Mac OS X Security

Leon Towns-von Stauber

O’Reilly Mac OS X Conference 2002

http://www.occam.com/ocr/osx/
<table>
<thead>
<tr>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Out-of-the-Box Security</td>
<td>1</td>
</tr>
<tr>
<td>File Security</td>
<td>3</td>
</tr>
<tr>
<td>Privileged Access</td>
<td>9</td>
</tr>
<tr>
<td>Open Directory</td>
<td>19</td>
</tr>
<tr>
<td>Password Server</td>
<td>27</td>
</tr>
<tr>
<td>Extra Password Protection</td>
<td>33</td>
</tr>
<tr>
<td>Network Services</td>
<td>41</td>
</tr>
<tr>
<td>Packet Filtering</td>
<td>55</td>
</tr>
<tr>
<td>Network Encryption</td>
<td>60</td>
</tr>
<tr>
<td>Miscellany</td>
<td>68</td>
</tr>
<tr>
<td>Resources</td>
<td>79</td>
</tr>
<tr>
<td>Recent Issues</td>
<td>83</td>
</tr>
<tr>
<td>Closing Remarks</td>
<td>85</td>
</tr>
</tbody>
</table>
Due to time constraints, this presentation will merely introduce you to security-related features and issues in Mac OS X.

- You can find more details in man pages, the Server Administrator’s Guide, online help, and other resources.
- I’ll assume user experience with OS X, and basic UNIX familiarity will help.
- Mac OS X (Server) 10.2.1 / Darwin 6.1
This presentation Copyright © 2002 Leon Towns-von Stauber. All rights reserved.

Mac OS, AirPort, and QuickTime are trademarks of Apple Computer. See Apple’s Trademark List.

UNIX is a trademark of The Open Group.

xFiles, BrickHouse, Pseudo, PuzzlePalace, and CheckMate are trademarks of Brian Hill.

SSH Helper is a trademark of Gideon Softworks.

SSH Agent is a trademark of the Utrecht University Department of Philosophy.

VPN Tracker is a trademark of Equinux.
• Apple’s customers were used to a secure out-of-the-box experience

• Mac OS X has the most secure default configuration of any major UNIX platform

• Finally, a UNIX vendor that takes security seriously
Out-of-the-Box Security

• No network-accessible services are enabled
  • Except for the Rendezvous multicast DNS server
    (more on this later)
• The root account is disabled
• NB: Neither of these statements is true for Mac OS X Server
File Security

- UNIX Permissions
- BSD Flags
• Filesystem objects use traditional UNIX and BSD access restrictions
• Every object has an owning user and group
• Read, write, and execute permissions are applied for the user, group, and everyone else
• Permissions can be viewed and changed with Get Info in the Finder
• That and more with xFiles
Viewing and setting permissions with Get Info
• At the command line:

• View with `ls -l`

• Example (in ~/Sites):

```
-rw-r-----  1 leonvs  admin     0 Aug 29 03:21 Icon?
drwxr-x---  8 leonvs  admin   272 Feb 13  2001 images
-rwxr-x---  1 leonvs  admin  6186 Feb 13  2001 index.html
```

• Change owning user with `chown`

• Change owning groups with `chgrp`

• Change permissions with `chmod`

• Other options: setuid, setgid, sticky
• At the command line:
  
  • Set default permissions for shell processes with umask in shell init script

  • Octal argument masks out unwanted permissions
- Can set files to immutable or append-only
  - Prevent unauthorized changes to configs, logs, etc.
- At CLI, use chflags
- HFS Locked attribute is mapped to BSD immutable flag
- Can view and set in Get Info dialog
- /Developer/Tools/GetFileInfo -al file
- /Developer/Tools/SetFile -a L file
  - Same as chflags uchg file
- Cause of occasional permissions errors when trying to empty Trash
Privileged Access

- The root Account
- Administrative User Accounts
- Domain Administrators
• root is the UNIX “superuser”
  • Unrestricted by file permissions
  • Can take on the identity of any other user
• root logins disabled in Mac OS X
  • Password is locked
• Enabling root logins
  • NetInfo Manager
    • Under Security, Authenticate..., then Enable Root User and set a password
  • Or, at the CLI, passwd root
• The root account is enabled in Mac OS X Server
  • Password set the same as the first user account created
  • Reset one of these passwords so they’re not the same
• Enabling root logins is almost never necessary and not recommended

