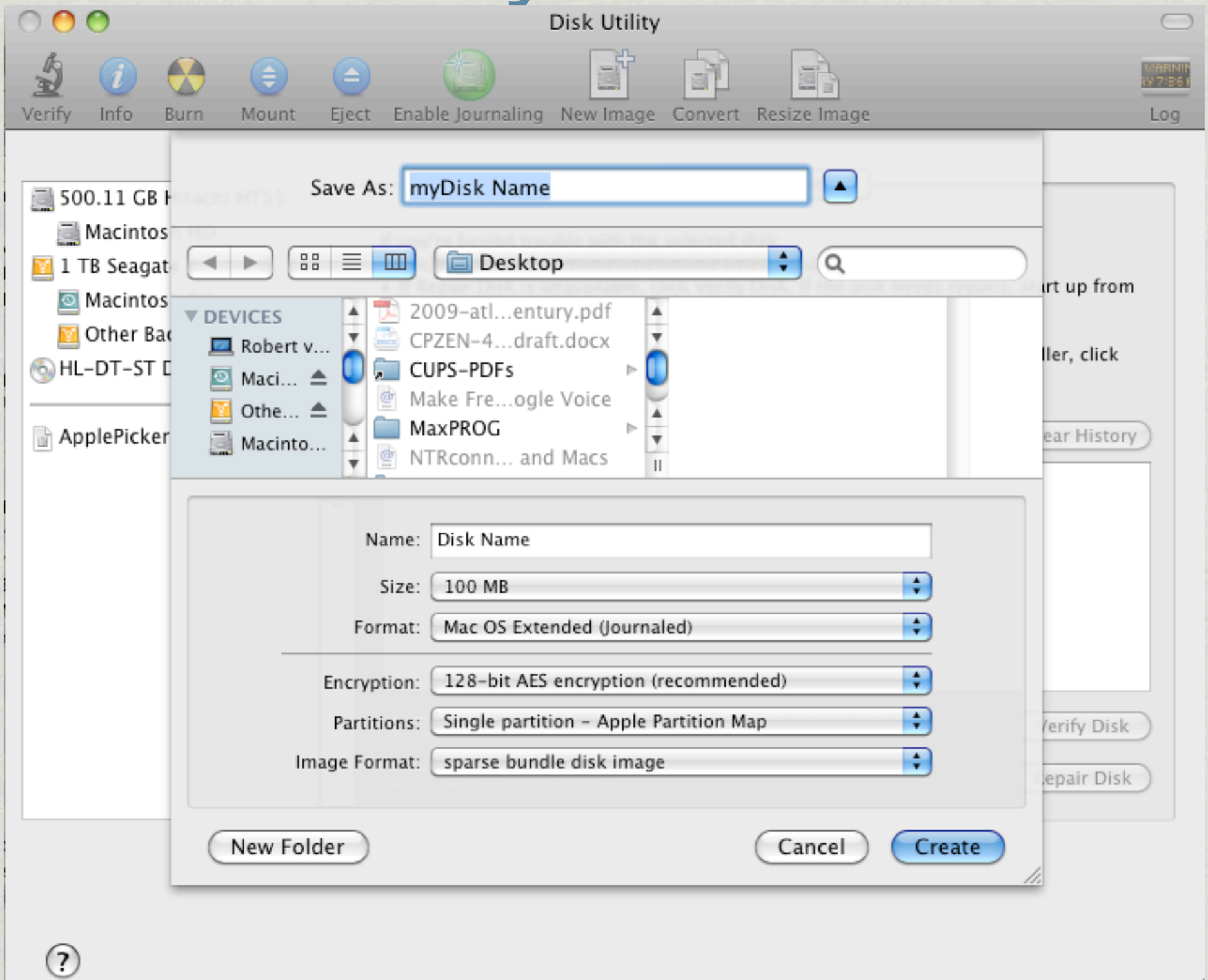
VirusBarrier X6

FileVault

- Is part of OSX
- Uses 128-bit AES encryption of a sparse image
- Fairly transparent to the user, but
  - Backup of an open file will not occur, so need to log off before running Time Machine
  - Data recovery apps will fail when trying to recover anything within FileVault
- Create your own encrypted sparse image for sensitive files using Disk Utility
  - store files on sparse image and dismount

