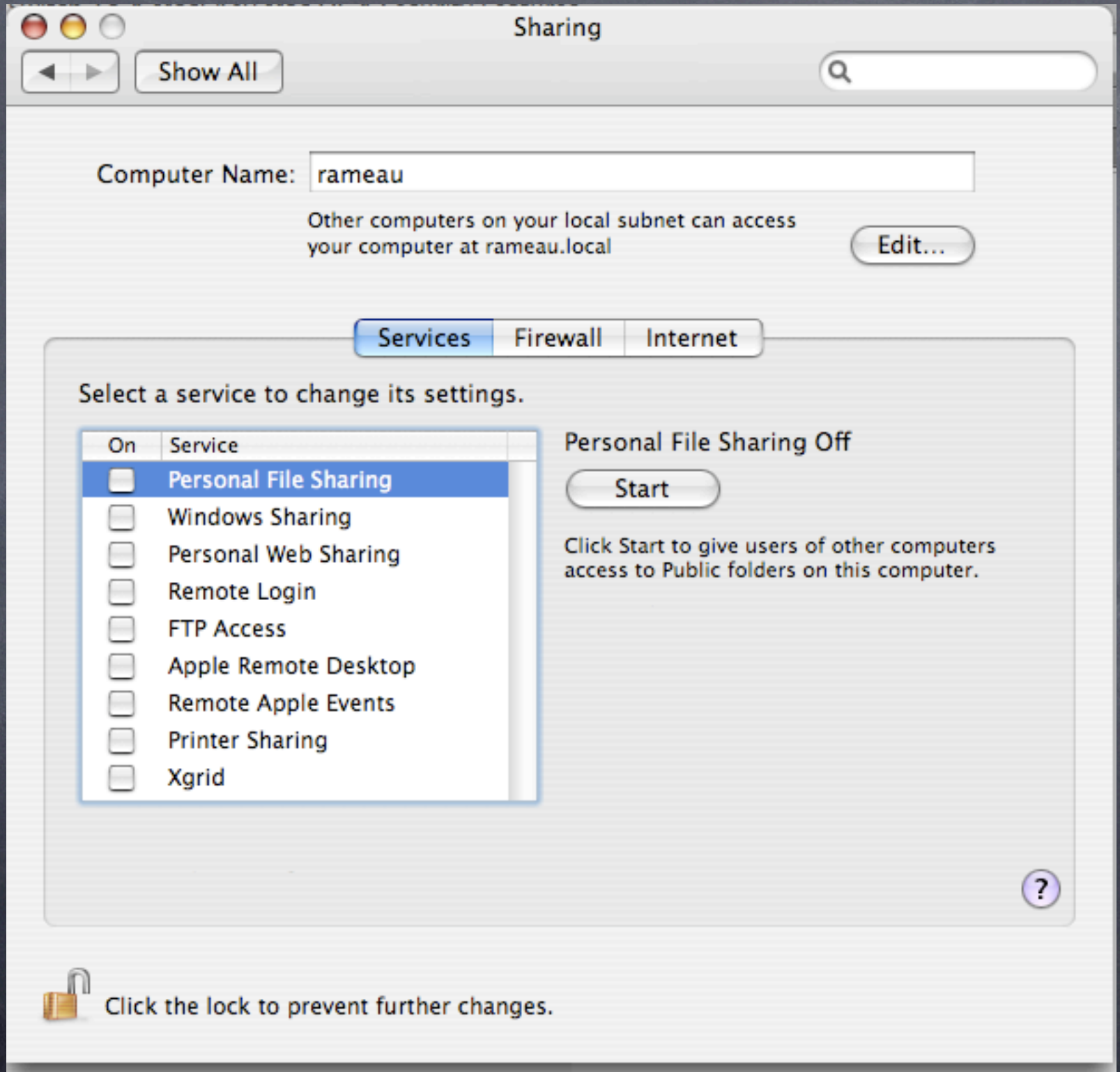
Secure your Mac

23C3

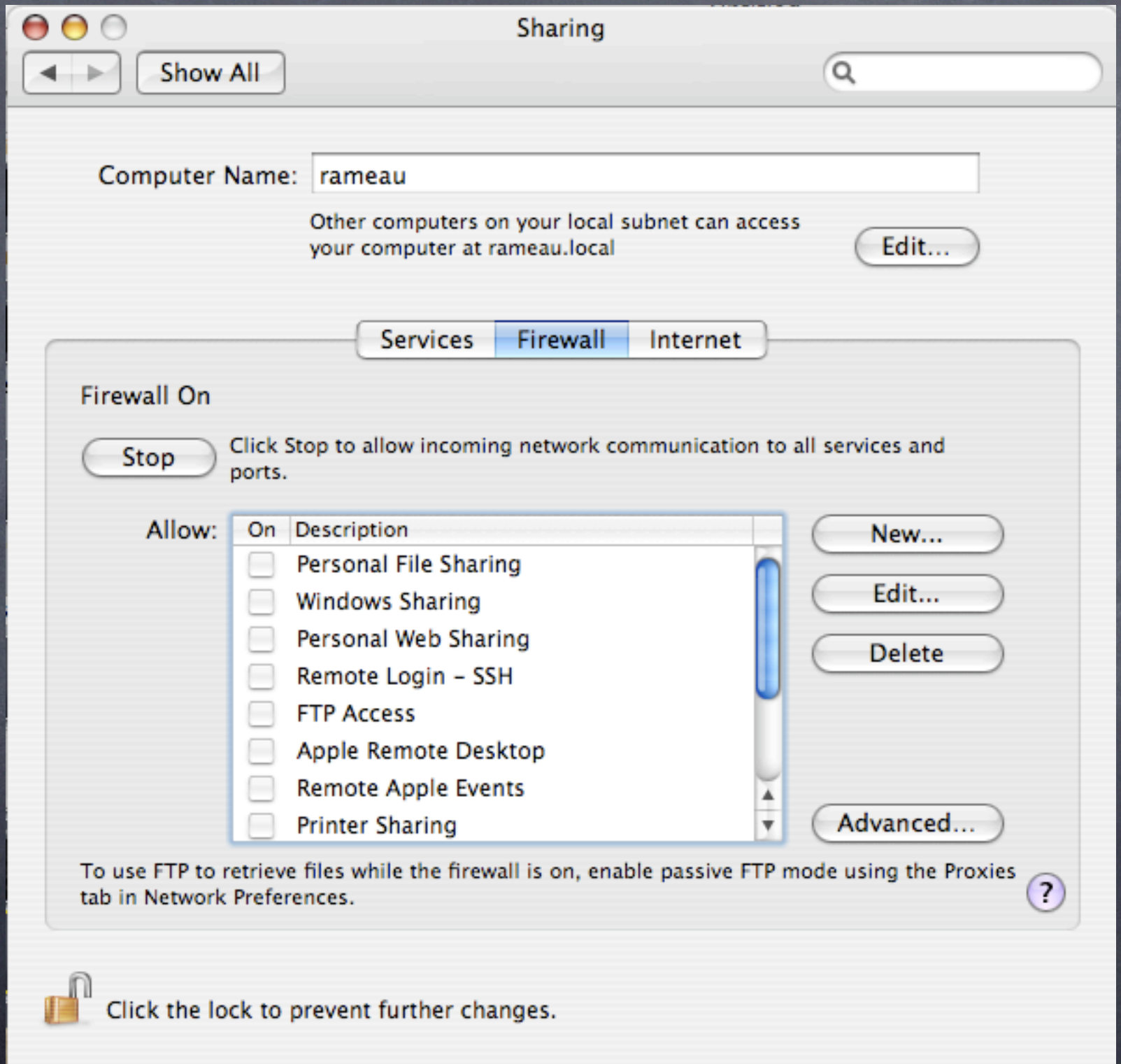
- MITM attacks
- 0day spl0itz
- ARP spoofing
- Physical attacks
- Evil Firewire devices

