Draft NIST Special Publication 800-179

Guide to Securing Apple OS X 10.10 Systems for IT Professionals:

A NIST Security Configuration Checklist

Mark Lee Badger
Murugiah Souppaya
Mark Trapnell
Eric Trapnell
Dylan Yaga
Karen Scarfone

C O M P U T E R S E C U R I T Y

National Institute of Standards and Technology
U.S. Department of Commerce

Draft NIST Special Publication 800-179

Guide to Securing Apple OS X 10.10 Systems for IT Professionals:

A NIST Security Configuration Checklist

Mark Lee Badger
Murugiah Souppaya
Mark Trapnell
Dylan Yaga
Computer Security Division
Information Technology Laboratory

Eric Trapnell
Software and Systems Division
Information Technology Laboratory

Karen Scarfone
Scarfone Cybersecurity
Clifton, VA

June 2016

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3541 *et seq.*, Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-179
Natl. Inst. Stand. Technol. Spec. Publ. 800-179, 126 pages (June 2016)
CODEN: NSPUE2

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at http://csrc.nist.gov/publications.

Public comment period: June 23 through August 15, 2016

All comments are subject to release under the Freedom of Information Act (FOIA).

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930), Gaithersburg, MD 20899-8930
Email: 800-179comments@nist.gov

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Abstract

This publication assists IT professionals in securing Apple OS X 10.10 desktop and laptop systems within various environments. It provides detailed information about the security features of OS X 10.10 and security configuration guidelines. The publication recommends and explains tested, secure settings with the objective of simplifying the administrative burden of improving the security of OS X 10.10 systems in three types of environments: Standalone, Managed, and Specialized Security-Limited Functionality.

Keywords

Apple OS X; checklist; endpoint device security; hardening guide; host security; mobile device security; operating system security; secure configuration;

Acknowledgments

The authors wish to thank their colleagues who reviewed drafts of this document and contributed to its technical content.

Trademark Information

All registered trademarks or trademarks belong to their respective organizations.

Table of Contents

Executive Summary ..... **x**

1. Introduction **1**

1.1 Purpose and Scope 1
1.2 Audience 1
1.3 Document Structure 1

2. OS X Security Guide Development **3**

2.1 OS X System Roles and Requirements 3
2.2 Security Categorization of Information and Information Systems 4
2.3 Threats to OS X Technologies 6
2.3.1 Local Threats 6
2.3.2 Remote Threats 9
2.4 OS X Environments 13
2.4.1 Standalone 13
2.4.2 Managed 14
2.4.3 Specialized Security-Limited Functionality (SSLF) 15
2.5 Security Controls Documentation 15
2.6 Implementation and Testing of Security Controls 16
2.7 Monitoring and Maintenance 17
2.8 Summary of Recommendations 17

3. OS X Security Components Overview **19**

3.1 Gatekeeper 19
3.2 Software Updates 19
3.3 Privacy Settings 19
3.4 Credential Management 20
3.5 Host-Based Firewalls 20
3.6 Storage Encryption 20
3.7 Code Execution Protection 21
3.8 Encrypted Virtual Memory 22
3.9 Application Whitelisting 22

4. Installation, Backup, and Patching **23**

4.1 Performing an Installation 23
4.1.1 Media Sanitization 23
4.1.2 Old Patches 23
4.1.3 OS Installation and Upgrades 24
4.1.4 Migration Assistant 26
4.2 Backing Up 27
4.3 Installing Updates 29
4.3.1 Mac App Store 29
4.3.2 Manual Package Updates 30
4.4 Summary of Recommendations 30

5. Overview of OS X Managed Security Configuration **32**

5.1 Directory Services ... 32
5.2 Profile Manager ... 32
5.3 Application Installation and Configuration ... 33
5.4 Security Content Automation Protocol (SCAP) ... 34

6. NIST OS X Security Configuration ... 35

6.1 System Hardware and Firmware ... 35
6.1.1 Restricting Access to Firmware ... 36
6.1.2 Disabling Hardware Components ... 36
6.2 Filesystem Security ... 37
6.2.1 General ... 37
6.2.2 Storage Encryption ... 38
6.2.3 Secure Erase ... 40
6.2.4 File and Folder Permissions ... 41
6.2.5 Spotlight ... 41
6.3 User Accounts and Groups ... 41
6.3.1 User Account Types ... 41
6.3.2 Login Options ... 43
6.3.3 Parental Controls ... 45
6.3.4 Password Policies ... 45
6.3.5 Session Locking ... 46
6.3.6 Credential Storage ... 47
6.3.7 Alternate Credentials ... 48
6.3.8 Sudo ... 48
6.4 Auditing ... 48
6.4.1 Audit Policies and Tools ... 49
6.4.2 Date and Time Setting ... 49
6.4.3 System Crash and Panic Reporting ... 50
6.5 Software Restriction ... 51
6.5.1 Gatekeeper ... 51
6.5.2 Parental Controls ... 52
6.6 Network Services ... 52
6.6.1 Firewalls ... 53
6.6.2 Sharing ... 54
6.6.3 IPv6 ... 56
6.6.4 SSH Daemon ... 56
6.6.5 Wireless Networking ... 56
6.6.6 Bonjour ... 57
6.6.7 DNS Servers ... 57
6.7 Applications ... 57
6.7.1 Mail ... 58
6.7.2 Safari ... 58
6.7.3 Configuring Software Updates ... 59
6.8 Other Security Management Options ... 60
6.8.1 CD and DVD Preferences ... 60
6.8.2 Login Banners ... 60
6.8.3 Privacy ... 60

6.8.4 Virtualization 61
6.8.5 Other System Preferences 61
6.9 Summary of Recommendations 63

7. Putting It All Together 65

List of Appendices

Appendix A. NIST Security Configurations 66
Appendix B. Mapping OS X Controls to NIST SP 800-53 Rev 4 68
Appendix C. Tools 85
Appendix D. Resources 87
Appendix E. Acronyms and Abbreviations 89
Appendix F. Terminal Command Variables 91
Appendix G. Special Files 92
Appendix H. Process Restarting 93
Appendix I. File Attributes 95
I.1. Permissions and Ownership 95
I.2. Access Control Lists 97
Appendix J. Terminal Configuration Commands 99
J.1. Disabling Hardware Components 99
J.2. Accessibility Settings 100
J.3. Finder Preferences 100
J.4. User Account Types 101
J.5. Login Window 102
J.6. Password Policy 103
J.7. Session Locking 106
J.8. Firewalls 107
J.9. Sharing Services 108
J.10. SSH Daemon 108
J.11. Wireless Networking 109
J.12. Network Services 110
J.13. Software Updates 111
J.14. CD and DVD Preferences 111
J.15. Privacy 112
J.16. Power Management 112
J.17. Miscellaneous Settings 113

List of Figures

Figure 1: System Image Utility 25
Figure 2: Time Machine System Backup 27
Figure 3: Time Machine Select Disk Menu 28
Figure 4: Software Update Options 30
Figure 5: Advanced Finder Preferences 37
Figure 6: FileVault 2 Settings 39
Figure 7: Login Options Pane 43
Figure 8: Setting the NTP Servers 50
Figure 9: Gatekeeper Options 52
Figure 10: Sharing Options 55
Figure 11: Privacy Options 59
Figure 12: Administrator Access for Systemwide Preferences 62
Figure 13: Distribution of Security Controls 67

List of Tables

Table 1: `audit_control` Flags 49
Table 2: `pf` Firewall Services and Ports 53
Table 3: Access Control (AC) Family Controls 68
Table 4: Awareness and Training (AT) Family Controls 71
Table 5: Audit and Accountability (AU) Family Controls 71
Table 6: Security Assessment and Authorization (CA) Family Controls 72
Table 7: Configuration Management (CM) Family Controls 72
Table 8: Contingency Planning (CP) Family Controls 75
Table 9: Identification and Authentication (IA) Family Controls 75
Table 10: Incident Response (IR) Family Controls 77
Table 11: Maintenance (MA) Family Controls 78
Table 12: Media Protection (MP) Family Controls 78
Table 13: Physical and Environmental Protection (PE) Family Controls 78
Table 14: Planning (PL) Family Controls 79
Table 15: Personnel Security (PS) Family Controls 79
Table 16: Risk Assessment (RA) Family Controls 79
Table 17: System and Services Acquisition (SA) Family Controls 80

Table 18: System and Communications Protection (SC) Family Controls 80
Table 19: System and Information Integrity (SI) Family Controls 81
Table 20: File Permissions 82
Table 21: `pf` Firewall Rules 83
Table 22: Built-in Commands Used to Write OS X Configuration Data 85
Table 23: OS X Security Resources 87
Table 24: Terminal Command Variable Descriptions 91
Table 25: Files Requiring Manual Editing 92
Table 26: Settings Requiring Process Restart 93
Table 27: Recommended File Permissions and Ownership 95
Table 28: Disabling Hardware Components 99
Table 29: Accessibility Settings 100
Table 30: Finder Preferences 100
Table 31: User Account Settings 101
Table 32: Login Window GUI Settings 102
Table 33: Login Window Terminal Settings 102
Table 34: Password Policy Settings 104
Table 35: Session Locking Settings 106
Table 36: Application Firewall Settings 107
Table 37: pf Firewall Settings 107
Table 38: Sharing Settings 108
Table 39: SSH Settings 108
Table 40: Wireless Networking Settings 109
Table 41: Network Services Settings 110
Table 42: Software Update Settings 111
Table 43: CD and DVD Settings 111
Table 44: Privacy Settings 112
Table 45: Power Management Settings 112
Table 46: Miscellaneous Settings 113

Executive Summary

When an IT security configuration checklist (e.g., hardening or lockdown guide) is applied to a system in combination with trained system administrators and a sound and effective security program (which includes a robust patch management program), a substantial reduction in vulnerability exposure can be achieved. Accordingly, the National Institute of Standards and Technology (NIST) has produced the *Guide to Securing Apple OS X 10.10 Systems for IT Professionals: A NIST Security Configuration Checklist* to assist personnel responsible for the administration and security of OS X 10.10[1] systems. This guide contains information that can be used by system administrators to secure local OS X 10.10 desktops and laptops more effectively in a variety of environments, including Standalone and Managed environments. The guidance should only be applied throughout an enterprise by trained and experienced system administrators.

