Mac OS X at the Edge

Advanced Technologies and Security in OS X

Bruce Potter potter_bruce@bah.com gdead@shmoo.com

Who is this guy?

- Don’t believe anything I say

- Co-author of Mac OS X Security (New Riders), 802.11 Security (O’Reilly), Mastering BSD Security (O’Reilly Q4 2004)
- Founder of The Shmoo Group, NoVAWireless (now CAWNet)
- Currently a senior associate at Booz Allen Hamilton
- Ported many security apps to OS X Server in 99/00 timeframe

The History of Linux In One Slide

- This is a LUG, right? Old news here…
- Linux is just the Kernel
  - Open Source UNIX-alike
- Distro's add the tools and packaging
  - Debian, RedHat, SuSe, Mandrake, Slackware, etc…
  - To each his own
- "Chaotic" development model
  - Allows for rapid development, but may limit seamless integration

What Makes OS X Different

- Someone FINALLY put a usable UI on a UNIX core
  - Developed from a single vision (Thanks Steve)
  - Linux's strength is its weakness
    - Too many cooks in the kitchen?
- Seamless integration of many applications
- Seamless integration of peripherals
- Advanced networking, Super hardware
- Amazing printing support
  - Well, maybe not…
- Open source core - Darwin
- The Bottom Line: Many new and innovative technologies
  - Unknown or insuffiently explored security ramifications
  - "Thankfully" only a 3-5% market penetration

OS X Binaries - Mach-O

- Not statically linked, not dynamically linked
  - The best of both worlds
- Linker called at runtime to determine dependencies and write binding information to binary
  - Called **prebinding**… changes checksums
  - Further invocations of binary use prebound info
  - When running Software Update, responsible for the “Optimizing System”
- Ctool - tool for checksumming and file stating
  - http://www.macsecurity.org/tools/ctool/

Linux Binaries - ELF

- Executable and Linkable Format
- Standard static and dynamic linking we're all familiar with
- Dynamic executables are dynamically linked each time they are executed
- Has the advantage of being able to update one symbol at a time
- MUCH easier to checksum for integrity
  - Osiris (osiris.shmoo.com), tripwire, et al
- Slightly slower performance than Mach-O

OS X GUI - Cocoa and Aqua

- Cocoa - OS X Native frameworks using Objective C for rapid app development
  - Allows for easy UI building
  - Can glue legacy code to new OS X native UI
  - Apple distributes Xcode for free for OS X app development
    - Even I can code in Objective C with Xcode
    - Hot Spot Defense Kit (airsnarft.shmoo.com)
- Aqua - the OS X user interface
  - Apps are Aqua “compliant” not Aqua enabled or somesuch
  - It’s a UI “paradigm”
  - Shoot me now…

Linux GUI - Gnome/KDE and X

- Gnome/KDE
  - Competing Desktop Environments
  - Broad enough they really fill the same layer as Cocoa
  - Allow for easy-ish UI building under many different languages
  - Different open source tools available to ease development
- X Windows
  - Underlying Windowing system
  - Been around forever… not so much a “paradiigm” as a “confusing pile”
  - Now, OS X 10.3 ships with X on the CD
    - You still have to install it, but it’s an Apple supplied package
- Due to whole window manager/desktop environment/windowing system (of differing versions for different distros) it can be a real mess to make stable, uniform applications
  - Why do you think StarOffice is in Java?
  - OpenOffice has gone native.. What a PIA for the developers

OS X - Rendezvous

- No-configuration networking
- Uses Link Local addressing
  - So THAT'S what 169.254 is
- Service and host discovery via multicast
  - Now you have TWO nameservice mechanisms for IP… hope you or the OS doesn't get confused
- Finally, a "secure" IM
  - iChat can use rendezvous… at least it doesn't transgress your firewall
- Also, iTunes uses Rendezvous
- Hokie security model
  - Don't route multicast, don't accept packets with TTL <255
  - What about the "enterprise"?