• Limited superuser privileges are available to administrative user accounts
  • Defined by membership in the admin user group
  • Account created during OS install is an admin account
• Administrative users have four sources of privilege
  • Directory permissions
  • sudo
  • Authorization API
  • AFP access
• If desired, could grant some or all of the same privileges to other groups or users (except AFP access?)
• Permissions

  • /Applications, /Library, /Developer owned and writable by admin group

• sudo

  • Run command-line utilities as root or another user by preceding the invocation with sudo

• Configured in /etc/sudoers
• Authorization API

  • Uses password authentication to allow activities requiring privileged access

  • Used by System Preferences, Installer, administrative applications, etc.

  • Configured in /etc/authorization

  • authopen

    • CL tool that uses Authorization API to open files as privileged user
Privileged Access

Admin Users

- Apple Filesharing (AFP) access
  - Admin users can mount AFP shares as any user by providing admin account password
  - Used to test AFP setups for users
  - Open Directory properties in /config/AppleFileServer
    - special_admin_privs
    - admin_gets_sp
    - allow_root_login
  - Unfortunately, no documentation
- Open Directory Domain Administrators
  - Users can be designated as administrators of particular Open Directory domains
- Configured in Workgroup Manager
  - Stored in `admin_limits` Open Directory property
- Specify which aspects of users, groups, and machines can be managed
- Can limit to specific users, groups, and machines
  - Can’t specify elements NOT to be managed
Setting domain admin privileges in Workgroup Manager
Open Directory

- NetInfo
- LDAP
• NetInfo Security Features
  • Flexible granting of write privileges
    • _writers_property property
      • _writers_passwd: user
  • Access restriction by subnet
    • trusted_networks property in root directory of domain
  • Specified as partial dotted-decimal address, or name from /networks
• More NetInfo Security Features

  • Firewall in Mac OS X Server can be configured to limit access to NetInfo ports, even if dynamic
  • netinfod can be configured to run on statically assigned port, to enable port-based filtering in OS X or external firewall
    • port property in root directory
Limiting NetInfo access in Mac OS X Server Firewall config
• NetInfo Security Shortcomings
  • Unshadowed password hashes (if using Basic authentication)
    • _shadow_property does not work
  • Partial workaround: set restrictive file permissions on NetInfo utilities
  • Unsecured network communications
    • Parent/child and master/clone interactions in the clear
  • Solution: IPsec
• Issues with client-to-server binding

  • No real client authentication

    • Use trusted_networks, and secure possession of your network addresses as well as possible

  • Broadcast binding makes clients more vulnerable to rogue servers

    • Rogue needs only valid host/IP information and a quick response
• Based on OpenLDAP
  • Can set up OpenLDAP ACLs in `/etc/openldap/slapd.conf`
  • Secure network client access via SSL
    • Enabled on client in Directory Access
Enabling SSL on LDAP connections
Password Server

- Overview
- Planning Issues
• Part of Mac OS X Server Open Directory

• If Password Server authentication is enabled for an account, instead of a password hash, a 128-bit password ID is stored for the account
  • Password ID is a key to an entry in Password Server
  • Authentication scheme determined by authentication_authority property
    • Other schemes: Basic-Specific (could use MD5 password, or PKI cert (future)), Kerberos (future), ...
• Based on SASL (Simple Authentication and Security Layer)

• Supports many authentication protocols, including CRAM-MD5, Windows LAN Manager, Windows NT, APOP, ...