The guidance presented in this document is applicable only to OS X 10.10 systems. The recommendations in this guide should not be applied to systems running anything other than OS X 10.10.

This guide provides detailed information about the security of OS X 10.10 and security configuration guidelines for the OS X 10.10 operating system. The guide documents the methods that system administrators can use to implement each security setting recommended. The principal goal of the document is to recommend and explain tested, secure settings for OS X 10.10 systems with the objective of simplifying the administrative burden of improving the security of OS X 10.10 systems in three types of environments: Standalone, Managed, and one custom environment, Specialized Security-Limited Functionality as defined in NIST SP 800-70 Revision 3, *National Checklist Program for IT Products – Guidelines for Checklist Users and Developers*. [2]

- **Standalone**. Standalone, sometimes called Small Office/Home Office (SOHO), describes small, informal computer installations that are used for home or business purposes. Standalone encompasses a variety of small-scale environments and devices, ranging from laptops, mobile devices, and home computers, to telecommuting systems located on broadband networks, to small businesses and small branch offices of a company. Historically, Standalone environments are the least secured and most trusting. Generally, the individuals performing Standalone system administration are not knowledgeable about security. This can result in environments that are less secure than they need to be because the focus is generally on functionality and ease of use.

- **Managed.** Managed environments, sometimes referred to as Enterprise environments, have systems that share a common hardware and software configuration, and are centrally deployed and managed and are protected from threats on the Internet by using firewalls and other network security devices. Managed environments generally have a group dedicated to supporting users and providing security. The combination of structure

[1] Starting with version 10.8, Apple dropped the "Mac" portion of the name from Mac OS X.
[2] http://dx.doi.org/10.6028/NIST.SP.800-70r3.

and skilled staff allows better security practices to be implemented during initial system deployment and in ongoing support and maintenance, and for a consistent security posture to be maintained across the enterprise. Generally, Managed environments are more restrictive than Standalone environments.

- **Specialized Security-Limited Functionality (SSLF).** An SSLF environment is a likely target for attack or data exposure, and therefore security takes precedence over usability. This environment encompasses computers that are usually limited in their functionality to specific specialized purposes. They may contain highly confidential information (e.g., personnel records, medical records, financial information) or perform vital organizational functions (e.g., accounting, payroll processing). Typically, providing sufficiently strong protection for these systems involves a tradeoff between security and functionality based on the premise that any more functionality than is strictly necessary provides more opportunity for exploitation. This environment is characterized by a significant reduction in system functionality and a higher risk of applications breaking, resulting in an increased support cost. An SSLF environment could be a subset of another environment. While some Standalone users understandably might want to choose this environment due to concern for being as secure as possible, this environment is usually not advised for most Standalone users administering their own systems due to the significant tradeoffs and administrative complexity. In most cases, the SSLF environment is also not suitable for widespread enterprise usage.

By implementing the recommendations described throughout this publication, organizations should be able to meet the baseline requirements for OS X 10.10 systems. This is based upon the management, operational, and technical security controls described in NIST Special Publication (SP) 800-53 Revision 4, *Recommended Security Controls for Federal Information Systems and Organizations*.[3]

Although the guidance presented in this document has undergone considerable testing, every system and environment is unique, so system administrators should perform their own testing. The development of the NIST security baselines was driven by the need to create more secure OS X 10.10 system configurations. These NIST security baselines provide guidance on how to define specific configurations with varying levels of security and make certain tradeoffs depending on the target environment. Because some settings in the baselines may reduce the functionality or usability of the system, caution should be used when applying the security baselines. Specific settings in the baselines should be modified as needed (with due consideration of the security implications, including the possible need for compensating controls) so that the settings conform to local policies and support required system functionality. NIST strongly recommends that organizations fully test the baselines on representative systems before widespread deployment. Some settings may inadvertently interfere with applications, particularly legacy applications that may require a less restrictive security profile.

The security configuration guidance provided in this document was tested on clean OS X 10.10 installations. NIST recommends that system administrators build their systems from a clean

[3] http://dx.doi.org/10.6028/NIST.SP.800-53r4

formatted state to begin the process of securing OS X 10.10 systems. NIST also recommends that the installation process be performed on a secure network segment or off the organization's network until the security configuration is completed, all patches are applied, and strong passwords are set for all accounts.

After the OS X 10.10 operating system has been installed and securely configured, it should be regularly monitored and patched when necessary to mitigate software vulnerabilities. Once Apple releases an update, it should be tested thoroughly and applied to all systems within an organization as soon as possible. Updates to third-party applications should receive similar treatment.

This guidance document also includes recommendations for configuring selected applications built into OS X 10.10, such as web browsers and email clients. This list is not intended to be a complete list of applications for OS X 10.10, nor does it imply NIST's endorsement of particular products. Many of the configuration recommendations for the applications focus on preventing damage from malware, either to the applications themselves or to the OS X 10.10 system, while the applications are being used.

This document provides recommendations to assist organizations in making their OS X 10.10 systems more secure. The settings and recommendations provide system administrators with the information necessary to modify the settings and to comply with local policy or special situations. The baseline recommendations and settings provide a high level of security for OS X 10.10 systems when used in conjunction with a sound and comprehensive local security policy and other relevant security controls. The guidelines are also appropriate for organizational environments that are configuring and deploying laptops for mobile users and desktop computers for telecommuters.

1. Introduction

1.1 Purpose and Scope

This publication is designed to assist IT professionals in securing OS X 10.10 desktops and laptops (systems). Only trained and competent system administrators should apply these guidelines. Other versions of OS X are outside the scope of this publication.

The guide provides detailed information about the security features of OS X 10.10 and security configuration guidelines for the OS X 10.10 operating system. The guide documents the methods that IT professionals can use to implement each security setting recommended. The principal goal of the document is to recommend and explain tested, secure settings for OS X 10.10 desktops and laptops with the objective of simplifying the administrative burden of improving their security in three types of environments: Standalone, Managed, and Specialized Security-Limited Functionality (SSLF). The proposed controls are consistent with the minimum security controls for an IT system as represented in the NIST SP 800-53 publication.

1.2 Audience

This document has been created for IT professionals, particularly system administrators and information security personnel (security managers, engineers, administrators, etc.) who are responsible for securing or maintaining the security of OS X 10.10 systems. Auditors and others who need to assess the security of systems may also find this publication useful. The document assumes that the reader has experience installing and administering OS X-based systems.[4] The document discusses in technical detail various OS X 10.10 security settings.

1.3 Document Structure

The remainder of this document is organized into the following sections and appendices:

- Section 2 provides insight into the threats and security controls that are relevant for various environments, such as a large enterprise or a home office, and describes the need to document, implement, and test controls, as well as monitor and maintain systems on an ongoing basis.
- Section 3 presents an overview of the security components offered by OS X 10.10.
- Section 4 provides guidelines for installing, backing up, and patching OS X 10.10 systems.
- Section 5 discusses security policy configuration and how security baselines can best be used.
- Section 6 provides an overview of the settings in the NIST security baselines and

[4] For an overview of information security terms, see NISTIR 7298 Revision 2: http://dx.doi.org/10.6028/NIST.IR.7298r2

explains how the settings can provide better security for systems.

- Section 7 provides guidelines for IT professionals on how to use the guide effectively to secure OS X 10.10 systems.
- Appendix A discusses the components of the NIST security baselines.
- Appendix B maps the guide's security controls and baseline settings to the controls in NIST Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.
- Appendix C lists built-in tools used to create the security configuration for OS X 10.10 systems.
- Appendix D lists resources that may be useful OS X 10.10 security references.
- Appendix E lists acronyms and abbreviations used in this document.
- Appendix F gives a description of variables used in many Terminal commands in this document.
- Appendix G lists files that require manual editing.
- Appendix H lists processes that must be restarted in order to successfully apply settings.
- Appendix I lists file ownership, permissions, and access control list (ACL) recommendations.
- Appendix J describes all of the Terminal commands needed for system configuration.

IT professionals should read the entire publication, including the appendices, before using the security baselines or implementing any of the other recommendations or suggestions in the guide. Readers with limited OS X 10.10 administration and security experience are cautioned not to apply the baselines or other recommendations to systems on their own. As described in Section 7, effective use of this publication involves extensive planning and testing.

2. OS X Security Guide Development

In today's computing environment, the security of all computing resources, from network infrastructure devices to users' desktop and laptop computers, is essential. There are many threats to users' computers, ranging from remotely launched network service exploits to malware spread through emails, websites, and file downloads. Increasing the security of individual computers protects them from these threats and reduces the likelihood that a system will be compromised or that data will be disclosed to unauthorized parties. Effective and well-tested security configurations mean that less time and money is spent eradicating malware, restoring systems from backups, and reinstalling operating systems and applications. In addition, having stronger host security increases network security (e.g., home, business, government, the Internet); for example, most distributed denial of service attacks against networks use large numbers of compromised hosts.

The goal of this guide is to provide security configuration guidelines to the users and system administrators of OS X 10.10 systems. This advice can be adapted to any environment, from individual Standalone installations to large geographically diverse organizations. This guide draws on a large body of vendor knowledge and government and security community experience gained over many years of securing computer systems.

This section of the guide is based largely on the steps proposed in NIST's FISMA Implementation Project for achieving more secure information systems.[5] Sections 2.1 and 2.2 address the need to categorize information and information systems. Each OS X 10.10 system can be classified as having one of three roles; each system can also be classified according to the potential impact caused by security breaches. Section 2.3 describes threats and provides examples of security controls that can mitigate threats. Section 2.4 outlines the primary types of environments for information systems—Standalone, Managed, and Specialized Security-Limited Functionality—and ties each environment to typical threat categories and security controls. Section 2.5 briefly describes the security-related documentation that affects configuration and usage of systems and applications. Section 2.6 provides a brief overview of the implementation of the security controls and the importance of performing functionality and security testing. Finally, Section 2.7 discusses the need to monitor the security controls and maintain the system.