Linux - ZeroConf

- Actually, it's the basis for Rendezvous
- IP addessing without DHCP server
- Multicast DNS
- Service discovery (finding printers, routers, etc…) automagically
- ZeroConf applications under linux
  - ….
  - …
  - Uhhh…

Wither ZeroConf on Linux

- From http://www.redhat.com/archives/fedora-devel-list/2004-March/msg00308.html

The mdnsd daemon for Linux is written, tested, debugged, and ready to go, yet it's not in any of the standard distributions. What we keep hearing from application developers (like people working on CUPS) is, "We'd love to use mdnsd, but it's not in any of the standard Linux distributions." What we keep hearing from the people working on the distributions is, "We don't know any Linux applications today that use mdnsd, so that must mean
there's no demand for it."

There are four files: A library, a header, a daemon, and a script to start it at boot time. You put those four files in, and CUPS can start using it. Support of link-local addressing is not necessary for CUPS to start using this, and neither is the "dot-local" gethostbyname() name lookup support.

I stand by my original statement: I don't understand what more I need to do to convince the Linux community of the benefit of this. It runs on OS X, OS 9, Windows, VxWorks, FreeBSD, etc. It runs on Pocket PC devices like the HP iPaq 5555, and PalmSource is working on adding it to Palm OS 6. It runs on every current network printer and an increasing list of other devices, like TiVos, Roku HD1000s, etc. Why isn't it already in standard Linux distributions so things like CUPS can start using it?

OS X - Bluetooth

- Short range wireless technology (PAN)
- Many BT devices available
  - Phones, keyboards, mice, printers, headphones, etc…
- BT Security research still in its infancy
- Discoverable mode is something to be used wisely
- OS X makes a great BT Wardriving platform
  - Continuously scans
  - BTW: discovered BT devices are stored in /var somewhere in a UTF-16 encoded file

Linux - Bluetooth

- Bluez is the best BT stack available
  - Bluez.sourceforge.net
  - Default FC2 install, download utils and libs, install RPM, modprobe, and you're up and working… impressively easy all things considered
  - Unlike OS X, developers have access to low-level BT functionality
  - btscanner is a real Bluetooth device discovery program
- Many K* apps support/leverage Bluetooth
  - Kde-bluetooth.sourceforge.net - relatively stable set of tools and interfaces
    - OBEX, device browse, pairing, etc..
    - Lots of apps built on top of KDE Bluetooth Framework
- I'm unaware of any "out of the box" BT support under Linux
  - Obviously, b/c of uncontrolled hardware platform compatiblity issues may still arise.

OS X - File Sharing

- Files sharing itself is not new… but the breadth is
- OS X wants to play nice
  - Apple file service for other Mac's
  - SAMBA for Windows users
  - NFS for UNIX folks
- Each has its own security mechanisms
- The GUI's try and prevent you from resharing
  - Transitivity issues
- AFS can be tunneled through SSH natively
  - Others can be "forced"
  - No real notification if SSH connection fails

Linux - File Sharing

- The same core functionality available as OS X for NFS and SAMBA
  - Generally an install time option for your particular distro
- Some UI functionality depending on desktop manager and/or distro
- AFS can be configured using netatalk (though be prepared for some integration issues)

OS X Data at Rest Security - File Vault

- AES encryption of your home dir
  - A huge improvement over the “encrypted volumes” available in DiskCopy (now DiskUtility)
- Different from Windows file encryption
  - Windows = attribute of a file
  - OS X = attribute of a directory
- “master password” for unlocking any file on a host
- Unclear how this integrates into an enterprise
- Disk Utility encryption has it’s places
  - .dmg files which when launched are mounted
  - AES-128 to protect the image
    - Password can be stored in keychain
  - Great for mail, customer documents, etc

Linux Data at Rest Security -Many Options

- CFS - Matt Blaze's filesystem encryption implementation
- EncFS - Userspace, dyanmically sized directory encryption for 2.4/2.6 kernels
- Loop-AES - AES encryption for whole filesystems (new release on 9/7/04)
- But, really, there's no standard from distro to distro.. And UI tools likely won't understand what to do with an undecrypted volume
- Lots of pointers: http://www.infoanarchy.org/wiki/wiki.pl?Hard_Disk_Encryption

OS X “DigItal Hub” - iStuff

- iMovie, iDVD, iPhoto, iTunes, iCal, etc..
  - All play nice together
  - Primitive interfaces between the programs
- No security vulnerabilities.. Yet
  - Lots of untested code
  - Little if any SUID executables
  - However… what about malicious JPEG’s, MOV’s, .ics’s, etc…
- Potential problems down the road
  - One exploit to rule them all?