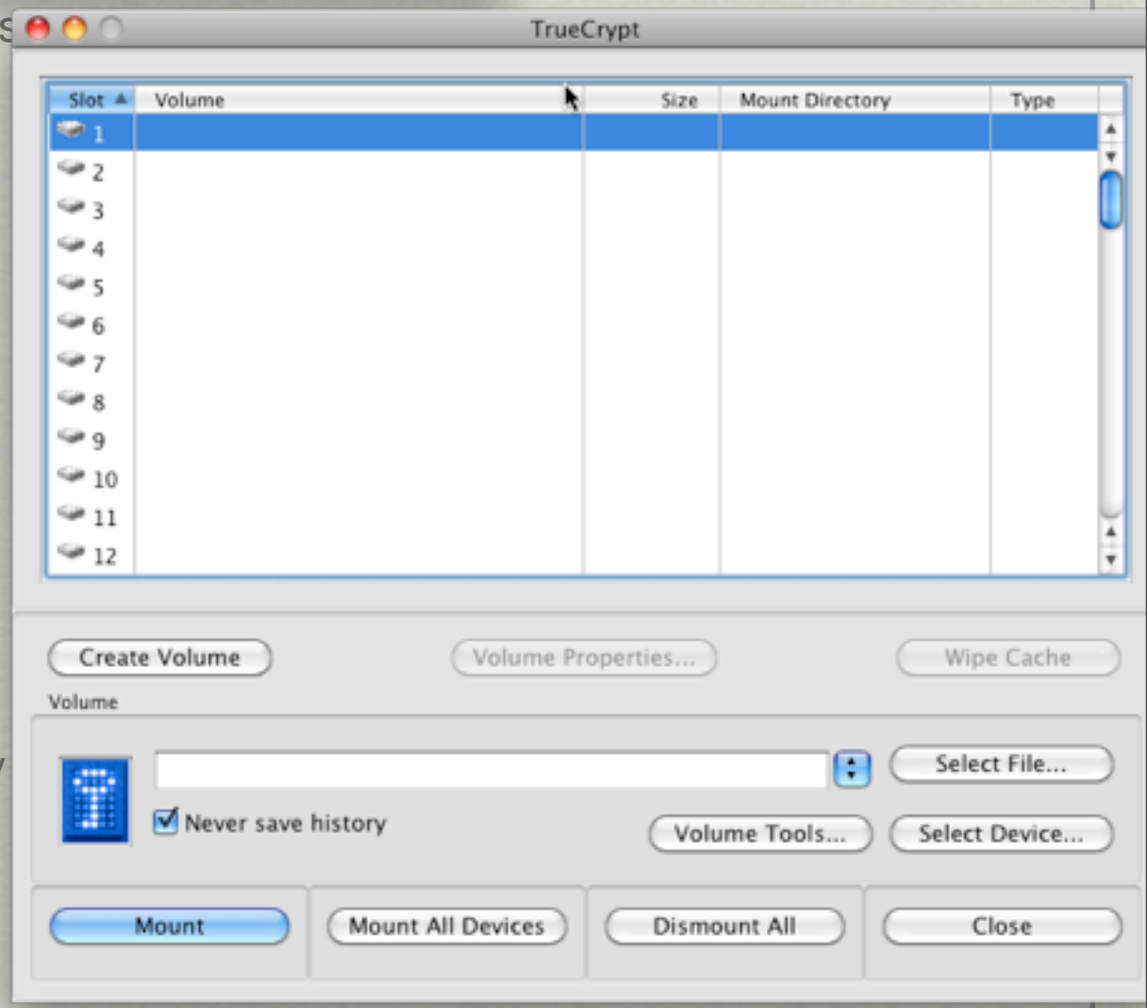


Disk Utility



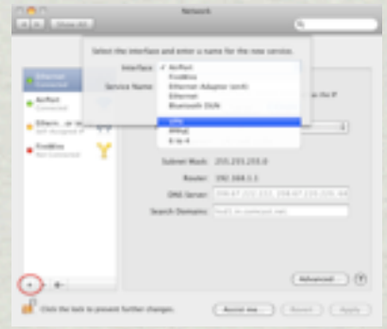
Free File, Folder and Volume Encryption

- Cryptor
  - Simple one step interface
- jFileCrypt
  - Provides easy password protection of individual files
  - Written in Java 5 and uses the Java Cryptographic Extensions
  - Supports AES, Blowfish, DES and several other algorithms
- TrueCrypt
  - Cross-platform
  - Can create an encrypted partition on a USB flash drive
  - Can create a hidden volume for plausible deniability