2.1 OS X System Roles and Requirements

OS X security should take into account the role that the system plays. In the past, OS X systems were divided into three roles: inward-facing, outward-facing, and mobile. An inward-facing OS X system is typically a user workstation on the interior of a network that is not directly accessible from the Internet. An outward-facing OS X system is one that is directly connected to the Internet. A system with a mobile role typically moves between a variety of environments and physical locations. Over time, the mobile role has become the predominant role for most OS X systems. Therefore, this publication assumes the mobile role.

With the mobile role, for network connectivity the system might use both traditional wired

[5] More information on the project is available at http://csrc.nist.gov/groups/SMA/fisma/index.html.

methods (e.g., Ethernet) and wireless methods (e.g., IEEE 802.11). The mobility of the system makes it more difficult to manage centrally. It also exposes the system to a wider variety of threat environments; for example, in a single day the system might be in a home environment, an office environment, a wireless network hotspot, and a hotel room. An additional threat is the loss or theft of the system. This could lead to loss of productivity at a minimum, but could also include the disclosure of confidential information or the possible opening of a backdoor into the organization if remote access is not properly secured.

Most OS X systems today are used for the same combination of tasks: accessing websites, reading email, performing instant messaging, using social networks, and conducting other tasks with both work-related and personal contexts. This range of activity, as well as the frequent lack of perimeter defenses, exposes OS X systems to a wider variety of threats than they were exposed to in the past.

2.2 Security Categorization of Information and Information Systems

The classic model for information security defines three objectives of security: maintaining confidentiality, integrity, and availability. *Confidentiality* refers to protecting information from being accessed by unauthorized parties. *Integrity* refers to ensuring the authenticity of information—that information is not altered, and that the source of the information is genuine. *Availability* means that information is accessible by authorized users. Each objective addresses a different aspect of providing protection for information.

Determining how strongly a system needs to be protected is based largely on the type of information that the system processes and stores. For example, a system containing medical records probably needs much stronger protection than a computer only used for viewing publicly released documents. This is not to imply that the second system does not need protection; every system needs to be protected, but the level of protection may vary based on the value of the system and its data. To establish a standard for determining the security category of a system, NIST created Federal Information Processing Standards (FIPS) Publication (PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*.[6] FIPS PUB 199 establishes three security categories—low, moderate, and high—based on the potential impact of a security breach involving a particular system. The FIPS PUB 199 definitions for each category are as follows:

> "The potential impact is **LOW** if the loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

[6] FIPS PUB 199 is available for download from http://csrc.nist.gov/publications/PubsFIPS.html.

> The potential impact is **MODERATE** if the loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
>
> The potential impact is **HIGH** if the loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries."

Each system should be protected based on the potential impact to the system of a loss of confidentiality, integrity, or availability. Protection measures (otherwise known as *security controls*) tend to fall into two categories. First, security weaknesses in the system need to be resolved. For example, if a system has a known vulnerability that attackers could exploit, the system should be patched so that the vulnerability is removed or mitigated. Second, the system should offer only the required functionality to each authorized user, so that no one can use functions that are not necessary. This principle is known as *least privilege*.[7] Limiting functionality and resolving security weaknesses have a common goal: give attackers as few opportunities as possible to breach a system.

Although each system should ideally be made as secure as possible, this is generally not feasible because the system needs to meet the functional requirements of the system's users. Another common problem with security controls is that they often make systems less convenient or more difficult to use. When usability is an issue, many users will attempt to circumvent security controls; for example, if passwords must be long and complex, users may write them down. Balancing security, functionality, and usability is often a challenge. This guide attempts to strike a proper balance and make recommendations that provide a reasonably secure solution while offering the functionality and usability that users require.

Another fundamental principle recommended by this guide is using multiple layers of security. For example, a host may be protected from external attack by several controls, including a network-based firewall, a host-based firewall, and OS patching. The motivation for having

[7] For more information on least privilege and other fundamental principles of computer security, see "The Protection of Information in Computer Systems" by Jerome Saltzer and Michael Schroeder (http://web.mit.edu/Saltzer/www/publications/protection/).

multiple layers is that if one layer fails or otherwise cannot counteract a certain threat, other layers might prevent the threat from successfully breaching the system. A combination of network-based and host-based controls is generally most effective at providing consistent protection for systems. Note that in many situations, such as Standalone environments, there may not be any network-based controls present, thus creating a reliance on layers of host-based controls.

NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, proposes minimum baseline management, operational, and technical security controls for information systems. These controls are to be implemented based on the security categorizations proposed by FIPS 199, as described earlier in this section. This guidance should assist agencies in meeting baseline requirements for OS X 10.10 systems deployed in their environments.

2.3 Threats to OS X Technologies

To secure a system, it is essential first to define the threats that need to be mitigated. This knowledge of threats is also key to understanding the reasons the various configuration options have been chosen in this guide. Most threats against data and resources are possible because of mistakes—either bugs in operating system and application software that create exploitable vulnerabilities, or errors made by users and administrators. Threats may involve intentional actors (e.g., an attacker who wants to access credit cards on a system) or unintentional actors (e.g., an administrator who forgets to disable user accounts of a terminated employee). Threats can be local, such as a disgruntled employee, or remote, such as an attacker in another country. The following sections describe each major threat category, list possible controls, provide examples of threats, and summarize the potential impact of the threat. The list of threats is not exhaustive; it simply represents the major threat categories that were considered during the selection of the security controls as described in this guide. Organizations should conduct risk assessments to identify the specific threats against their systems and determine the effectiveness of existing security controls in counteracting the threats, then perform risk mitigation to decide what additional measures (if any) should be implemented.[8]

2.3.1 Local Threats

Local threats require either physical access to the system or logical access to the system (e.g., an authorized user account). Local threats are grouped into three categories: boot process, unauthorized local access, and privilege escalation.

2.3.1.1 Boot Process

- **Threat**: An unauthorized individual boots a computer from third-party media (e.g., removable drives, Universal Serial Bus [USB] token storage devices). This could permit the attacker to circumvent operating system (OS) security measures and gain

[8] NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, contains guidance on performing risk assessment and mitigation. It is available for download from http://csrc.nist.gov/publications/PubsSPs.html.

unauthorized access to information.

- **Examples**:
  - While traveling, an employee misplaces a laptop, and the party that acquires it tries to see what sensitive data it contains.
  - A disgruntled employee boots a computer off third-party media to circumvent other security controls so the employee can access sensitive files (e.g., confidential data stored locally, local password file).
  - Booting from the recovery partition in OS X.
- **Impact**: Unauthorized parties could cause a loss of confidentiality, integrity, and availability.
- **Possible Controls**:
  - Implement physical security measures (e.g., locked doors, badge access) to restrict access to equipment.[9]
  - Enable a strong and difficult-to-guess password for the Extensible Firmware Interface (EFI) and configure the EFI to boot the system from the local hard drive only, assuming that the case containing the OS and data is physically secure. This will help protect the data unless the hard drive is removed from the computer.
  - Secure local files via encryption to prevent access to data in the event the physical media is placed in another computer.

2.3.1.2 Unauthorized Local Access

- **Threat**: An individual who is not permitted to access a system gains local access.
- **Examples**:
  - A visitor to a company sits down at an unattended computer and logs in by guessing a weak password for a user account.
  - A former employee gains physical access to facilities and uses old credentials to log in and gain access to company resources.
- **Impact**: Because the unauthorized person is masquerading as an authorized user, this could cause a loss of confidentiality and integrity; if the user has administrative rights, this could also cause a loss of availability.

[9] Organizations should have a physical and environmental protection policy that includes requirements for providing adequate physical security for systems and networks. Most technical controls can be easily defeated without physical security.

- **Possible Controls**:
  - Require valid username and password authentication before allowing any access to system resources, and enable a password-protected screen saver. These actions help to prevent an attacker from walking up to a computer and immediately gaining access.
  - Enable a logon banner containing a warning of the possible legal consequences of misuse.
  - Implement a password policy to enforce stronger passwords, so that it is more difficult for an attacker to guess passwords.
  - Do not use or reuse a single password across multiple accounts; for example, the password for a personal email account should not be the same as that used to gain access to the OS X system.
  - Establish and enforce a checkout policy for departing employees that includes the immediate disabling of their user accounts.
  - Physically secure removable storage devices and media, such as CDs and flash drives, that contain valuable information. An individual who gains access to a workspace may find it easier to take removable media than attempt to get user-level access on a system.

2.3.1.3 Privilege Escalation

- **Threat**: An authorized user with normal user-level rights escalates the account's privileges to gain administrator-level access.
- **Examples**:
  - A user takes advantage of a vulnerability in a service to gain administrator-level privileges and access another user's files.
  - A user guesses the password for an administrator-level account, gains full access to the system, and disables several security controls.
- **Impact**: Because the user is gaining full privileges on the system, this could cause a loss of confidentiality, integrity, and availability.
- **Possible Controls**:
  - Restrict access to all administrator-level accounts and administrative tools, configuration files, and settings. Use strong, difficult-to-guess passwords for all

administrator-level accounts.[10] These actions will make it more difficult for users to escalate their privileges.

- Disable unused local services. Vulnerabilities in these services may permit users to escalate their privileges.
- Install application and OS updates. These updates will resolve system vulnerabilities, reducing the number of attack vectors that can be used.
- Encrypt sensitive data. Even administrator-level access would not permit a user to access data in encrypted files.

2.3.2 Remote Threats

Unlike local threats, remote threats do not require physical or logical access to the system. The categories of remote threats described in this section are network services, data disclosure, and malicious payloads.