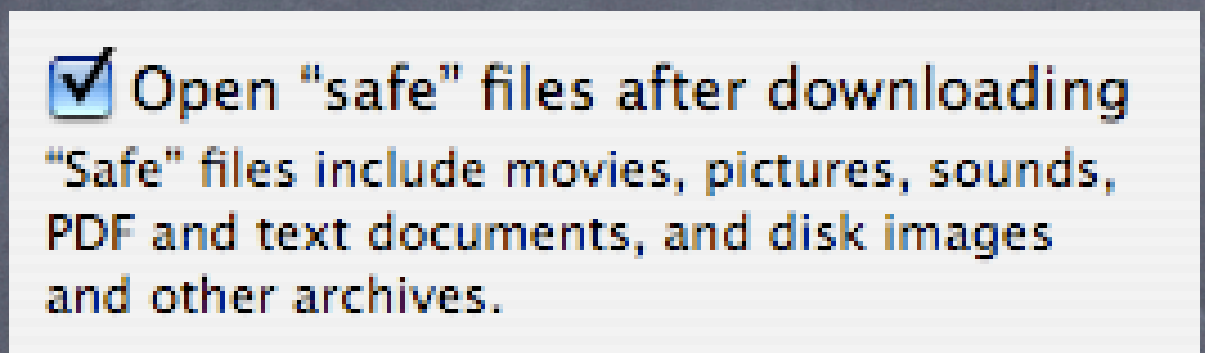

Sharing
Show All
Computer Name:
rameau
Other computers on your local subnet can access your computer at rameau.local
Edit...
Services
Firewall
Internet
Select a service to change its settings.
On
Service
Personal File Sharing
Windows Sharing
Personal Web Sharing
Remote Login
FTP Access
Apple Remote Desktop
Remote Apple Events
Printer Sharing
Xgrid
Personal File Sharing Off
Start
Click Start to give users of other computers access to Public folders on this computer.
?
Click the lock to prevent further changes.

Was lauscht trotzdem?

- slpd
- mDNSResponder
- notifyd
- ntp

```
udp4       0      0  *.*                    *.*
udp4       0      0  *.svrloc               *.*
udp4       0      0  rameau.49780           *.*
udp4       0      0  *.mdns                 *.*
udp4       0      0  *.mdns                 *.*
udp4       0      0  *.mdns                 *.*
udp4       0      0  *.49647                *.*
udp4       0      0  localhost.49198        localhost.1023
udp4       0      0  *.*                    *.*
udp4       0      0  *.49190                *.*
udp4       0      0  *.*                    *.*
udp6       0      0  *.123                                 *.*
udp4       0      0  *.ntp                  *.*
udp4       0      0  localhost.49179        localhost.1022
udp4       0      0  localhost.49178        localhost.1022
udp4       0      0  localhost.1022         *.*
udp4       0      0  localhost.1023         *.*
udp4       0      0  rameau.ntp             *.*
udp6       0      0  fe80:5::217:f2ff:fe46:7b0c.123        *.*
udp4       0      0  localhost.ntp          *.*
udp6       0      0  fe80:1::1.123                         *.*
udp6       0      0  localhost.123                         *.*
udp6       0      0  *.5353                                *.*
udp4       0      0  *.mdns                 *.*
udp4       0      0  localhost.netinfo-loca *.*
udp4       0      0  *.*                    *.*
icm6       0      0  *.*                                   *.*
icm6       0      0  *.*                                   *.*
icm6       0      0  *.*                                   *.*
```


Sharing
Show All
Computer Name: rameau
Other computers on your local subnet can access your computer at rameau.local
Edit...
Services
Firewall
Internet
Firewall On
Stop
Click Stop to allow incoming network communication to all services and ports.
Allow:
On
Description
Personal File Sharing
Windows Sharing
Personal Web Sharing
Remote Login - SSH
FTP Access
Apple Remote Desktop
Remote Apple Events
Printer Sharing
New...
Edit...
Delete
Advanced...
To use FTP to retrieve files while the firewall is on, enable passive FTP mode using the Proxies tab in Network Preferences.
?
Click the lock to prevent further changes.



"safe" files, hihi

FileVault

FileVault secures your home folder by encrypting its contents. It automatically encrypts and decrypts your files while you're using them.

WARNING: Your files will be encrypted using your login password. If you forget your login password and you don't know the master password, your data will be lost.

A master password is **not set** for this computer.
This is a "safety net" password. It lets you unlock any FileVault account on this computer.

Set Master Password...

FileVault protection is **off** for this account.
Turning on FileVault may take a while.

Turn On FileVault...

