CIS Mac OS X Tiger Level I Security Benchmark

Version 2.0
October 16th, 2006

Edited by Matt Emerson

Terms of Use

BACKGROUND.

THE CENTER FOR INTERNET SECURITY ("CIS") PROVIDES BENCHMARKS, SCORING TOOLS, SOFTWARE, DATA, INFORMATION, SUGGESTIONS, IDEAS, AND OTHER SERVICES AND MATERIALS FROM THE CIS WEBSITE OR ELSEWHERE (“PRODUCTS”) AS A PUBLIC SERVICE TO INTERNET USERS WORLDWIDE. RECOMMENDATIONS CONTAINED IN THE PRODUCTS (“RECOMMENDATIONS”) RESULT FROM A CONSENSUS-BUILDING PROCESS THAT INVOLVES MANY SECURITY EXPERTS AND ARE GENERALLY GENERIC IN NATURE. THE RECOMMENDATIONS ARE INTENDED TO PROVIDE HELPFUL INFORMATION TO ORGANIZATIONS ATTEMPTING TO EVALUATE OR IMPROVE THE SECURITY OF THEIR NETWORKS, SYSTEMS, AND DEVICES. PROPER USE OF THE RECOMMENDATIONS REQUIRES CAREFUL ANALYSIS AND ADAPTATION TO SPECIFIC USER REQUIREMENTS. THE RECOMMENDATIONS ARE NOT IN ANY WAY INTENDED TO BE A “QUICK FIX” FOR ANYONE’S INFORMATION SECURITY NEEDS.

NO REPRESENTATIONS, WARRANTIES, OR COVENANTS.

CIS MAKES NO REPRESENTATIONS, WARRANTIES, OR COVENANTS WHATSOEVER AS TO (I) THE POSITIVE OR NEGATIVE EFFECT OF THE PRODUCTS OR THE RECOMMENDATIONS ON THE OPERATION OR THE SECURITY OF ANY PARTICULAR NETWORK, COMPUTER SYSTEM, NETWORK DEVICE, SOFTWARE, HARDWARE, OR ANY COMPONENT OF ANY OF THE FOREGOING OR (II) THE ACCURACY, RELIABILITY, TIMELINESS, OR COMPLETENESS OF THE PRODUCTS OR THE RECOMMENDATIONS. CIS IS PROVIDING THE PRODUCTS AND THE RECOMMENDATIONS “AS IS” AND “AS AVAILABLE” WITHOUT REPRESENTATIONS, WARRANTIES, OR COVENANTS OF ANY KIND.

USER AGREEMENTS.

BY USING THE PRODUCTS AND/OR THE RECOMMENDATIONS, I AND/OR MY ORGANIZATION (“WE”) AGREE AND ACKNOWLEDGE THAT:

1. NO NETWORK, SYSTEM, DEVICE, HARDWARE, SOFTWARE, OR COMPONENT CAN BE MADE FULLY SECURE;
2. WE ARE USING THE PRODUCTS AND THE RECOMMENDATIONS SOLELY AT OUR OWN RISK;
3. WE ARE NOT COMPENSATING CIS TO ASSUME ANY LIABILITIES ASSOCIATED WITH OUR USE OF THE PRODUCTS OR THE RECOMMENDATIONS, EVEN RISKS THAT RESULT FROM CIS’S NEGLIGENCE OR FAILURE TO PERFORM;
4. WE HAVE THE SOLE RESPONSIBILITY TO EVALUATE THE RISKS AND BENEFITS OF THE PRODUCTS AND RECOMMENDATIONS TO US AND TO ADAPT THE PRODUCTS AND THE RECOMMENDATIONS TO OUR PARTICULAR CIRCUMSTANCES AND REQUIREMENTS;
5. NEITHER CIS, NOR ANY CIS PARTY (DEFINED BELOW) HAS ANY RESPONSIBILITY TO MAKE ANY CORRECTIONS, UPDATES, UPGRADES, OR BUG FIXES; OR TO NOTIFY US OF THE NEED FOR ANY SUCH CORRECTIONS, UPDATES, UPGRADES, OR BUG FIXES; AND
6. NEITHER CIS NOR ANY CIS PARTY HAS OR WILL HAVE ANY LIABILITY TO US WHATSOEVER (WHETHER BASED IN CONTRACT, TORT, STRICT LIABILITY OR OTHERWISE) FOR ANY DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, OR SPECIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOSS OF PROFITS, LOSS OF SALES, LOSS OF OR DAMAGE TO REPUTATION, LOSS OF CUSTOMERS, LOSS OF SOFTWARE, DATA, INFORMATION OR EMAILS, LOSS OF PRIVACY, LOSS OF USE OF ANY COMPUTER OR OTHER EQUIPMENT, BUSINESS INTERRUPTION, WASTED MANAGEMENT OR OTHER STAFF RESOURCES OR CLAIMS OF ANY KIND AGAINST US FROM THIRD PARTIES) ARISING OUT OF OR IN ANY WAY CONNECTED WITH OUR USE OF OR OUR INABILITY TO USE ANY OF THE PRODUCTS OR RECOMMENDATIONS (EVEN IF CIS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES), INCLUDING WITHOUT LIMITATION ANY LIABILITY ASSOCIATED WITH INFRINGEMENT OF INTELLECTUAL PROPERTY, DEFECTS, BUGS, ERRORS, OMISSIONS, VIRUSES, WORMS, BACKDOORS, TROJAN HORSES OR OTHER HARMFUL ITEMS.