2.3.2.1 Network Services

- **Threat**: Remote attackers exploit vulnerable network services on a system. This includes gaining unauthorized access to services and data, and causing a denial of service (DoS) condition.
- **Examples**:
  - An attacker gains access to a system through a service that did not require authentication.
  - An attacker impersonates a user by taking advantage of a weak remote access protocol.
  - A worm searches for systems with an unsecured service listening on a particular port, and then uses the service to gain full control of the system.
- **Impact**: Depending on the type of network service that is being exploited, this could cause a loss of confidentiality, integrity, and availability.
- **Possible Controls**:
  - Disable unused services. This provides attackers with fewer chances to breach the system.
  - Install application and OS updates. These updates will resolve system software

[10] NIST SP 800-63, *Electronic Authentication Guideline*, contains additional information on password strength. It is available for download from http://dx.doi.org/10.6028/NIST.SP.800-63-2

vulnerabilities, reducing the number of attack vectors that can be used.

- Require strong authentication (preferably multifactor authentication) before allowing access to a service. Implement a password policy to enforce stronger passwords that are harder to guess. Establish and enforce a checkout policy for departing employees that includes the immediate disabling of their user accounts. These actions help to ensure that only authorized users can access each service.

- Do not use weak remote access protocols and applications; instead, use only accepted, industry standard strong protocols (e.g., Internet Protocol Security [IPsec], Secure Shell [SSH], Transport Layer Security [TLS]) for accessing and maintaining systems remotely.

- Use firewalls or packet filters to restrict access to each service to the authorized hosts only. This prevents unauthorized hosts from gaining access to the services and also prevents worms from propagating from one host to other hosts on the network.

- Enable logon banners containing a warning of the possible legal consequences of misuse.

2.3.2.2 Data Disclosure

- **Threat**: A third party intercepts confidential data sent over a network.

- **Examples**:

  - On a nonswitched wired network or an unsecured wireless network, a third party is running a network monitoring utility. When a legitimate user transmits a file in an insecure manner, the third party captures the file and accesses its data.

  - An attacker intercepts usernames and passwords sent in plaintext over a local network segment or a wireless network.

  - A man in the middle attack could occur on untrusted networks.

- **Impact**: The interception of data could lead to a loss of confidentiality. If authentication data (e.g., passwords) are intercepted, it could cause a loss of confidentiality and integrity, and possibly a loss of availability, if the intercepted credentials have administrator-level privileges.

- **Possible Controls**:

  - Use switched networks for wired networks, which make it more difficult to sniff

packets.[11]

- Use a secure user identification and authentication system, preferably with multifactor authentication.
- Encrypt network communications or application data through the use of various protocols (e.g., TLS, IPsec, SSH, WPA2). This protects the data from being accessed by a third party.
- Use trusted and known Domain Name System (DNS) servers.

2.3.2.3 Malicious Payloads

- **Threat**: Malicious payloads such as viruses, worms, Trojan horses, and active content attack systems through many vectors. End users of the system may accidentally trigger malicious payloads.
- **Examples**:
  - A user visits a web site and downloads a free game that includes a Trojan horse. When the user installs the game on her computer, the Trojan horse is also installed, which compromises the system.
  - A user with administrative-level privileges surfs the web and accidentally visits a malicious web site, which successfully infects the user's system.
  - A user installs and operates peer-to-peer (P2P) file sharing software to download music files, and the P2P software installs spyware programs onto the system.
  - A user opens and executes a payload that was attached to a spam or spoofed message.
  - A user connects an untrusted or unprotected USB storage device.
  - A user interacts with content hosted on a social network site.
- **Impact**: Malware often gains full administrative-level privileges to the system, or inadvertently crashes the system. Malware may cause a loss of confidentiality, integrity, and availability.
- **Possible Controls**:
  - Operate the system on a daily basis with a standard or managed user account. Only use administrator-level accounts when needed for specific maintenance tasks. Many instances of malware cannot successfully infect a system unless the current user has

[11] Switched networks cannot completely prevent packet sniffing. For example, techniques such as address resolution protocol (ARP) spoofing can be used to convince a switch to direct traffic to an attacker's machine instead of the intended destination. The attacker's machine can then forward the packets to the legitimate recipient.

administrative privileges.

- Educate users on avoiding malware infections, and make them aware of local policy regarding the use of potential transmission methods such as instant messaging (IM) software, P2P file sharing services, social network services, and unknown or untrusted applications not downloaded from the Mac App Store. Users who are familiar with the techniques for spreading malware should be less likely to infect their systems.
- Use antivirus software as an automated way of preventing most infections and detecting the infections that were not prevented.
- Use application whitelisting technology.
- Use email clients that support spam filtering—automatically detecting and quarantining messages that are known to be spam or have the same characteristics as typical spam.
- Do not install or use non-approved applications (e.g., P2P, IM) to connect to unknown servers. Educate users regarding the potential impact caused by the use of P2P, IM, social network services, and unknown, untrusted, or unsigned software applications not downloaded from the Mac App Store.
- Configure server and client software such as email servers and clients, web proxy servers and clients, and productivity applications to reduce exposure to malware. For example, email servers and clients could be configured to block email attachments with certain file types. This should help to reduce the likelihood of infections.
- Configure systems, particularly in Specialized Security-Limited Functionality environments, so that the default file associations prevent automatic execution of active content files (e.g., Java, JavaScript).

This section has described various types of local and remote threats that can negatively affect systems. The possible controls listed for the threats are primarily technical, as are the controls discussed throughout this document. However, it is important to further reduce the risks of operating an OS X system by also using management and operational controls. Examples of important operational controls are restricting physical access to a system; performing contingency planning;[12] backing up the system, storing the backups in a safe and secure location, and testing the backups regularly; and monitoring Apple mailing lists for relevant security bulletins. Management controls could include developing policies regarding OS X system security and creating a plan for maintaining OS X systems. By selecting and implementing management, operational, and technical controls for OS X, organizations can better mitigate the threats that OS X systems may face.

[12] For more information regarding contingency planning, refer to NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, available at http://csrc.nist.gov/publications/PubsSPs.html.

Another reason to use multiple types of controls is to provide better security in situations where one or more controls are circumvented or otherwise violated. This may be done not only by attackers, but also by authorized users with no malicious intent. For example, taping a list of passwords to a monitor for convenience may nullify controls designed to prevent unauthorized local access to that system. Establishing a policy against writing down passwords (management control), educating users on the dangers of password exposure (operational control), and performing periodic physical audits to identify posted passwords (operational control) may all be helpful in reducing the risks posed by writing down passwords. Technical controls may be helpful as well, such as using Personal Identity Verification (PIV) smart cards[13] or derived PIV[14] or another method other than or in addition to passwords for system authentication (preferably multifactor authentication).

2.4 OS X Environments

This section describes the types of environments in which an OS X host may be deployed—Standalone, Managed, and custom—as described in the NIST National Checklist Program. The typical custom environment for OS X is Specialized Security-Limited Functionality, which is for systems at high risk of attack or data exposure, with security taking precedence over functionality. Each environment description also summarizes the primary threats and controls that are typically part of the environment.

2.4.1 Standalone

Standalone, sometimes called Small Office/Home Office (SOHO), describes small, informal computer installations that are used for home or business purposes. Standalone encompasses a variety of small-scale environments and devices, ranging from laptops, mobile devices, and home computers, to telecommuting systems located on broadband networks, to small businesses and small branch offices of a company. Historically, Standalone environments are the least secured and most trusting. Generally, the individuals performing Standalone system administration are less knowledgeable about security. This often results in environments that are less secure than they need to be because the focus is usually on functionality and ease of use. A Standalone system might not use any security software (e.g., antivirus software, personal firewall). In some instances, there are no network-based controls such as firewalls, so Standalone systems may be directly exposed to external attacks. Therefore, Standalone environments are frequently targeted for exploitation.

Because the primary threats in Standalone environments are external, and Standalone computers generally have less restrictive security policies than Managed or Specialized Security-Limited Functionality computers, they tend to be most vulnerable to attacks from remote threat categories. (Although remote threats are the primary concern for Standalone environments, it is still important to protect against other threats.) Standalone systems are typically threatened by attacks against network services and by malicious payloads (e.g., viruses, worms). These attacks

---

[13] See *Best Practices for Privileged User PIV Authentication* available at http://csrc.nist.gov/publications/papers/2016/best-practices-privileged-user-piv-authentication.pdf

[14] See *Guidelines for Derived Personal Identity Verification (PIV) Credentials* available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-157.pdf

are most likely to affect availability (e.g., crashing the system, consuming all network bandwidth, breaking functionality) but may also affect integrity (e.g., infecting data files) and confidentiality (e.g., providing remote access to sensitive data, emailing data files to others).

Standalone security has improved with the proliferation of small, inexpensive, hardware-based firewall routers that protect to some degree the Standalone machines behind them. The adoption of personal firewalls is also helping to better secure Standalone environments. Another key to Standalone security is strengthening the hosts on the Standalone network by patching vulnerabilities and altering settings to restrict unneeded functionality.

2.4.2 Managed

The Managed environment, also known as an Enterprise environment, is typically comprised of large organizational systems with defined, organized suites of hardware and software configurations, usually consisting of centrally-managed workstations and servers protected from threats on the Internet with firewalls and other network security devices. Managed environments generally have a group dedicated to supporting users and providing security. The combination of structure and skilled staff allows better security practices to be implemented during initial system deployment and in ongoing support and maintenance. Managed installations typically use a domain model to effectively manage a variety of settings and allow the sharing of resources (e.g., file servers, printers). The enterprise can enable only the services needed for normal business operations, with other possible avenues of exploit removed or disabled. Authentication, account, and policy management can be administered centrally to maintain a consistent security posture across an organization.