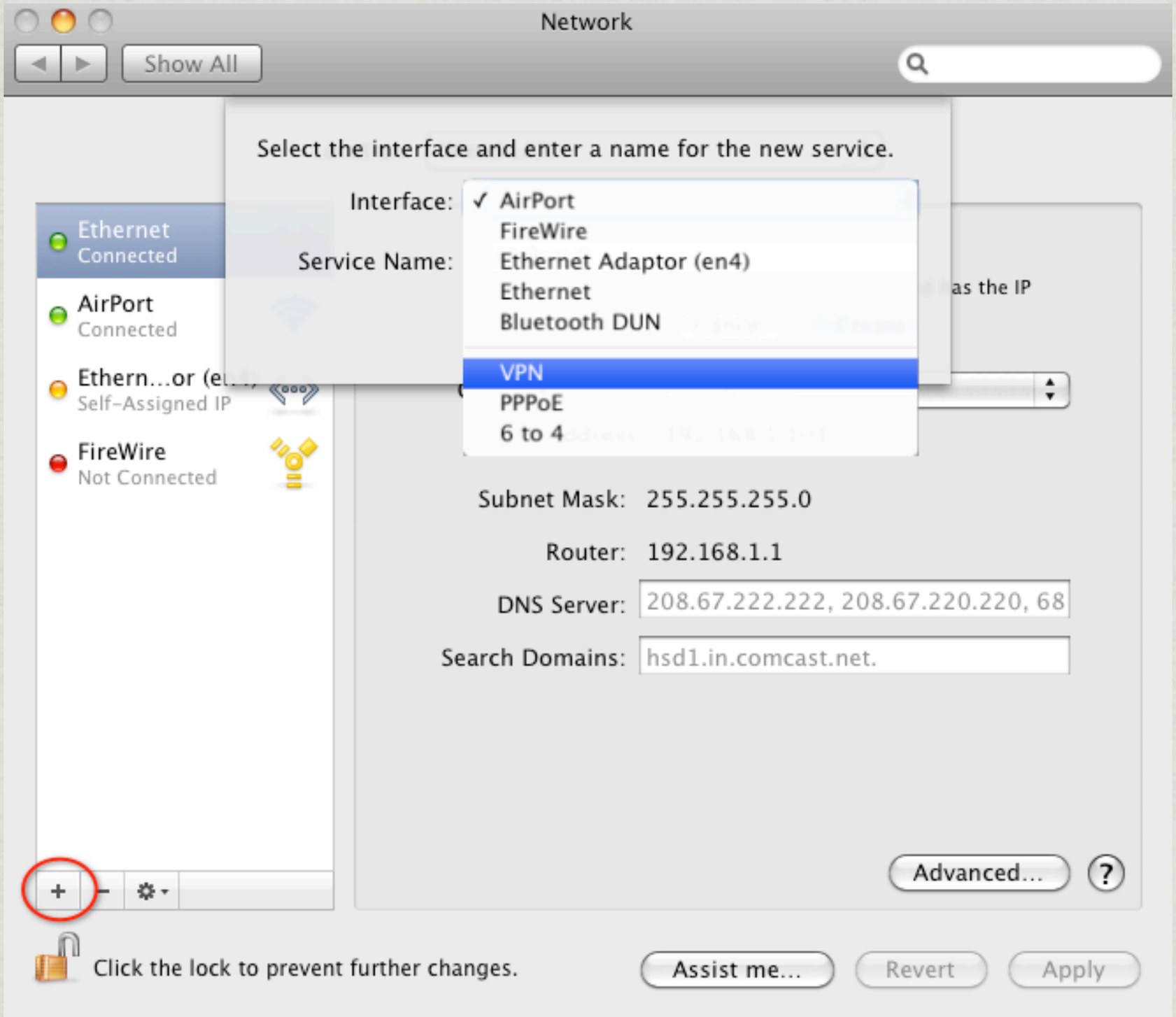
Securing your network connection with VPN

- Mac OS X has built-in VPN Client (virtual private network)
  - Requires a VPN server
    - Support for most common algorithms (L2TP, PPTP, IPSec)
  - Used by many business for remote users