GRANT OF LIMITED RIGHTS.

CIS HEREBY GRANTS EACH USER THE FOLLOWING RIGHTS, BUT ONLY SO LONG AS THE USER COMPLIES WITH ALL OF THE TERMS OF THESE AGREED TERMS OF USE:

1. EXCEPT TO THE EXTENT THAT WE MAY HAVE RECEIVED ADDITIONAL AUTHORIZATION PURSUANT TO A WRITTEN AGREEMENT WITH CIS, EACH USER MAY DOWNLOAD, INSTALL AND USE EACH OF THE PRODUCTS ON A SINGLE COMPUTER;
2. EACH USER MAY PRINT ONE OR MORE COPIES OF ANY PRODUCT OR ANY COMPONENT OF A PRODUCT THAT IS IN A .TXT, .PDF, .DOC, .MCW, OR .RTF FORMAT, PROVIDED THAT ALL SUCH COPIES ARE PRINTED IN FULL AND ARE KEPT INTACT, INCLUDING WITHOUT LIMITATION THE TEXT OF THIS AGREED TERMS OF USE IN ITS ENTIRETY.

RETENTION OF INTELLECTUAL PROPERTY RIGHTS; LIMITATIONS ON DISTRIBUTION.

THE PRODUCTS ARE PROTECTED BY COPYRIGHT AND OTHER INTELLECTUAL PROPERTY LAWS AND BY INTERNATIONAL TREATIES. WE ACKNOWLEDGE AND AGREE THAT WE ARE NOT ACQUIRING TITLE TO ANY

INTELLECTUAL PROPERTY RIGHTS IN THE PRODUCTS AND THAT FULL TITLE AND ALL OWNERSHIP RIGHTS TO THE PRODUCTS WILL REMAIN THE EXCLUSIVE PROPERTY OF CIS OR CIS PARTIES. CIS RESERVES ALL RIGHTS NOT EXPRESSLY GRANTED TO USERS IN THE PRECEDING SECTION ENTITLED “GRANT OF LIMITED RIGHTS.”