The Managed environment is more restrictive and provides less functionality than the Standalone environment. Managed environments typically have better control on the flow of various types of traffic, such as filtering traffic based on protocols and ports at the enterprise's connections with external networks. Because of the supported and largely homogeneous nature of the Managed environment, it is typically easier to use more functionally-restrictive settings than it is in Standalone environments. Managed environments also tend to implement several layers of defense (e.g., firewalls, antivirus servers, intrusion detection systems, patch management systems, email filtering), which provides greater protection for systems. In many Managed environments, interoperability with legacy systems may not be a major requirement, further facilitating the use of more restrictive settings. In a Managed environment, this guide should be used by advanced users and system administrators. The Managed environment settings correspond to an enterprise security posture that will protect the information in a moderate risk environment.

In the Managed environment, systems are typically susceptible to local and remote threats. In fact, threats often encompass all the categories of threats defined in Section 2.3. Local attacks, such as unauthorized usage of another user's workstation, most often lead to a loss of confidentiality (e.g., unauthorized access to data) but may also lead to a loss of integrity (e.g., data modification) or availability (e.g., theft of a system). Remote threats may be posed not only by attackers outside the organization, but also by internal users who are attacking other internal systems across the organization's network. Most security breaches caused by remote threats involve malicious payloads sent by external parties, such as malware acquired via email or

infected websites. Threats against network services tend to affect a smaller number of systems and may be caused by internal or external parties. Both malicious payloads and network service attacks are most likely to affect availability (e.g., crashing the system, consuming all network bandwidth, breaking functionality) but may also affect integrity (e.g., infecting data files) and confidentiality (e.g., providing remote access to sensitive data). Data disclosure threats tend to come from internal parties who are monitoring traffic on local networks, and they primarily affect confidentiality.

2.4.3 Specialized Security-Limited Functionality (SSLF)

A Specialized Security-Limited Functionality (SSLF) environment is any environment that is at high risk of attack or data exposure. Systems that are often found in SSLF environments include outward-facing web, email, and DNS servers, and firewalls. Typically, providing sufficiently strong protection for these systems involves a significant reduction in system functionality. It assumes systems have limited or specialized functionality in a highly threatened environment such as an outward facing firewall or public Web server, or whose data content or mission purpose is of such value that aggressive trade-offs in favor of security outweigh the potential negative consequences to other useful system attributes such as interoperability with other systems. The SSLF environment encompasses computers that contain highly confidential information (e.g., personnel records, medical records, financial information) and perform vital organizational functions (e.g., accounting, payroll processing, air traffic control). These computers might be targeted by third parties for exploitation, but also might be targeted by trusted parties inside the organization.

An SSLF environment could be a subset of a Standalone or Managed environment. For example, three desktops in a Managed environment that hold confidential employee data could be thought of as an SSLF environment within a Managed environment. In addition, a laptop used by a mobile worker might be an SSLF environment within a Standalone environment. An SSLF environment might also be a self-contained environment outside any other environment—for instance, a government security installation dealing in sensitive data.

Systems in SSLF environments face the same threats as systems in Managed environments. Threats from both insiders and external parties are a concern. Because of the risks and possible consequences of a compromise in an SSLF environment, it usually has the most functionally restrictive and secure configuration. The suggested configuration is complex and provides the greatest protection at the expense of ease of use, functionality, and remote system management. In an SSLF environment, this guide is targeted at experienced security specialists and seasoned system administrators who understand the impact of implementing these strict requirements.

2.5 Security Controls Documentation

An organization typically has many documents related to the security of OS X systems. Foremost among the documents is an OS X security configuration guide that specifies how OS X

systems should be configured and secured.[15] As mentioned in Section 2.2, NIST SP 800-53 proposes management, operational, and technical security controls for systems, each of which should have associated documentation. In addition to documenting procedures for implementing and maintaining various controls, every environment should also have other security-related policies and documentation that affect the configuration, maintenance, and usage of systems and applications. Examples of such documents are as follows:

- Rules of behavior and acceptable use policy
- Configuration management policy, plan, and procedures
- Authorization to connect to the network
- IT contingency plans
- Security awareness and training for end users and administrators.

2.6 Implementation and Testing of Security Controls

Implementing security controls can be a daunting task. As described in Section 2.2, many security controls have a negative impact on system functionality and usability. In some cases, a security control can even have a negative impact on other security controls. For example, installing a patch could inadvertently break another patch, or enabling a firewall could inadvertently block antivirus software from automatically updating its signatures or disrupt patch management software, remote management software, and other security and maintenance-related utilities. Therefore, it is important to perform testing for all security controls to determine what impact they have on system security, functionality, and usability, and to take appropriate steps to address any significant issues.

As described in Section 5, NIST has compiled a set of security baselines, as well as additional recommendations for security-related configuration changes. The controls proposed in this guide and the NIST OS X security baselines are consistent with the FISMA controls, as discussed in Section 2.2. See Section 5 for more information on the composition and use of these baselines.

Although the guidelines presented in this document have undergone considerable testing, every system is unique, so it is possible for specific settings to cause unexpected problems. System administrators should perform their own testing, especially for the applications used by their organizations, to identify any functionality or usability problems before the guidance is deployed throughout organizations.[16] It is also important to confirm that the desired security settings have

[15] Organizations should verify that their OS X security configuration guides are consistent with this publication. Organizations without OS X security configuration guides should modify this document to create a configuration guide tailored for their environments.

[16] Any changes made to the baselines or settings should be documented, as part of the overall documentation of OS X systems' security configuration.

been implemented properly and are working as expected.

2.7 Monitoring and Maintenance

Every system needs to be monitored (ideally, continuously) and maintained on a regular basis so that security issues can be identified and mitigated promptly, reducing the likelihood of a security breach. However, no matter how carefully systems are monitored and maintained, incidents may still occur, so organizations should be prepared to respond to them.[17] Depending on the environment, some preventative actions may be partially or fully automated. Guidance on performing various monitoring and maintenance activities is provided in subsequent sections of this document or other NIST publications. Recommended actions include the following:

- Subscribing to and monitoring various vulnerability notification mailing lists
- Acquiring and installing software updates (e.g., OS and application patches, antivirus signatures)
- Monitoring event logs to identify problems and suspicious activity
- Providing remote system administration and assistance
- Monitoring changes to OS and software settings as configuration drifts may occur overtime
- Protecting and sanitizing media
- Responding promptly to suspected incidents
- Assessing the security posture of a system through vulnerability assessments[18]
- Disabling unneeded user accounts and deleting accounts that have been disabled for some time
- Maintaining system, peripheral, and accessory hardware (periodically and as needed), and logging all hardware maintenance activities.

2.8 Summary of Recommendations

- Protect each system based on the potential impact to the system of a loss of confidentiality, integrity, or availability.

---

[17] Organizations should have an incident response policy and a formal incident response capability. For guidance on incident handling preparation and execution, see NIST SP 800-61 Revision 2, *Computer Security Incident Handling Guide*, available at http://dx.doi.org/10.6028/NIST.SP.800-61r2.

[18] See NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*, for more information on performing vulnerability assessments. The publication is available at http://csrc.nist.gov/publications/PubsSPs.html.

- Reduce the opportunities that attackers have to breach a system by resolving security weaknesses and limiting functionality according to the principle of least privilege.

- Select security controls that provide a reasonably secure solution while supporting the functionality and usability that users require.

- Use multiple layers of security so that if one layer fails or otherwise cannot counteract a certain threat, other layers might prevent the threat from successfully breaching the system.

- Conduct risk assessments to identify threats against systems and determine the effectiveness of existing security controls in counteracting the threats. Perform risk mitigation to decide what additional measures (if any) should be implemented.

- Document procedures for implementing and maintaining security controls. Maintain other security-related policies and documentation that affect the configuration, maintenance, and usage of systems and applications, such as acceptable use policy, configuration management policy, and IT contingency plans.

- Test all security controls, including the settings in the NIST security baselines, to determine what impact they have on system security, functionality, and usability. Take appropriate steps to address any significant issues before applying the controls to production systems.

- Monitor and maintain systems on a regular basis so that security issues can be identified and mitigated promptly. Actions include acquiring and installing software updates, monitoring event logs, providing remote system administration and assistance, monitoring changes to OS and software settings, protecting and sanitizing media, responding promptly to suspected incidents, performing vulnerability assessments, disabling and deleting unused user accounts, and maintaining hardware.

3. OS X Security Components Overview

This section presents an overview of selected security features offered by the OS X operating system (OS). This section highlights the security features and security-supporting features in OS X 10.10 such as privacy protection, anti-malware, and firewall capabilities.

3.1 Gatekeeper

Gatekeeper was a new feature in OS X 10.8[19] that essentially enforces high-level application whitelisting for installing applications. Already-installed applications are unaffected by Gatekeeper settings. There are three configuration options for Gatekeeper: to allow only applications from the Mac App Store, to allow only applications from the Mac App Store and "identified developers"[20], and to allow all applications. These settings can be overridden by choosing Open in the Finder for a restricted application and then providing administrator-level credentials.

3.2 Software Updates

In OS X 10.10, software updates are obtained from the Mac App Store. The system can be configured to automatically download updates, and also install them. See Section 4.3 for more information on OS X updates.

In previous versions of OS X, updates to the operating system and its built-in applications were acquired through the Software Update application. Updates are now obtained through the Mac App Store application. Another significant change is that the system can be configured not only to automatically download updates, but also to install them. See Section 4.3 for more information on OS X updates.

3.3 Privacy Settings

OS X provides several privacy settings to allow users control over the actions performed with their information. Examples include the following:

- Activating or deactivating Location Services, and restricting which applications can use Location Services
- Controlling which applications can access the user's Calendar and Contacts
- Sharing anonymous diagnostic information with Apple
- Configuring Safari to use "Do Not Track" headers

[19] Months after OS X 10.8's release, Gatekeeper was added as a feature to OS X 10.7.5.

[20] Apple provides what it calls a "safe downloads list", which identifies the developers whose applications can be downloaded through this Gatekeeper option.