- [x] Require password to wake this computer from sleep or screen saver

For all accounts on this computer:

- [x] Disable automatic login
- [x] Require password to unlock each secure system preference
- [ ] Log out after 60 minutes of inactivity
- [x] Use secure virtual memory
  You must restart for this change to take affect.
- [ ] Disable remote control infrared receiver

This computer will work with only the paired remote.

Unpair

Click the lock to prevent further changes.

?

```
sudo strings /var/vm/swapfile0 |grep -A 4 -i longname
```

ARP spoofing

- ARP table anzeigen mit:

  arp -a

- Gateway statisch eintragen mit

  sudo arp -s hostname ether_addr

- MAC Adresse des Gateways steht meistens auf den Switches

Man-In-The-Middle Attacks

- Attacker redirects traffic and acts as man in the middle
- Impersonate Gateway
- Spoofed DNS, ARP or whatever entries
- Steal sensitive data like passwords or credit card information
- You're fucked

Man-In-The-Middle Attacks

- Always check your ssh fingerprints
- Use public key authentication with passphrase
- Make sure all relevant fingerprints are stored in ~/.ssh/known_hosts before you leave for Berlin
- Don't dismiss 'certificate not valid' messages on SSL enabled websites

Man-In-The-Middle Attacks

- The best solution: OpenVPN

OpenVPN

- Paranoid Setup
- AES-256 signed and encrypted tunnel
- Server certificate to prevent MITM
- HMAC-Authentication

OpenVPN Paranoid Setup

```
local 80.237.242.115
port 443
proto tcp
dev tun
ca ca.crt
cert paranoid.crt
key paranoid.key  # This file should be kept secret
dh dh2048.pem
server 10.0.7.0 255.255.255.0
push "route 192.168.20.0 255.255.255.0"
push "redirect-gateway"
push "dhcp-option DNS 80.237.128.144"
keepalive 5 41
tls-auth ta.key 0 # This file is secret
cipher AES-256-CBC # we are very paranoid here
comp-lzo
max-clients 10
persist-key
persist-tun
status openvpn-status.log
verb 4
mute 20
```

OpenVPN Paranoid Setup

- Jeder hier im Raum kriegt freien Zugang
- Für die Dauer des 23C3

Firewire

- DMA is on by default
- PowerPC: Open Firmware Secure Mode
- Intel Macs: No way to turn it off
- Nice demo by Maximilian Dornseif

IOFirewireController.cpp

```
void IOFireWireController::initSecurity( void )
{
   // assume security mode is normal
   IOFWSecurityMode mode = kIOFWSecurityModeNormal;
   // check OpenFirmware security mode
   {
      IORegistryEntry * options = IORegistryEntry::fromPath( "/options", gIODTPlane );
      if( options != NULL )
      {
         OSString * securityModeProperty = OSDynamicCast( OSString, options->getProperty
("security-mode") );
         if( securityModeProperty != NULL && strcmp("none", securityModeProperty-
>getCStringNoCopy()) != 0 )
         {
            // set security mode to secure/permanent
            mode = kIOFWSecurityModeSecurePermanent;
         }
         options->release();
         options = NULL;
      }
   }
   // now that we've determined our security mode, set it
   setSecurityMode( mode );
}
```

Auf Intel

```
void IOFireWireController::initSecurity( void )
{
    // assume security mode is normal
    IOFWSecurityMode mode = kIOFWSecurityModeNormal;

    setSecurityMode( mode );
}
```

```
void IOFireWireController::initSecurity( void )
{
    // assume security mode is secure/permanent
    IOFWSecurityMode mode = kIOFWSecurityModeSecurePermanent;

    setSecurityMode( mode );
}
```

Download at

http://metalab.at/wiki/SYMWorkshop

and replace

/System/Library/Extensions/
IOFirewireFamily.kext

USB???