SUBJECT TO THE PARAGRAPH ENTITLED “SPECIAL RULES” (WHICH INCLUDES A WAIVER, GRANTED TO SOME CLASSES OF CIS MEMBERS, OF CERTAIN LIMITATIONS IN THIS PARAGRAPH), AND EXCEPT AS WE MAY HAVE OTHERWISE AGREED IN A WRITTEN AGREEMENT WITH CIS, WE AGREE THAT WE WILL NOT (I) DECOMPILE, DISASSEMBLE, REVERSE ENGINEER, OR OTHERWISE ATTEMPT TO DERIVE THE SOURCE CODE FOR ANY SOFTWARE PRODUCT THAT IS NOT ALREADY IN THE FORM OF SOURCE CODE; (II) DISTRIBUTE, REDISTRIBUTE, ENCUMBER, SELL, RENT, LEASE, LEND, SUBLICENSE, OR OTHERWISE TRANSFER OR EXPLOIT RIGHTS TO ANY PRODUCT OR ANY COMPONENT OF A PRODUCT; (III) POST ANY PRODUCT OR ANY COMPONENT OF A PRODUCT ON ANY WEBSITE, BULLETIN BOARD, FTP SERVER, NEWSGROUP, OR OTHER SIMILAR MECHANISM OR DEVICE, WITHOUT REGARD TO WHETHER SUCH MECHANISM OR DEVICE IS INTERNAL OR EXTERNAL, (IV) REMOVE OR ALTER TRADEMARK, LOGO, COPYRIGHT OR OTHER PROPRIETARY NOTICES, LEGENDS, SYMBOLS OR LABELS IN ANY PRODUCT OR ANY COMPONENT OF A PRODUCT; (V) REMOVE THESE AGREED TERMS OF USE FROM, OR ALTER THESE AGREED TERMS OF USE AS THEY APPEAR IN, ANY PRODUCT OR ANY COMPONENT OF A PRODUCT; (VI) USE ANY PRODUCT OR ANY COMPONENT OF A PRODUCT WITH ANY DERIVATIVE WORKS BASED DIRECTLY ON A PRODUCT OR ANY COMPONENT OF A PRODUCT; (VII) USE ANY PRODUCT OR ANY COMPONENT OF A PRODUCT WITH OTHER PRODUCTS OR APPLICATIONS THAT ARE DIRECTLY AND SPECIFICALLY DEPENDENT ON SUCH PRODUCT OR ANY COMPONENT FOR ANY PART OF THEIR FUNCTIONALITY, OR (VIII) REPRESENT OR CLAIM A PARTICULAR LEVEL OF COMPLIANCE WITH A CIS BENCHMARK, SCORING TOOL OR OTHER PRODUCT. WE WILL NOT FACILITATE OR OTHERWISE AID OTHER INDIVIDUALS OR ENTITIES IN ANY OF THE ACTIVITIES LISTED IN THIS PARAGRAPH.

WE HEREBY AGREE TO INDEMNIFY, DEFEND, AND HOLD CIS AND ALL OF ITS OFFICERS, DIRECTORS, MEMBERS, CONTRIBUTORS, EMPLOYEES, AUTHORS, DEVELOPERS, AGENTS, AFFILIATES, LICENSORS, INFORMATION AND SERVICE PROVIDERS, SOFTWARE SUPPLIERS, HARDWARE SUPPLIERS, AND ALL OTHER PERSONS WHO AIDED CIS IN THE CREATION, DEVELOPMENT, OR MAINTENANCE OF THE PRODUCTS OR RECOMMENDATIONS (“CIS PARTIES”) HARMLESS FROM AND AGAINST ANY AND ALL LIABILITY, LOSSES, COSTS, AND EXPENSES (INCLUDING ATTORNEYS' FEES AND COURT COSTS) INCURRED BY CIS OR ANY CIS PARTY IN CONNECTION WITH ANY CLAIM ARISING OUT OF ANY VIOLATION BY US OF THE PRECEDING PARAGRAPH, INCLUDING WITHOUT LIMITATION CIS’S RIGHT, AT OUR EXPENSE, TO ASSUME THE EXCLUSIVE DEFENSE AND CONTROL OF ANY MATTER SUBJECT TO THIS INDEMNIFICATION, AND IN SUCH CASE, WE AGREE TO COOPERATE WITH CIS IN ITS DEFENSE OF SUCH CLAIM. WE FURTHER AGREE THAT ALL CIS PARTIES ARE THIRD-PARTY BENEFICIARIES OF OUR UNDERTAKINGS IN THESE AGREED TERMS OF USE.

SPECIAL RULES.

THE DISTRIBUTION OF THE NSA SECURITY RECOMMENDATIONS IS SUBJECT TO THE TERMS OF THE NSA LEGAL NOTICE AND THE TERMS CONTAINED IN THE NSA SECURITY RECOMMENDATIONS THEMSELVES (HTTP://NSA2.WWW.CONXION.COM/CISCO/NOTICE.HTM).