3.4 Credential Management

A *keychain* is a mechanism for securely storing your passwords for applications and other small pieces of sensitive information, such as cryptographic keys, digital certificates, and account numbers. Using a keychain can greatly reduce the number of passwords that you have to remember. The keychain itself has a password that you must enter to gain access to the passwords stored in the keychain; this protects the keychain contents from being accessed by someone else. Because you only have to remember a single password, you can choose more complex, harder-to-guess passwords for your applications.

By default, the keychain is stored on the OS X computer. You can also save keychains to removable media, such as a USB flash drive.[21] This allows you to securely transport your passwords between OS X computers. You can also have multiple keychains, such as a portable keychain with only those passwords that need to be used on multiple computers, and a regular keychain (stored on the local computer) with the other passwords.

3.5 Host-Based Firewalls

OS X offers two host-based firewalls—an application-based one that can be configured through the GUI, and a protocol-based one that can be configured through the command line. The application-based firewall filters incoming network traffic only, by application, based on the digital signature of each application. For example, it can be configured to prohibit the use of email services (SMTP, POP3, etc.) with any application other than the designated email client application, and it can prohibit the use of all email services when the designated email client application is not running. If an organization wanted to prohibit the use of chat services, it could configure the application-based firewall to block all incoming chat service attempts.

The protocol-based firewall, `pf`[22], is a more traditional port-based firewall that can restrict both incoming and outgoing network traffic based on the TCP and UDP port numbers that the traffic uses. pf is intended to be used by administrators and advanced users who want stronger protection than the application-based firewall can provide. An example is restricting the email servers accessible to the OS X host. Rules for the application-based firewall and the `pf` firewall may conflict with each other, but if either firewall denies access, the traffic is blocked. Additional information about `pf` is located in Section 6.6.1.

3.6 Storage Encryption

OS X 10.10 supports three forms of storage encryption: FileVault, FileVault 2, and Disk Utility. These three encryption methods possess varying functionality and strengths.

FileVault is a legacy utility for encrypting a user's home folder on an OS X host. FileVault was replaced starting in OS X 10.7 by FileVault 2[23], but OS X maintained support for the legacy FileVault for those users who, for various reasons, cannot or do not want to upgrade to FileVault

---

[21] Consult your organization's removable media policies to determine if this is acceptable in your environment.
[22] Before OS X 10.8, the protocol-based firewall was called `ipfw`. The `pf` firewall provides similar functionality to `ipfw`.
[23] Note that the OS X 10.10 GUI uses the name FileVault, which is in fact FileVault 2.

2. For example, a host cannot start using FileVault 2 until each of its users stops using legacy FileVault. However, it is recommended to use FileVault 2 for the enhanced security it provides. One of the drawbacks of FileVault 2 is that it requires considerably more disk space than legacy FileVault, so it is possible that a host could have enough free space available to continue running legacy FileVault but not upgrade to FileVault 2. On OS X 10.10, it is no longer possible to create a new instance of the legacy FileVault.

The reason why FileVault 2 needs more space is because it provides full disk encryption[24], not encryption of just the home folder portions of the disk. Also, FileVault 2 requires that the Recovery Partition (which typically is hidden from user view) be installed on the startup volume. FileVault 2 can provide significantly stronger storage protection than the original FileVault could because of its increased coverage. Another important fact to note is that FileVault 2 uses XTS-AES 128-bit encryption.

Neither the legacy FileVault nor FileVault 2 can be used to encrypt data stored on removable media, network drives, and other non-local locations. For those cases, OS X provides Disk Utility, which performs many functions, including encryption of disk images. A disk image is essentially a virtual container that holds files and folders. Disk Utility can encrypt disk images, which allows encrypted files to be sent to others via email, file transfers, etc., and to be stored securely on removable media, network shares, and other locations. Also, Disk Utility can use 128-bit or 256-bit AES encryption.

3.7 Code Execution Protection

The following are examples of OS X 10.10's code execution protection features:

- Address space layout randomization (ASLR) is a security technique that is supported by many operating systems, including OS X 10.10. When ASLR is used, executables and their related components (libraries, etc.) are placed into memory at random locations, so that an attacker (or malware) cannot predict or readily guess where one component is located based on the location of another component. ASLR is built into OS X 10.10, and the OS provides no option for disabling or otherwise configuring it.

- Execute disable (XD) is a feature built into the CPUs of OS X 10.10 systems that separates data and executables in memory. This helps to deter an attacker from injecting malicious "data" and then executing that data. There is no option for disabling XD.

- Several OS X features rely on application signing to identify particular applications and verify their integrity—examples include the application-based firewall and the keychains. Apple signs applications included with OS X, and third-party applications may be signed by their developers as well. Also, the operating system may sign unsigned applications for use with certain OS features.

- OS X offers application sandboxing. This separates an application from the rest of the

[24] For more information on storage encryption technologies, see SP 800-111: *Guide to Storage Encryption Technologies for End User Devices*, available at http://dx.doi.org/10.6028/NIST.SP.800-111

host in designated ways, dictating which resources it is allowed to utilize. Examples include restricting network access and file access. Application sandboxing was expanded in OS X 10.8 to include several built-in applications such as Mail and FaceTime. Also, sandboxing is used for all new applications on the Mac App Store. However, sandbox support must be built into the application, and the user cannot force an application to run in a sandbox.

- OS X has a quarantine feature for downloaded files. When a file is downloaded from an external source, such as a web server or an email attachment, the application that downloaded it (Safari, Mail, or Messages) tags it as quarantined. When a user attempts to execute a quarantined file, the user is presented with the download metadata (timestamp and location) and asked whether they still want to execute the file or not. If they agree to execute it, the quarantine tagging is removed. The purpose of quarantining is to reduce the likelihood that a user will run a malicious executable that they have downloaded.

3.8 Encrypted Virtual Memory

OS X secures its virtual memory by encrypting it, thwarting attempts to extract sensitive data from it. This feature has been enabled by default in OS X since version 10.6. Disabling virtual memory encryption does not appear to be possible after OS X 10.8.

3.9 Application Whitelisting

OS X provides application whitelisting capabilities through its Parental Controls feature. This feature, if enabled, restricts which installed applications may be executed by a particular user. See Section 6.5.2 for additional information.

4. Installation, Backup, and Patching

This section provides guidance on installing, backing up, and patching OS X systems, as well as migrating data between OS X systems and identifying security issues in OS X systems.

4.1 Performing an Installation

This section discusses the basic methods for performing an OS X 10.10 installation, both for new installations and for upgrades. This section breaks down the installation process into three phases: media sanitization, old patches, and OS installation, migration, and upgrades.

4.1.1 Media Sanitization

If a computer has previously been used for another purpose, it may be necessary to sanitize its storage media (i.e., hard drive) before using it again. There could be sensitive information that has not been fully scrubbed from the media. Fortunately, OS X provides the Disk Utility feature, which has options for media sanitization. For example, it can be used to securely erase a disk partition, offering three levels of erasure: single-pass, 3-pass, and 7-pass. Although a single-pass erasure may be more convenient in some cases, it is generally recommended to do at least seven passes when overwriting data on standard hard drives.[25] Note that if the hard drive is solid state (flash-based), a single pass will deter most data recovery attempts. Depending on the sensitivity of the data on the media, additional preventive measures may be required. Third-party media sanitization utilities can be used instead of Disk Utility if desired, following the same guidelines about the number of passes.

An alternative strategy to securely erasing a disk partition is to install OS X 10.10 on the partition, and then securely erase all free space remaining on the partition after the installation is completed. This can be accomplished using Disk Utility's Erase Free Space option. Erase Free Space should offer enough protection to allow safe reuse in many cases – especially reuse within the same organization. The Erase Free Space option offers three levels of erasure: single-pass, 3-pass, and 7-pass. The above recommendations for the number of passes per media type apply. Note that erasing free space can take a considerable amount of time, depending on the size and the speed of the storage device.

4.1.2 Old Patches

Preparation for installing or upgrading to OS X 10.10 may necessitate installing all old patches to a previous version of the operating system.[26] For example, if a system is being upgraded from a previous version of OS X, it is recommended to install all existing patches for the OS before doing the upgrade. Also, if a new install is being done but data is being migrated from an old system, it is recommended that the old system's OS be fully patched first.

---

[25] More information on sanitizing storage devices is available from the Department of Defense's *National Industrial Security Program Operating Manual*, DoD 5220.22-M, located at http://www.dtic.mil/whs/directives/corres/html/522022m.htm, and from NIST SP 800-88, *Guidelines for Media Sanitization*, located at http://dx.doi.org/10.6028/NIST.SP.800-88r1.

[26] Apple states that some updates rely on previous updates: https://support.apple.com/en-us/HT201541

4.1.3 OS Installation and Upgrades

For OS X, a new installation and an upgrade use the same software, called an "installer". New installations and upgrades follow the same basic process, except that new installations will ask more questions than an upgrade will. For example, when a new install occurs, the Setup Assistant performs operations such as configuring networking and creating an initial administrator account that are not necessary for an upgrade. The Installer also presents the user with the option to run the Migration Assistant, which can transfer a user's configuration settings, accounts, data, etc. from another OS X system. See Section 4.1.4 for more on the Migration Assistant.

As of October 2015, it is no longer possible to obtain a new copy of OS X 10.10 from Apple via the Mac App Store. However, 10.10 can be downloaded using an Apple account that has previously downloaded the OS. It can be obtained through the **Purchased** tab in the Mac App Store. Organizations should consider saving a copy of the version of OS X that comes with new systems so that they can restore to that version later if necessary. [27]

A new installation can be performed as "clean" or as a reinstall over an existing OS X 10.10 installation. Apple recommends doing a clean install if OS X 10.10 is already installed. Accordingly, this section will only provide instructions for clean installations and upgrades, not reinstallations.

There are several methods of performing an installation or upgrade. These tend to fall into two categories:

- A **dynamic installation process**, involving performing a full installation of OS X 10.10 from installation media, then completing the configuration of the installed system (e.g., configuring security settings).