• Can set password policies, such as minimum length and expiration time

  • In Workgroup Manager, under the Advanced tab of a user, click Options...
Password Server Options

Minimum length: [ ] characters

- Force the user to change password
- At next login
  - Every [ ] days
- Disable login as of [ ]
- Disable inactive account after [ ] days

[ ] Cancel [ ] OK
• Specified for Open Directory domain by
  /config/passwordserver
• Does not support loginwindow on pre-10.2 clients
• Passwords either encrypted or hashed
  • Reversibly encrypted if APOP or AFP 2-Way Random
    are enabled
  • Otherwise only a one-way hash is stored
• Like Kerberos, it is vital that the Password Server server
  be kept tightly secured
• No Password Server service replication
  • Server must be highly available
  • If server goes down, all Password Server-based authentication fails
  • Consider not using for admin accounts
  • Try regular sync of
    /var/db/authserver/authservermain to warm standby server
Extra Password Protection

- Shadowed Password File
- Keychain Access
- Screen Effects
- Open Firmware
- `chkpasswd`
• Can set up a shadowed password flat file

• `nidump passwd . | sudo tee /etc/master.passwd`

• `sudo vipw`, then save and exit

• `/etc/passwd` contains account information,
  `/etc/master_passwd` (only readable by root) contains password hashes

• Configure `lookupd` to look at flat files for user information
• Convenience feature, stores multiple passwords in a Keychain, recoverable with a Keychain passphrase
  • Can also make secure (encrypted) notes
  • Located in ~/Library/Keychains
• Make sure users lock their Keychains with a (good) passphrase!
  • In Keychain Access, under Edit, select settings for particular Keychain
  • For each item in a Keychain, require confirmation with a Keychain passphrase
Setting Keychain Passphrase
• Can lock screen saver with login password

• System Preferences -> Screen Effects -> Activation -> Use my user account password
• Can set password in Open Firmware
  • Disables most boot options
  • Password required to access OF
• Open Firmware Password application downloaded from Apple Web site
• Sets security-mode in NVRAM to command
• Can prevent boot without password by setting to full
  • `sudo nvram security-mode = full`
Setting Open Firmware Password
• Simple command to prompt for user password and return success or failure

• `chkpasswd username`

• Useful for scripts performing actions that should require privileged access
Network Services

- hosts_access
- xinetd
- SSH (Secure Shell)
- Apache
- File Sharing
- CUPS (Common UNIX Printing System)
- Apple Mail Server
- Streaming Server
- DHCP & NetBoot
- SNMP
• Network-based access restrictions
  • Used by services managed by inetd (indicated by tcpd in inetd.conf)
  • Sendmail, SSH, and others can be compiled to support it
• Controlled by two files: /etc/hosts.allow and /etc/hosts.deny
• Part of tcp_wrappers software
• man 5 hosts_access for details of syntax
Network Services  xinetd

• Replaces inetd in Jaguar as front end for many network services (which are rarely used in Mac OS X)

• Similar access restrictions to tcp_wrappers

• Configured in /etc/xinetd.conf and in
  /etc/xinetd.d/ for individual services

  • Man page for xinetd.conf doesn’t appear to be installed
• Enabled by Remote Login in Sharing Preferences
• Configured in /etc/sshd_config
• Can restrict access by user or group
• Several options related to use of rhosts/shosts files
• More options in authorized_keys files
• man sshd_config and man sshd
• Native web server in Mac OS X and Mac OS X Server

• Configured with (well-commented) files in /etc/httpd/

• Can restrict access by network address

• Can require authentication

• SSL encryption available
• In Mac OS X Server, can set privileges and enable/disable guest access to share points (defined in Workgroup Manager)

• AFP (in Mac OS X Server)
  • Can be run over SSH for encryption
  • Can use Kerberos authentication

• NFS (in Mac OS X Server)
  • Access can be restricted by network address
  • Re-export NFS mounts using AFP, and gain user-based authentication and encrypted transport
Configuring AFP security options in Server Settings
- SMB
  - Numerous security-affecting parameters in `/etc/smb.conf`
- FTP (in Mac OS X Server)
  - Can use Kerberos authentication
  - `/Library/FTPServer/Configuration/ftpaccess`
• CUPS is the print engine in Jaguar

• CUPS server configured in /etc/cups/cupsd.conf
  • Very similar to Apache configuration

• Can restrict access to printer browsing and to CUPS web interface by network address
  • Limited to localhost access by default

• Can require authentication to access web interface
  • For example, can require admin group membership
    • AuthClass set to Anonymous by default