CIS HAS CREATED AND WILL FROM TIME TO TIME CREATE, SPECIAL RULES FOR ITS MEMBERS AND FOR OTHER PERSONS AND ORGANIZATIONS WITH WHICH CIS HAS A WRITTEN CONTRACTUAL RELATIONSHIP. THOSE SPECIAL RULES WILL OVERRIDE AND SUPERSEDE THESE AGREED TERMS OF USE WITH RESPECT TO THE USERS WHO ARE COVERED BY THE SPECIAL RULES.

CIS HEREBY GRANTS EACH CIS SECURITY CONSULTING OR SOFTWARE VENDOR MEMBER AND EACH CIS ORGANIZATIONAL USER MEMBER, BUT ONLY SO LONG AS SUCH MEMBER REMAINS IN GOOD STANDING WITH CIS AND COMPLIES WITH ALL OF THE TERMS OF THESE AGREED TERMS OF USE, THE RIGHT TO DISTRIBUTE THE PRODUCTS AND RECOMMENDATIONS WITHIN SUCH MEMBER’S OWN ORGANIZATION, WHETHER BY MANUAL OR ELECTRONIC MEANS. EACH SUCH MEMBER ACKNOWLEDGES AND AGREES THAT THE FOREGOING GRANT IS SUBJECT TO THE TERMS OF SUCH MEMBER’S MEMBERSHIP ARRANGEMENT WITH CIS AND MAY, THEREFORE, BE MODIFIED OR TERMINATED BY CIS AT ANY TIME.

CHOICE OF LAW; JURISDICTION; VENUE

WE ACKNOWLEDGE AND AGREE THAT THESE AGREED TERMS OF USE WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF MARYLAND, THAT ANY ACTION AT LAW OR IN EQUITY ARISING OUT OF OR RELATING TO THESE AGREED TERMS OF USE SHALL BE FILED ONLY IN THE COURTS LOCATED IN THE STATE OF MARYLAND, THAT WE HEREBY CONSENT AND SUBMIT TO THE PERSONAL JURISDICTION OF SUCH COURTS FOR THE PURPOSES OF LITIGATING ANY SUCH ACTION. IF ANY OF THESE AGREED TERMS OF USE SHALL BE DETERMINED TO BE UNLAWFUL, VOID, OR FOR ANY REASON UNENFORCEABLE, THEN SUCH TERMS SHALL BE DEEMED SEVERABLE AND SHALL NOT AFFECT THE VALIDITY AND ENFORCEABILITY OF ANY REMAINING PROVISIONS.

Table of Contents

1. Introduction 6

Description 6

2. Rules 7

2.1. Rule: *Start from a fresh installation of Mac OS X* 7

2.2. Rule: *Check for software updates regularly* 7

2.3. Rule: *Enable network time synchronization* 7

2.4. Group: *Configure locking screen saver* 8

2.4.1. Rule: *Require a password to unlock the screen saver* 8

2.4.2. Rule: *Set the screen saver to appear after a period of inactivity* 8

2.5. Rule: *Disable automatic login* 8

2.6. Rule: *Disable root login* 8

2.7. Rule: *Normal use should be as a regular user, not an administrator* 9

2.8. Rule: *Display login banner* 9

2.9. Rule: *Leave unused services disabled* 9

2.10. Rule: *Enable firewall* 10

2.11. Rule: *Enable logging* 10

2.12. Rule: *Configure sshd* 10

2.13. Rule: *Use good passwords* 10

2.14. Rule: *Find world-writable files* 11

2.15. Group: *Encrypt home directory and swap files* 11

2.15.1. Rule: *Configure FileVault* 11

2.15.2. Rule: *Configure secure virtual memory* 12

2.16. Rule: *Disable Bluetooth* 12

3. Profiles 13

3.1. Profile: *Desktop system settings* 13

3.2. Profile: *Notebook system settings* 13

4. Appendices 14

5. References 15

1. Introduction

This benchmark provides recommendations on security settings for Mac OS X Tiger. The recommendations are aimed at general purpose Mac OS X systems used primarily by a single person in an ordinary office environment. Notebook computers used by travelling users are also covered. Neither servers nor other special-purpose systems are addressed.

An important goal of the recommendations is to maintain the unique functionality and ease-of-use of the Macintosh system by using the security features built in to the system by Apple. The security settings are prudent rather than paranoid, and are intended to be applicable to nearly all Mac OS X systems.

Note that the default security settings of Mac OS X are quite good. Millions of people use the default installation of Mac OS X on their home computers, and safely connect to the Internet.