- The **monolithic imaging process**, which refers to setting up and configuring one system completely, then cloning it (creating an image of it) and copying that image to other systems. After the image is put in place, minor configuration changes may be needed, such as to set a unique system name and to add accounts for local users.

Administrators should also be aware that by default, the OS X installer creates a recovery partition that is used in the event of a system failure. This is a good recovery mechanism, but it may present another attack vector.

The subsections below provide more detail on the available installation methods.

[27] If OS X 10.10 was never downloaded, it will not be available for download, even if the computer is already running OS X 10.10.

4.1.3.1 System Image Utility

System Image Utility is an Apple-provided utility that is available on OS X 10.10. System Image Utility is used to create a network disk image, which refers to a disk image that is accessible over a network. As part of the disk image creation process, the images can be preloaded with configuration profiles provided by Profile Manager. When the disk images are to be accessed over a network, a Mac with OS X Server software is required to host them. The utility supports three image creation options, visible in Figure 1:[28]

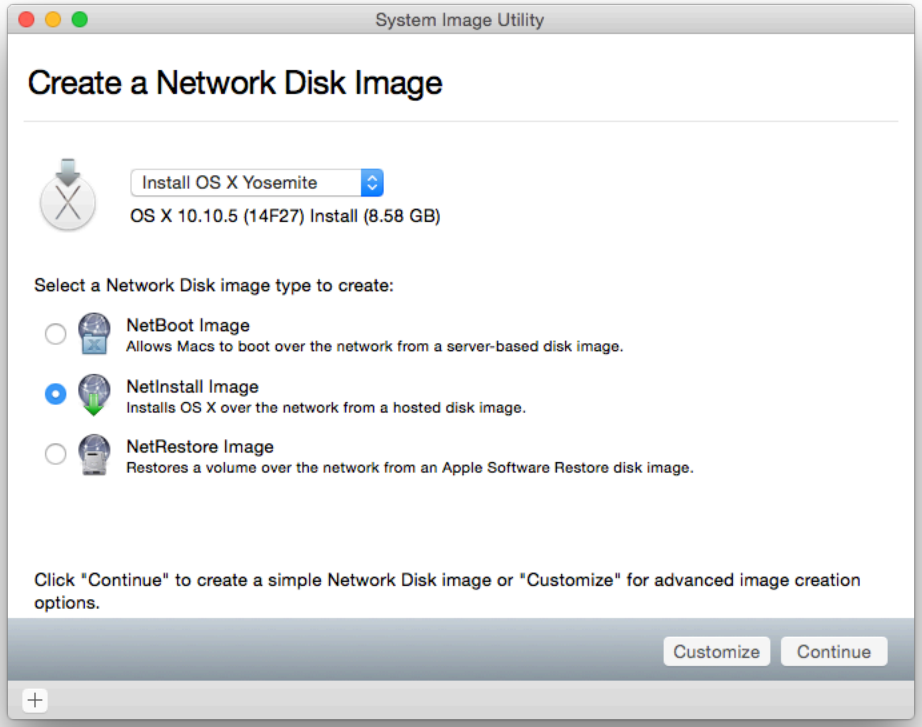

Figure 1: System Image Utility

- **NetBoot:** Boot an OS X 10.10 system from a remote network disk image (i.e., stored on an OS X Server). This image type is not appropriate for deploying images to systems, only for running systems remotely from an image.

- **NetInstall:** Install OS X 10.10 from a remote network disk image. This is basically the equivalent of using the standard OS X 10.10 installer. It allows an administrator to select

[28] https://support.apple.com/en-us/HT202061.

which OS X 10.10 packages are installed on a local system. The administrator will be responsible for configuring the system properly after the installation completes.

- **NetRestore:** Restore an OS X 10.10 volume from a remote Apple Software Restore disk image. This type of system image is a clone of a configured OS X 10.10 system, and using this image will restore the cloned image onto a local system. There are no configuration options available for a NetRestore installation; the entire cloned image will be restored onto the system.

NetRestore images are used with Apple Software Restore (filename asr), which is a command-line utility included in OS X 10.10 systems that can restore a system based on a NetRestore image.

Note that there must be a DHCP server on the local network at boot time for the client to connect to the image storing machine. OS X Server can provide a DHCP server, if needed. To enable a DHCP server in the OS X Server application, expand the **Advanced** section on the left pane, select **DHCP**, and then toggle the **On/Off** switch.

4.1.3.2 Third-Party Utilities

There is a variety of third-party utilities that can perform custom installations of OS X 10.10. These utilities perform what they call “imaging”, but this is much more complicated than simply copying an image to a host. Instead, these utilities perform modular installations of OS X 10.10 components that include extensive configuration of the system. The utilities can also execute scripts to perform customizations that are not directly supported by the utilities.

The advantage of using third-party utilities for installing OS X 10.10 is that they can handle both installation and configuration in an integrated and automated way, and administrators therefore do not have to do installation and configuration as separate steps. Configuration in particular can be a tedious manual process, although automated tools are increasingly available for implementing configurations. It is entirely feasible to do a standard OS X installation and then use a third-party utility to configure that installation. See Section 5 for more on security configuration automation techniques.

4.1.4 Migration Assistant

Migration Assistant is a utility built into OS X 10.10 that can “transfer user accounts, applications, and computer settings” and data to an OS X 10.10 system from another Mac, a Windows PC, a disk from a Mac or PC, or a Time Machine backup. Although Migration Assistant can be very helpful at transferring user data (e.g., files) and profiles (i.e., accounts), it can inadvertently cause problems by migrating compromised, vulnerable, or outdated applications, as well as migrating security misconfigurations from one system to another. Therefore, it is recommended that Migration Assistant only be used to transfer user data and local profiles[29], preferably through Time Machine backups. Applications should not be migrated

[29] If an OS X system uses a domain account (non-local account), the account itself should not be migrated using Migration Assistant. Only local accounts should be migrated.

using Migration Assistant. Also, data and profiles should not be migrated until after OS X 10.10 and all applications have been installed and fully patched.

4.2 Backing Up

To increase the availability of data in case of a system failure or data corruption caused by a power failure or other event, OS X has built-in capabilities to back up and restore data and systems. Time Machine is the built-in backup and restore utility. It does not provide all of the advanced backup and security features that third-party backup and restore utilities may offer, but it can encrypt its backups and it can recover an entire disk in case of failure. Also, it does backup updates once an hour, as long as the backup media is available, so it provides very granular backups.

By default, Time Machine is disabled. To enable it, go to **System Preferences**, then **Time Machine**, and set it to "ON". To configure it, click the "Select Disk…" button, select the disk that will hold the backups, enable the "Encrypt backups" option, and then click the "Use Disk" button. The system may prompt the user to allow the backup media to be erased and reformatted for compatibility. The system will also prompt the administrator to enter a backup password (to encrypt the backup) and a password hint. The administrator should enter a strong password to protect the backup and enter nothing useful for a password hint, to better protect the password. This password will be required every time the Time Machine backup media is connected to the OS X system, and to recover from a previously encrypted backup. See Figure 2 and Figure 3 for the Time Machine backup settings.

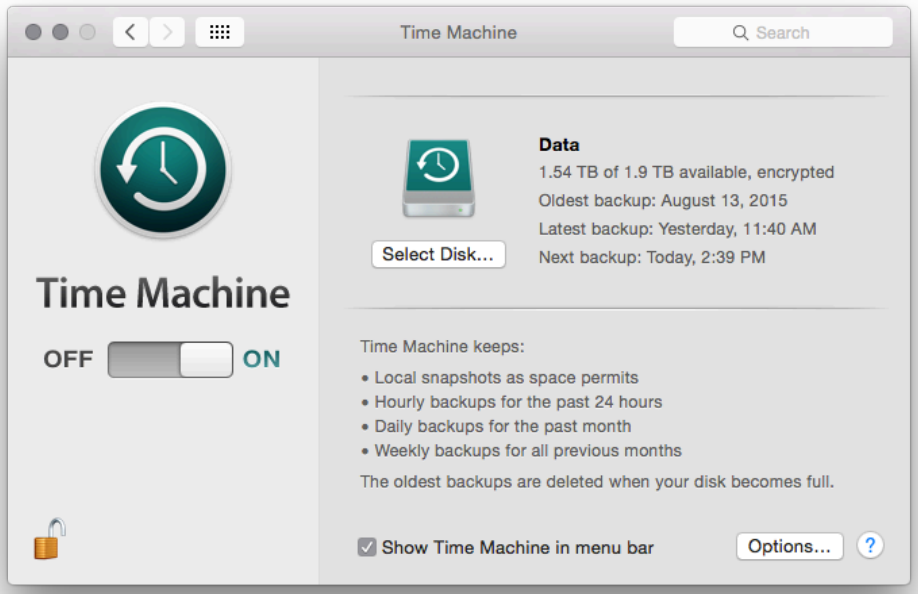

Figure 2: Time Machine System Backup

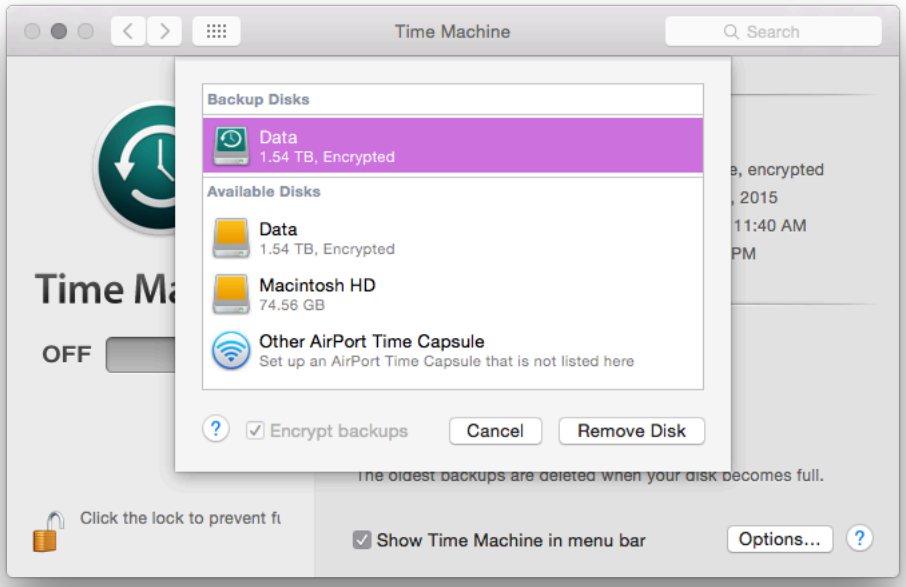

Figure 3: Time Machine Select Disk Menu

When using an encrypted Time Machine disk, it is important to understand that a different (perhaps newer) version of OS X may not be able to restore from the encrypted Time Machine disk. When using encrypted Time Machine backups, it is therefore important to have access to an OS X system running the same version (e.g., 10.10) that was used to create the backups in order to guarantee the ability to recover backed-up data.