- HotSpot Shield
  - Ad supported
  - Protect yourself from snoopers at Wi-Fi hotspots, hotels, airports, corporate offices.
  - Secure your web session, data, online shopping, and personal information online with HTTPS encryption.
  - Hides your IP address.
  - Access all content privately without censorship; bypass firewalls.
  - Works on wireless and wired connections alike.
  - Works on Windows 7 and Snow Leopard

VPN in Network PrefPane



HTTPS with TLS

- Most secure end-to-end web communications will (should) use HTTPS for transmission of sensitive personal data
- HTTPS requires that the browser accepts the server's trust certificate
- EFF makes available HTTPS everywhere for secure communications with a variety of other web sites
  - Firefox Plug-in
  - Google Search, Wikipedia, Twitter, Facebook, most of Amazon, GMX, Wordpress.com blogs, The New York Times, The Washington Post, Paypal, EFF, Tor, Ixquick

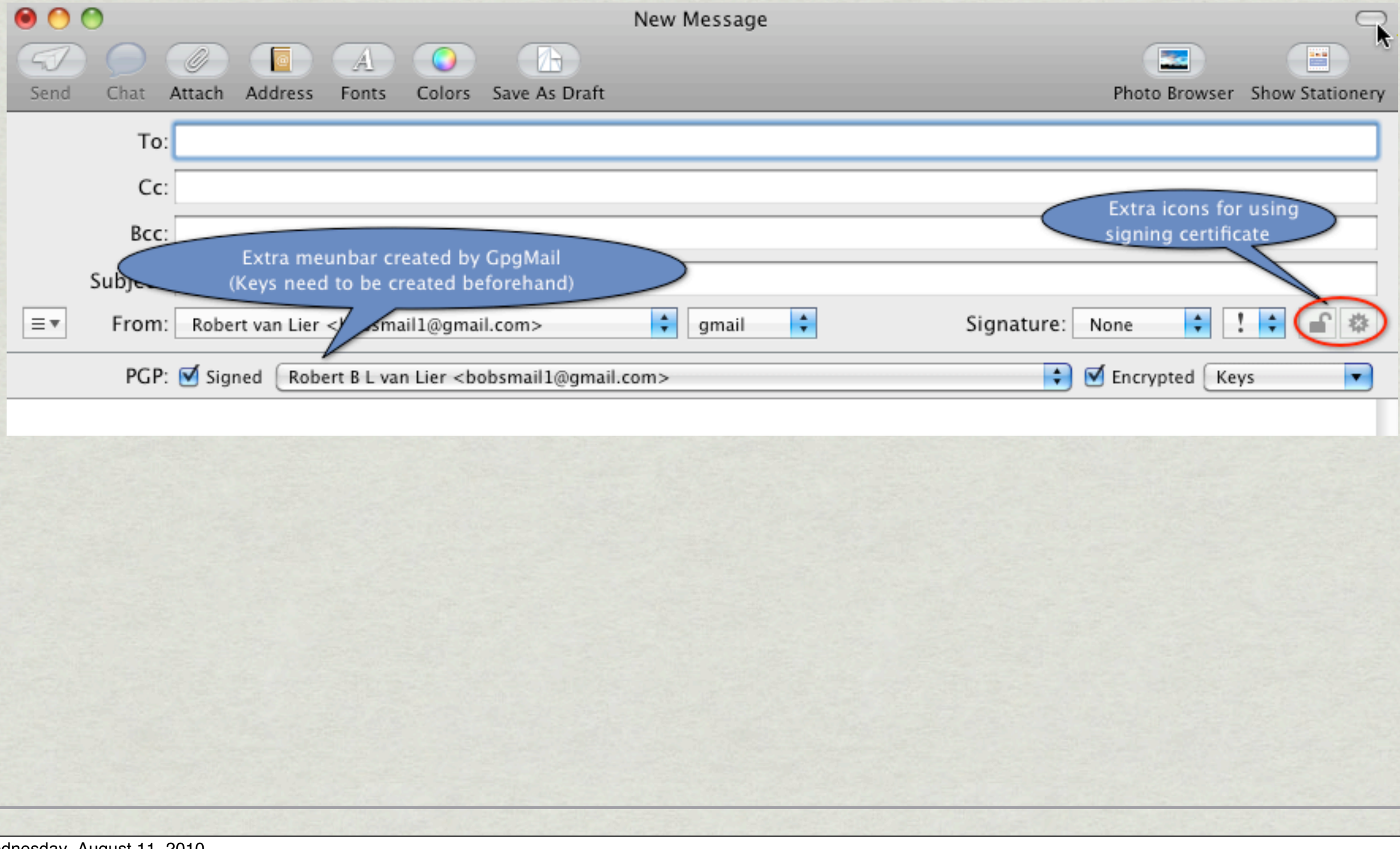
Anonymous Web Surfing