Really Paranoid

- Odays for Bonjour
  - maliciously crafted multicast packet -> remote root
  - turn off Bonjour entirely
- Odays for Spotlight
  - visiting a website -> remote root
  - turn off Spotlight entirely

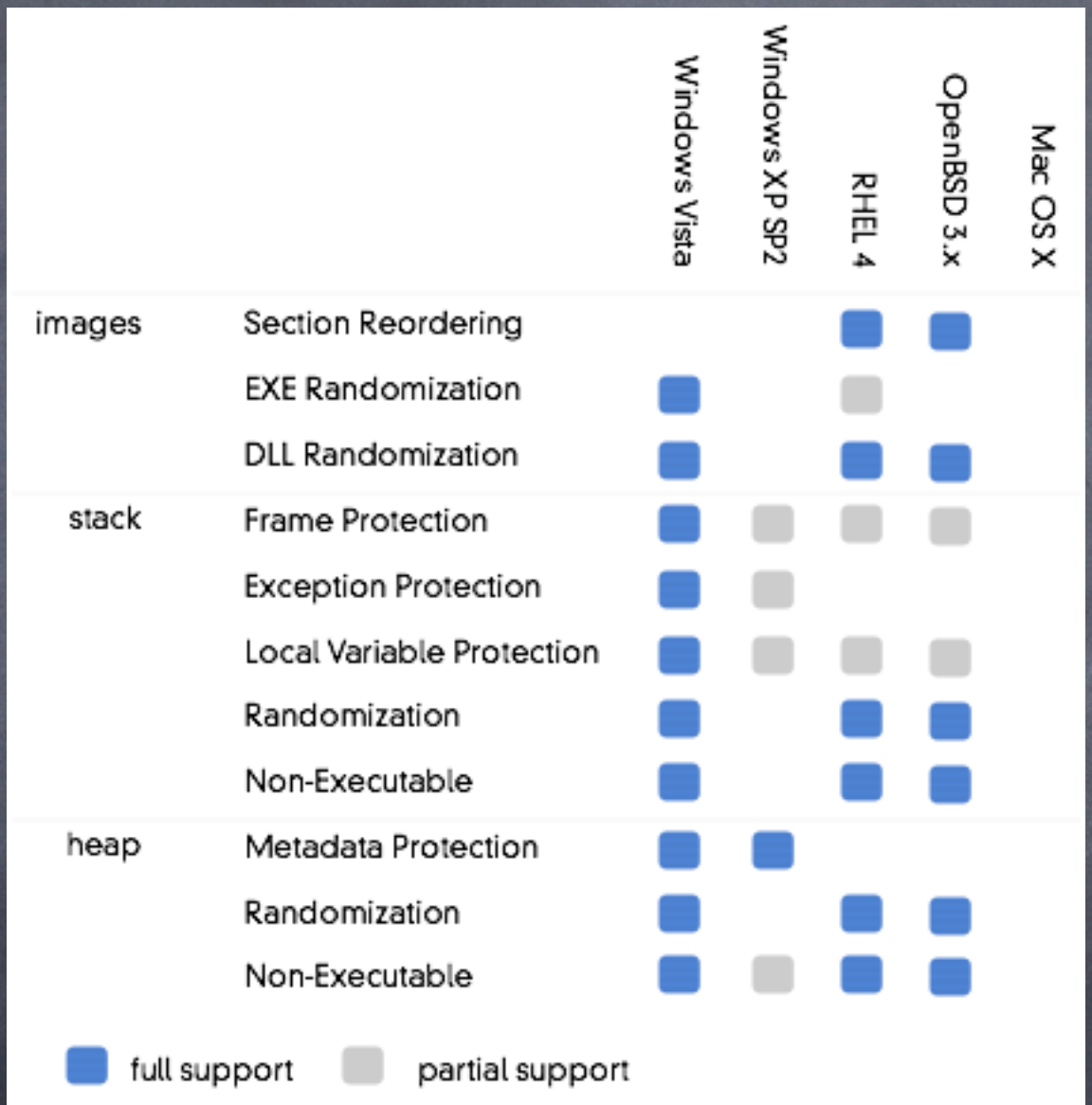
Odays on Mac OS X

- Honeypot in the congress network
- Capture Odays in action
- Learn about these attacks

Das wars.
Was hab ich vergessen?

Keychain Demo!

Apple muss was tun


Windows Vista
Windows XP SP2
RHEL 4
OpenBSD 3.x
Mac OS X
images
Section Reordering
EXE Randomization
DLL Randomization
stack
Frame Protection
Exception Protection
Local Variable Protection
Randomization
Non-Executable
heap
Metadata Protection
Randomization
Non-Executable
full support
partial support

Microsoft hat alle black hats gekauft.
Apple sollte das auch tun :)

Happy Hacking
cu@23c3

http://metalab.at/wiki/SYMWorkshop