Linux “Digital Hub” - many point solutions

- iTunes = more Linux audio programs than I can count
  - Jon Johansen can unDRM iTunes songs and let you stream them over your Airport Express - http://www.nanocrew.net/blog/
- iCal = more Linux calendaring options than I can count
- iPhoto = gimp? Heck, you could use gallery or something on a local webserver - http://gallery.menalto.com/modules.php?op=modload&name=News&file=index
  - Linspire sells knockoff iPhoto and iTunes products for Linux
- iMovie and iDVD = ?? I don’t know of any OSS movie manipulation tools that even come close
  - I’m sure there are professional for-pay ones…
- Again, no integratred solution. Also, no interoperable solutions

OS X - WebDAV

- From the WebDAV website:

  Briefly: WebDAV stands for "Web-based Distributed Authoring and Versioning". It is a set of extensions to the HTTP protocol which allows users to collaboratively edit and manage files on remote web servers

  - So, it's like a wiki with an API

- Neat for shared calendars and collaborative publishing
- Terrible if you don't trust everyone
- Subversion uses WebDAV as a mechanism for version control (yikes)
- An access control mechanism is a proposed standard

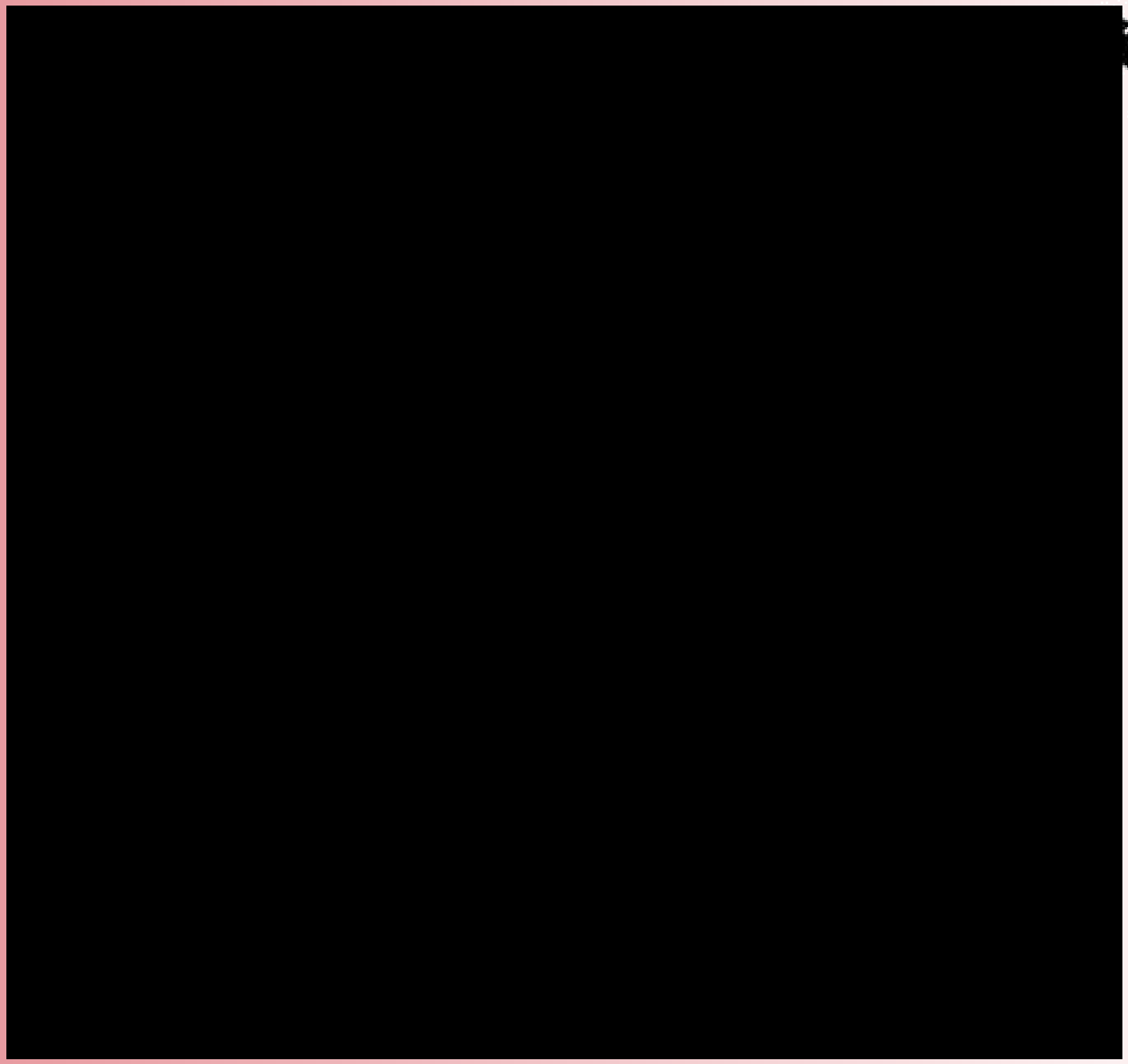
Linux - WebDAV

- Not integrated, but code can be downloaded from www.webdav.org

- Don’t worry, it seems that nobody cares about this technology anyway ;)

OS X Firewalling - IPFW

- Uses standard ipfw firewalling
  - Powerful
- Slaps on the simplest UI ever
  - TCP only.. All UDP is dropped except for replies
  - TCP/UDP is all there is, right?
  - In the Sharing Preferences Pane
- Best to just use the command line and your own rc scripts



Linux Firewalling - IPChains

- Very powerful. Very flexible.
- In every distro (jjust maybe not enabled)