- Using a proxy server masks your IP address
  - Commonly used by companies
- Anonymouse
  - web surfing
  - sending anonymous emails
  - posting to newsgroups
- Mailinator
  - Provides a temporary email address to avoid spam

Email Encryption

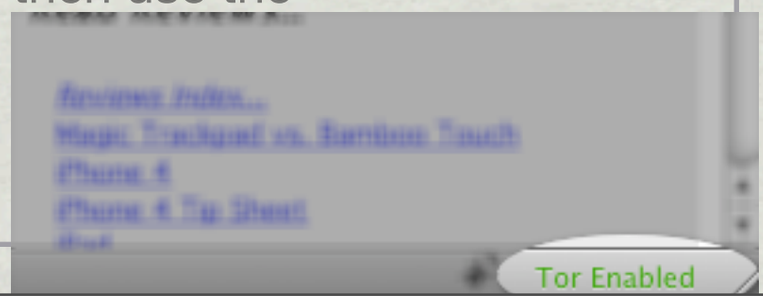
- PGP encryption uses a serial combination of hashing, data compression, symmetric-key cryptography, and, finally, public-key cryptography; each step uses one of several supported algorithms.
  - Developed by Phil Zimmermann in 1991
    - Court challenges unsuccessful
    - Now part of a web standard
- Several years ago PGP was available for Mac OS9 for free. For OSX it's now $99.
- GnuPG is an open source implementation of PGP
  - Additional GUI add-ons needed otherwise use terminal commands
  - GpgMail is an extension for Apple Mail
  - Thunderbird with Enigmail
- Get free Certificate from a CA
  - Comodo
  - TrustCenter (part of PGP Corp)
  - No longer available from Thwate (part of Verisign)
- Hushmail