The benchmark recommends additional settings which further improve system security over the defaults.

Description

This document is a CIS Level I benchmark for Mac OS X 10.4 Tiger. A Level I benchmark is the prudent level of minimum due care with respect to system security.

2. Rules

2.1. Rule: *Start from a fresh installation of Mac OS X*

In order to start from a known state and have confidence in the integrity of the system software, it is best to begin configuration from a fresh installation of the operating system.

Under ideal circumstances, the computer will remain physically disconnected from the network until it has been fully configured and patched. In this case, software updates from Apple must be downloaded to a separate system, checked for authenticity via their SHA-1 hashes, and written to removable media. The removable media can then be used to update the newly installed system. (Use `openssl sha1 file-name` to compute the SHA-1 hash of a file.)

If, however, disconnected installation is not feasible, the risk of attaching the system to the network and downloading the updates via the Software Update preference pane is relatively small.

When installing the system from the distribution, the defaults are acceptable. If, however, there are printer drivers, languages, or fonts that you will not be using, you may deselect them.

During the installation process, you will be prompted to create a user name and password for an initial account. This account will be an administrator. Pick a name for the account, and select a good password for it. Regular user accounts will be created later.

If you are unable to start from a fresh installation, the benchmark settings will still be useful, but it is possible that the system may have been altered in some not easily detectable way that might leave it vulnerable to unauthorized access or use.

2.2. Rule: *Check for software updates regularly*

Software sometimes contains defects that may make a system subject to unauthorized access. Apple provides software updates to correct these defects.

Ideally, software updates should first be tested on a laboratory system before applying them to systems used for real work. However, it is often not easy or possible to find time or resources to do this. Therefore, it is generally worthwhile to go ahead and apply the software updates from Apple, accepting the small risk that the update might cause a problem with the system.

The alternative of simply not applying the update, thereby leaving known software defects in place, is probably a greater risk on a general purpose system.

Remediation

In the Software Update preference pane, check the "Check for updates" box, and select "Weekly" or "Daily" from the pop-up menu.

2.3. Rule: *Enable network time synchronization*

Accurate time is an important security tool. It enables log file timestamps to be correlated across systems. Certain network authentication protocols, such as Kerberos (which is a component of both Apple's Open Directory and Microsoft's Active Directory), also rely on accurate time.

Remediation

In the Date & Time preference pane, check the "Set date & time automatically" box. If you have a local time server, enter it in the text field. Otherwise, select a geographically appropriate Apple time server.

2.4. Group: *Configure locking screen saver*

A locking screen saver can prevent unauthorized access by casual passers-by. The locking screen saver is like the lock on a car door: it deters casual mischief and attacks of opportunity. This action must be done for every user on the system.

2.4.1. Rule: *Require a password to unlock the screen saver*

Remediation

In the Security preference pane, check the "Require password to wake this computer from sleep or screen saver" checkbox. This action must be done for every user on the system.

2.4.2. Rule: *Set the screen saver to appear after a period of inactivity*

Remediation

In the Desktop & Screen Saver preference pane, set the screen saver to start after 15 minutes (or some other interval determined by local policy) of inactivity. Also set a hot corner so that the screen saver can be activated on demand. This action must be done for every user on the system.

2.5. Rule: *Disable automatic login*

To make the use of the computer easier for consumer users, the default installation of Mac OS X automatically logs the user into the system upon reboot.

Disable this feature so that unauthorized access to the computer cannot be gained simply by power-cycling the computer.

Remediation

In the Security preference pane, check the "Disable automatic login" checkbox.

2.6. Rule: *Disable root login*

By default on a clean OS X installation, the root account is disabled and has a blank password. It is recommended that the root account be left disabled.

Remediation

If you wish to further secure the root account by preventing other local administrators from enabling it, you can follow these steps to protect it with a non-trivial password:

1. Open "NetInfo Manager", found in the "Utilities" folder,
2. Select "Security --> Authenticate" (or click the lock icon) to authenticate as a local administator,
3. Select "Security --> Enable Root User" and set a non-trivial password for the root account,
4. Select "Security --> Disable Root User" to disable the root account.