• SSL/TLS encryption available for web interface
• Apple Mail Server supports diverse methods of secure authentication
  • SMTP: SMTP AUTH and Kerberos
  • POP: APOP and Kerberos
  • IMAP: CRAM-MD5 and Kerberos
• Can limit SMTP relay to specified hosts or networks
• All settings made in Server Settings
Network Services  Streaming Server

- QuickTime Streaming Server (included with OS X Server) or Darwin Streaming Server
- User accounts and passwords in /Library/QuickTimeStreaming/Config/qtuser
- Groups in qtgroup
- Users set up with qtpasswd
- Access files in media directories named qtaccess follow htaccess format
• DHCP & NetBoot/NetInstall services in Mac OS X Server share list whereby clients may be granted/refused access by MAC (Ethernet) address
Creating DHCP/NetBoot MAC address filter list in Server Settings
• Multitude of access restriction capabilities

• Start out by running `sudo snmpconf -g basic_setup`
  • Then check config files in `/usr/share/snmp`
Packet Filtering

- ipfw
- Graphical Tools
Packet Filtering

• Packet filter (ipfw) built into kernel

• ipfw list
  
  02000 allow ip from any to any via lo*
  02010 deny ip from 127.0.0.0/8 to any in
  02020 deny ip from any to 127.0.0.0/8 in
  02050 allow tcp from any to any out
  02060 allow tcp from any to any established
  12180 reset tcp from any to any setup
  12190 deny tcp from any to any
  65535 allow ip from any to any

• ipfw add 02070 allow tcp from any to any 22 in
Mac OS X Firewall in Sharing Preferences
Packet Filtering  Graphical Tools

Mac OS X Server Firewall in Server Settings
Packet Filtering  
Graphical Tools

BrickHouse
Network Encryption

- SSH (Secure Shell)
- SSL/TLS (Secure Sockets Layer/Transport Layer Security)
- IPsec
- PPTP (Point-to-Point Tunneling Protocol)
- AirPort and WEP (Wired Equivalent Privacy)
• Provides remote logins with secure authentication and encryption
• Enabled from Sharing Preferences (as Remote Login)
• Use only SSH2 if possible
  • SSH1 is vulnerable to man-in-the-middle attacks
    • dsniff
  • Protocol parameter in sshd_config (for server) and ssh_config (for client)
• Third-party GUI tools: SSH Helper, SSH Agent
• Provides encryption and certificate-based authentication

• Can be used with LDAP, IMAP, HTTP, WebDAV

• Server admin tools use it

• Command-line certtool simplifies management of certificates
Based on KAME, same software used on other BSD platforms

Provides authentication and encryption at a lower layer of the TCP/IP stack, transparent to applications

No built-in GUI

- Managed with setkey, racoon, and sysctl

VPN Tracker provides GUI
IPsec Setup with VPN Tracker
• Personal VPN used primarily by Microsoft

• Configured in Internet Connect

• In Mac OS X Server, vpnd provides a PPTP front end to the PPP daemon
• WEP provides minimal encryption for wireless 802.11 connections

• For security, you should use a strong 128-bit password, and create a closed network

• Setting up IPsec between hosts on wireless network would provide good security
Network Crypto  AirPort & WEP

AirPort Base Station Settings

New password: **************
Verify: **************
WEP key length: 128-bit

Name: Lakshmi
Contact: Leon Towns-von Stauber
Location: 

AirPort Network
Name: Lakshmi
Create a closed network
Channel: 1
Station density: Low
Multicast rate: 2

Enable interference robustness
Enable encryption (using WEP)