AppleMail with CA and GnuPG



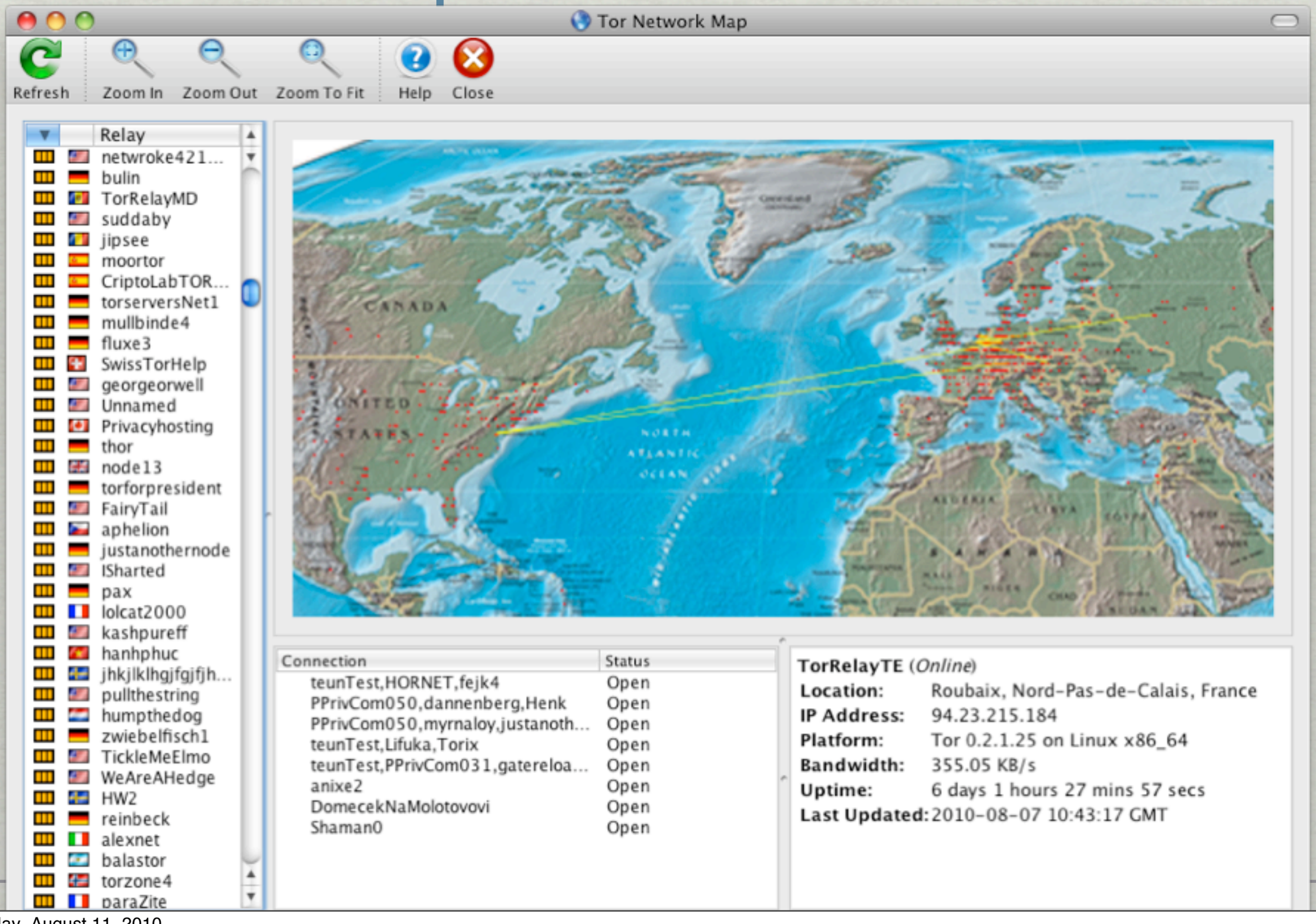
The TOR Project

- Tor is an open network that helps you defend against a form of network surveillance known as traffic analysis.
  - Personal freedom and privacy, confidential business activities and relationships, and state security
- Tor protects you by bouncing your communications around a distributed network of relays
  - Run by volunteers all around the world
  - Prevents somebody watching your Internet connection from learning what sites you visit
  - Prevents the sites you visit from learning your physical location.
  - Tor works with many of your existing applications, including web browsers, instant messaging clients, remote login, and other applications based on the TCP protocol.
- The easiest way to implement TOR on the Mac is with Vidalia and then use the TOR button extension in Firefox



Vidalia Control Panel

Tor Map


Tor Network Map
Refresh
Zoom In
Zoom Out
Zoom To Fit
Help
Close
Relay
netwroke421...
bulin
TorRelayMD
suddaby
jipsee
moortor
CriptoLabTOR...
torserversNet1
mullbinde4
fluxe3
SwissTorHelp
georgeorwell
Unnamed
Privacyhosting
thor
node13
torforpresident
FairyTail
aphelion
justanothernode
ISharted
pax
lolcat2000
kashpureff
hanhphuc
jhkjlklhgjfgjfjh...
pullthestring
humpthedog
zwiebelfisch1
TickleMeElmo
WeAreAHedge
HW2
reinbeck
alexnet
balastor
torzone4
paraZite
CANADA
UNITED STATES
NORTH ATLANTIC OCEAN
Connection
Status
teunTest,HORNET,fejk4
Open
PPrivCom050,dannenberg,Henk
Open
PPrivCom050,myrnaloy,justanoth...
Open
teunTest,Lifuka,Torix
Open
teunTest,PPrivCom031,gatereloa...
Open
anixe2
Open
DomecekNaMolotovovi
Open
Shaman0
Open
TorRelayTE (Online)
Location: Roubaix, Nord-Pas-de-Calais, France
IP Address: 94.23.215.184
Platform: Tor 0.2.1.25 on Linux x86_64
Bandwidth: 355.05 KB/s
Uptime: 6 days 1 hours 27 mins 57 secs
Last Updated: 2010-08-07 10:43:17 GMT

Conclusions

- There are a lot of simple security measures you can take to make your computing experience safer
- Mac OS is reasonably safe by nature
  - OS based on UNIX
  - Market has not attracted viruses

- Need to balance security with risk and hassle

Websites and Articles

- Apple security page
- Electronic Frontier Foundation
- Bruce Schneier
- The RSA
- Firewall Guide
- David Pouge
- Security Now