2.7. Rule: *Normal use should be as a regular user, not an administrator*

It is generally preferable to use a non-administrator account for day-to-day work. The system will typically prompt for an administrator user name and password when additional privilege is required to perform a particular operation, so it's rarely necessary to to log in as an administrator. Should trickery or software defects result in the execution of some sort of malware, damage will be limited only to areas over which the normal user account has control. If the logged in account were an administrator, the malware could write to files in `/Applications/` and other locations that are writable by the `admin` group. It may also be easier to obtain root privileges from an administrator account.

Remediation

In the Accounts preference pane, create an additional account, and be sure that the "Allow user to administer this computer" is cleared. Do not enter a password hint. Log in using this account, and use the administrator account name and password only as required.

This is also a good time to verify that there are no extraneous accounts present, especially if the system being configured was not loaded with a fresh installation of Mac OS X.

2.8. Rule: *Display login banner*

Many organizations require that a message be displayed to users before they log in. The login window can display such a banner.

Remediation

To make the login window display a pre-login message, run the following command as an administrator user (all on one line):

```
sudo defaults write /Library/Preferences/com.apple.loginwindow
LoginwindowText 'your banner text here'
```

2.9. Rule: *Leave unused services disabled*

Services are managed from the Sharing preference panel. By default, all services on Mac OS X are off. Enable only the services necessary.

If possible, enable a service only for the duration of its use. Disable the service when done using it.

The remote login service, which turns on `sshd`, is a commonly enabled and useful service.

The FTP service should probably never be used, since it transmits passwords over the network in clear text.

The services in the Sharing preference panel all relate to sharing information on the local computer with remote users. You do not need to enable any of the services in order to access files stored on remote systems. For example, it is not necessary to enable Windows file sharing to access files stored on a Windows server.

Remediation

In the Sharing preference pane, click on the "Services" tab and ensure that unused services are turned off. If there is any doubt, leave all services disabled (unchecked).

2.10. Rule: *Enable firewall*

The built-in firewall is managed from the Firewall tab of the Sharing preference panel.

By default, the firewall blocks all inbound TCP traffic not initiated from the system. It does not block outbound traffic, nor does it block any UDP traffic. When services are enabled from the Sharing preference panel, rules are added to the firewall to allow access to those services.

Remediation

In the Sharing preference pane, click on the "Firewall" tab and click the "Start" button to enable the firewall.

2.11. Rule: *Enable logging*

If your organization has a central log host, direct log messages to it. If not central log host exists, local log files can be found in `/var/log` by default. These logs can server as a valuable resource in tracking possible security issues, so be sure to review them as often as possible.

Remediation

Add the following line to `/etc/syslog.conf` (where `your.log.host` is the name of your central log server).

```
*       @your.log.host
```

2.12. Rule: *Configure sshd*

If the Remote Login service will be enabled, some additional configuration of `sshd` is recommended.

Remediation

Edit `/etc/sshd_config` and make the following modifications:

- Edit the "`#Protocol 2,1`" line to read "`Protocol 2`". Version 1 of the SSH protocol contains flaws that are not present in protocol version 2.
- Ensure that PermitRootLogin is set to "NO".
- It is assumed that all local user accounts will have SSH access. If this isn't desired, or if the system will be used in a directory service environment, add a line "`AllowUsers user1 user2 user3`" to limit login access to the listed users. Otherwise, anyone with an account in the directory will be able to log in to the system.
- To make `sshd` display a pre-login message, first create a file called (for example) `/etc/banner`, and put the desired message text in it.

Then, edit the "`#Banner /some/path`" line to read "`Banner /etc/banner`".

2.13. Rule: *Use good passwords*

Use a good password on your account. Apple provides a tool called the password assistant to help with selecting a good password.

This account password is very important: it should be used only for your Mac OS X account. Don't use it

for a web site password, or for any other purpose. Never type the password in on a computer that you do not control (e.g., from a kiosk or a computer in an internet cafe).

Remediation

Open the Accounts preference panel and click on the password tab. Click the "Change Password..." button, and click on the small picture of the key to the right of the "New Password" field to bring up the password assistant. You can have the assistant suggest a password for you, or come up with one yourself. A 12-character "memorable" password (as generated by the Password Assistant) is typically pretty easy to remember, and strong as well. Following your organization's password complexity rules will help you formulate a good password.

When the password quality bar turns green, your password is good.