- Several UI's to choose from
  - The config file can be… "confusing"
- Some commercial firewalls are available for Linux as well
- Better hardware options (more than one interface :)

OS X Enterprise Security - Kerberos

- We all use Kerberos, right?
- Shocking amount of kerb integration
  - ftp
  - Afp
  - Mail.app
  - LoginWindow
  - Telnet
  - Mac Manager

Linux Enterprise Security - Kerberos

- May or may not come in default distro
- Kerberized software can be downloaded and installed
  - Ktelnet, kftp, kwhatever… (no, not KDE)
- Or… use pam_krb5 and pam-enabled applications can make use of the kerberos infrastructure with having to rewrite them
  - W00t! Abstracting the authentication process actually works to our advantage sometimes

OS X Password Management - Keychain

- Password store for websites, disk images, etc..
  - No more “one application, one data store”
- A master password controls access to keychain
- Application must be keychain aware
- Selected passwords can be automatically decrypted

- All your eggs in one basket?
  - Easily “defeats” the point of a password

Linux Password Management - ??

- Some applications have integrated password management
  - Mozilla comes to mind
  - Ssh has ssh-agent for automatic log-ins
- Lots of little projects on sourceforge/freshmeat to store passwords securely
- No single framework (at least a widely adopted framework) like keychain

OS X - Hardware

- Powerbooks, iBooks
- G5 Desktops
- Xserves
- iMac, eMac
- … uh…

Linux - Hardware

- Old x86 boxes
- New IA64 servers
- Phones
- Pdas
- Cars
- Planes
- Damn near anything…

Questions?

- Besides *Mac OS X Security* consider:
  - Mac OS X for UNIX Geeks - O'Reilly and Assoc
  - Mac OS X Hacks - O'Reilly and Assoc

  - http://www.shmoo.com/~gdead/OSXSecurity.ppt