Cancel  OK
Login Options
· PAM (Pluggable Authentication Modules)
· Kerberos
· securelevel
· Rendezvous
· Process Accounting
· More Tools
· STOS & SE-Darwin
• Under Accounts Preferences
  • Auto Login is not appropriate for machines in most non-home environments
  • If you’re concerned about security, don’t Display Login Window as List of Users
  • Don’t enable display of password hints
• PAM is a cross-platform (UNIX) front end enabling the use of multiple authentication methods
• BSD utilities use PAM to access Security Server
  • Native Mac OS X apps contact Security Server through other APIs
  • Enables the use of Open Directory passwords, Password Server, etc. by legacy UNIX programs
• Configured per service in /etc/pam.d/
• In addition to mail services, AFP, and FTP, can be used to authenticate logins via loginwindow and TELNET
  • Note: TELNET is still a bad idea; use SSH
• Set up Kerberos server
  • Create accounts in OS X with Basic authentication and bogus passwords
  • Copy keytab from KDC to /etc/krb5.keytab in OS X
• Need `edu.mit.Kerberos` config file in 
  `/Library/Preferences, and ~/Library/Preferences` 
  for each user

• `loginwindow` support in `/etc/authorization`
  
  • Kerberos auth as requirement: in
    
    `system.login.console` string, replace
    `authinternal` with `krb5auth:authenticate`

  • Kerberos auth as side effect: change string for
    
    `system.login.done` from `switch_to_user` to
    `switch_to_user, krb5auth:login`
• Normally run at level 1

• Set higher with `sudo sysctl -w securelevel = 2`
  • Raw access to disk devices is read-only

• `man init` for more
• Rendezvous presents some security issues

• Any machine on the physical network can automatically acquire a valid IP address, no prior knowledge necessary
  • Could block traffic from 169.254.x.x addresses, or scan for rogue addresses
• mDNSResponder functions by default, listening for hostname to IP address mappings
  • Could create confusion if hostname is badly chosen, by malice or accident
  • Could disable all multicast traffic, or block access to port 5353
- Can enable tracking of every process run

- `sudo mkdir /var/account`
- `sudo touch /var/account/acct`
- `sudo accton /var/account/acct`
- Also handled by
  
  `/System/Library/StartupItems/Accounting/Accounting`

- `lastcomm`

- Watch out, file can get big quickly
  
  - By default, rotated daily
• Disk Copy can create password-locked encrypted disk images for confidential data

• PuzzlePalace offers drag-and-drop file encryption and decryption

• CheckMate calculates MD5 checksums of files, to help detect unauthorized changes
  • md5 does the same at the CLI

• Psuedo uses the Authorization API to launch applications with root privileges
Secure Trusted Operating System

- Consortium of developers from government, academia, and private enterprise

SE-Darwin

- Project to provide military-grade OS extensions to Darwin

http://www.stosdarwin.org/
• Apple’s Mac OS X site
  • http://www.apple.com/macosx/

• Apple’s Security Updates page
  • http://www.apple.com/support/security/security_updates.html

• MacSecurity.org
  • http://www.macsecurity.org/

• SANS Reading Room: Apple Issues
  • http://rr.sans.org/mac/mac_list.php
• Mac OS X Hints
  • http://www.macosxhints.com/

• Occam’s Razor Apple/NeXT page
  • http://www.occam.com/ocr/computer/apple.html

• Version Tracker
  • http://www.versiontracker.com/
• security-announce (Apple)
  • http://lists.apple.com/mailman/listinfo/security-announce/

• MacSec (MacSecurity.org)
  • http://www.macsecurity.org/mailman/listinfo/macsec/
• MacOSX-admin (Omni Group)
  • http://www.omnigroup.com/developer/mailinglists/macosx-admin/

• macos-x-server (Apple)
  • http://lists.apple.com/mailman/listinfo/macos-x-server/
Recent Issues

• Unspecified remote exploit in Terminal 1.3 (which came with 10.2)
  • Addressed by Security Update 2002-09-20

• NetInfo Manager is setuid root
  • When printing to PDF, can navigate filesystem and save files as root

• Buffer overflow in gm4
  • GNU m4 macro processor, installed with Developer Tools

• Probably doesn’t present security issue
Recent Issues

- SSL certificate chains processed improperly
  - Resolved in OmniWeb 4.1.1 and IE 5.2.2
- Buffer overflow in Stuffit Expander
  - Caused by long filenames in ZIP archives
  - Resolved in version 7.0
• This talk has focused on security issues, both risks and opportunities, specific to Mac OS X

• But remember that Mac OS X is UNIX, and similar considerations apply as to any other UNIX platform

• Evaluation forms

• Q & A