The "pwpolicy" command can be used to enfore the use of good passwords and is installed by default. See the associated man page for additional information.

2.14. Rule: *Find world-writable files*

Software installers are generally bad about leaving files and directories world-writable. Use the command

```
find /Applications /Library \( -type d -or -type f \) -perm +0002 -print
```

to get a list of world-writable directories and files in the usual suspect locations.

One quick way to remove world-writable permissions from all of these files is to run this command:

```
find /Applications /Library \( -type d -or -type f \) -perm +0002 -print
-exec chmod o-w {} \;
```

2.15. Group: *Encrypt home directory and swap files*

Encrypting swap files and user home directories will maintain the confidentiality of the data stored on the computer, even if the computer is lost or stolen. Note that OS X supports the creation of encrypted disk images to protect specific data. This is a valid option to using FileVault on the entire home directory.

2.15.1. Rule: *Configure FileVault*

FileVault transparently encrypts users' home directories. It must be enabled on a per-user basis.

For more information about FileVault, see Apple's documentation.

Warning! If the user forgets his login password, and also loses the master password, his data will be unrecoverable. If the FileVault passwords cannot be reliably managed, the risk of data loss probably outweighs the security benefits, and FileVault should not be enabled.

Remediation

Open the Security preference panel. To enable FileVault, first set a master password by clicking on the "Set Master Password..." button. The password assistant (click on the "?" button to the right of the Master Password text field) can help with selecting a strong password. Don't enter a password hint. Write down the

master password, seal it in an envelope, and store it in a safe or some other secure location. Now turn on FileVault by pressing the "Turn On FileVault" button.

Your organization may have a policy for managing the master password. If so, follow it by giving the master password to the appropriate organizational representative.

2.15.2. Rule: *Configure secure virtual memory*

Enabling secure virtual memory causes the swap files on the disk to be encrypted. It is possible for an attacker to look through the swap files on a stolen disk in search of passwords or other sensitive data; encrypting the swap files prevents this.

Remediation

Open the Security preference pane and click the "Use secure virtual memory" checkbox. The system must be rebooted in order for this setting to take effect.

2.16. Rule: *Disable Bluetooth*

Ensure that Bluetooth is disabled on all systems unless absolutely needed.

Remediation

Open the System Preferences pane, then Bluetooth. Click the Settings tab (if needed), then click the "Turn Bluetooth Off" button.

3. Profiles

3.1. Profile: *Desktop system settings*

Description

Use these settings for desktop Mac OS X systems.

Item Selections

Rules and Groups explicitly selected and deselected for this profile.

- Included: Start from a fresh installation of Mac OS X
- Included: Check for software updates regularly
- Included: Enable network time synchronization
- Included: Configure locking screen saver
- Included: Disable automatic login
- Included: Normal use should be as a regular user, not an administrator
- Included: Display login banner
- Included: Leave unused services disabled
- Included: Enable logging
- Included: Configure sshd
- Included: Use good passwords
- Included: Find world-writable files
- Included: Disable Bluetooth
- Included: Disable root login

3.2. Profile: *Notebook system settings*

Extends: Desktop system settings

Description

Use these additional settings on portable Mac OS X systems. These settings could also be applied to desktop systems at administrator discretion.

Item Selections

Rules and Groups explicitly selected and deselected for this profile.

- Included: Enable firewall
- Included: Encrypt home directory and swap files
- Included: Disable Bluetooth

4. Appendices

Appendix A: NIST 800-53 Mappings

This section contains references to the NIST 800-53 specification. It is intended for those who are required or desiring to map each recommendation in the benchmark to the associated 800-53 control.

Benchmark Item	NIST SP 800-53 Control
2.2	SI-2
2.3	AU-8
2.4	AC-11
2.5	IA-2
2.6	IA-2
2.7	AC-6
2.8	AC-8
2.9	AC-17, CM-7
2.10	AC-4
2.11	AU-2
2.12	AC-8, AC-17
2.13	IA-2
2.14	AC-3
2.15.2	SC-4

5. References

1. Apple product security web site. [link]
2. Apple security updates. [link]
3. Apple Mac OS X Common Criteria guide and tools (includes auditing tools). [link]
4. NIST Special Publication 800-53. [link]
5. NIST Special Publication 800-63, version 1.0.2. [link]