Another backup option built into OS X is iCloud. iCloud is available for limited backup capabilities, such as duplicating contacts in the cloud. Organizations should disable iCloud unless there is a specific reason to be using it for backup purposes or other reasons. Note that disabling iCloud also prevents use of the Find My Mac utility, which itself can pose security and privacy risks. To temporarily disable iCloud, go to **System Preferences**, then **iCloud**, and deselect all of the services listed in the pane (Mail, Contacts, Calendars & Reminders, etc.) Note that users can re-enable iCloud without administrative privileges.

Besides the backup methods provided by Apple, there are also various third-party local and enterprise utilities for backing up and restoring files and systems. These can be used instead of or in addition to the Apple backup methods.

Regardless of the backup method chosen, it is very important to verify periodically that backups and restores can be performed successfully; backing up a system regularly will not be beneficial if the backups are corrupt or the wrong files are being backed up, for example. Organizations should have policies and procedures that address the entire backup and recovery process, as well as the protection and storage of backup and recovery media. Because backups may contain

sensitive user data as well as system configuration and security information (e.g., passwords and KeyChain database), backup media should be properly protected to prevent unauthorized access. For additional guidance on backups and backup security, see NIST SP 800-34 Revision 1, *Contingency Planning Guide for Federal Information Systems*.[30]

4.3 Installing Updates

It is essential to keep a system's operating system and applications up to current patch levels to eliminate known vulnerabilities and weaknesses. Apple provides two mechanisms for distributing security updates for Apple-provided software: the Mac App Store and manual package updates. These are discussed below. There are also third-party applications that can be used to manage both Apple and non-Apple patches, and some non-Apple applications can update themselves automatically as well. Organizations should use one or more of these update mechanisms to ensure that the operating system and major applications are kept fully patched.

For more information on enterprise patch management and general recommendations for patching, see NIST SP 800-40 Revision 3, *Guide to Enterprise Patch Management Technologies*.[31]

4.3.1 Mac App Store

Through the App Store preferences pane, an OS X system can be configured to check the Mac App Store automatically every day for new updates, download them, and install them. If using this technique to keep an OS X system up-to-date, organizations should configure it to do the checks, downloads, and installations automatically. Figure 4 shows these options enabled. Note that because administrator-level credentials are needed for installation, update installation cannot be fully automated for typical users (who should not be running as administrator on a daily basis).

[30] http://csrc.nist.gov/publications/PubsSPs.html#800-34
[31] http://dx.doi.org/10.6028/NIST.SP.800-40r3

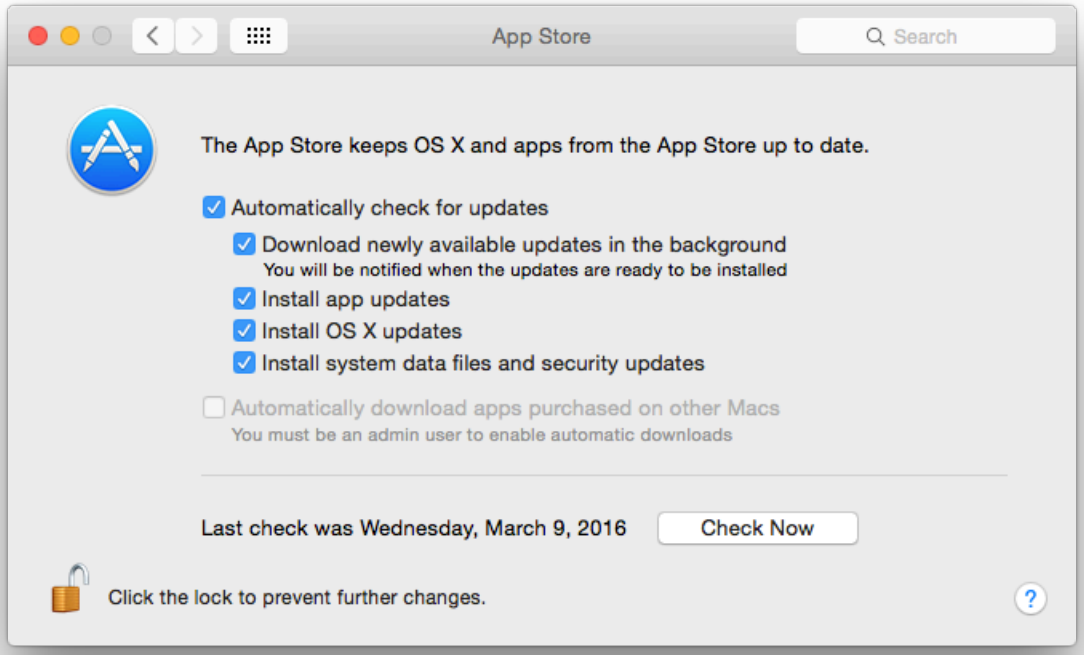

Figure 4: Software Update Options

Some organizations do not want the latest updates applied immediately to their OS X systems. For example, in a Managed environment, it may be undesirable for updates to be deployed to production systems until OS X administrators and security administrators have tested them. In addition, in large environments, many systems may need to download the same update simultaneously. This could cause a serious impact on network bandwidth. Organizations with such concerns often establish a local update server (using OS X Server) that contains approved updates and restrict the locations from which OS X systems can retrieve updates. [32] See Appendix J.13 for a list of commands that can be used to configure system update settings through the command line.

4.3.2 Manual Package Updates

As discussed at http://help.apple.com/securityguide/mac/10.7/#apd0EE658C4-40DC-4ECA-944D-549CD1A53ACB, each update can be downloaded and installed through the command line. This allows scripting of the update process.

4.4 Summary of Recommendations

- Before provisioning a computer for reuse, it should have its media sanitized prior to OS X installation.

[32] For more information on setting up a local update server, see https://support.apple.com/en-us/HT202030.

- Regardless of how an organization chooses to install OS X software and updates, the choices should be clearly described in a configuration management policies and procedures document, and both administrators and regular users should be instructed to follow the guidance contained therein.

- It is generally recommended to do at least seven passes when overwriting data on standard hard drives. Note that if the hard drive is solid state (flash-based), a single pass should be sufficient.

- When installing OS X, Apple recommends doing a clean install if OS X is already installed, instead of a reinstall.

- Until a new system has been fully installed and patched, either keep it disconnected from all networks, or connect it to an isolated, strongly protected network.

- It is very important to verify periodically that backups and restores can be performed successfully and that backups are protected.

- Keep systems up to current patch levels to eliminate known vulnerabilities and weaknesses.

5. Overview of OS X Managed Security Configuration

This section discusses options for managing the security configuration of OS X desktops and laptops in a Managed environment.

5.1 Directory Services

A directory service is responsible for managing computing resources, such as computers, printers, and networks. It handles user authentication and ensures that connected resources follow organizational policies. This eases system administration because the systems are managed from a central location. Furthermore, user accounts are independent of the individual machines, which allows users to log in to any directory-bound computer. OS X systems are compatible with both the Open Directory and the Active Directory services.

5.2 Profile Manager

Profile Manager works by manipulating a configuration profile, which is an XML file that contains security settings and other configuration settings. Profile Manager can apply a profile to an OS X 10.10 system, thus altering its configuration settings to correspond to a chosen policy. These settings typically include most of the settings that could be manually configured through the OS X 10.10 GUI.

Profile Manager provides several benefits compared to manual or script-based configurations:

- Prevents users from modifying system preferences. This may not be possible through a manual configuration.
- Easier to set up. Once a domain is set up, the policies can be pushed to all connected machines.
- Easier to manage; more scalable. Making changes to a hundred computers is as easy as making a change to one.

Profile Manager also has limitations:

- Less flexible than manual configuration. With manual configuration, every single file on the system can be accessed and changed.
- Requires directory infrastructure to be in place. The complexity of centralized management may not be justified for smaller environments.

It is important to keep in mind that, although centralized management makes it easy to configure many computers, it also raises the risk of inadvertent misconfiguration of many computers. Therefore, testing should be performed on all configurations before deployment. Applying a setting through both Profile Manager and a custom script should produce consistent behavior, except for password policy items, where the scripted behavior will take precedence. Where possible, using Profile Manager to configure settings is preferred since it will prevent further modification by the user. The NIST configuration checklist and Profile Manager have the

following settings in common:

- Screen saver grace period
- Disable AirDrop
- Warn before emptying trash
- Disable dictation
- Do not send diagnostic info to Apple
- Disable iSight camera
- Autohide Dock

Profile Manager supports the following password policy rules:

- History restriction
- Contains alphabetic char, numeric char, symbolic char
- Minimum length
- Maximum age

However, a Profile Manager password policy is not compatible with a script-based implementation. A script implementation offers more configuration options for a stronger password policy, so it is recommended over Profile Manager.

5.3 Application Installation and Configuration

There are several methods available for installing applications, including the following:

- **Apple disk images (`.dmg`).** These are mainly used when an application just needs to be copied into the correct location in order to install it.
- **Installer application.** Installer is an application built into OS X that is used to install software from package (`.pkg`) and metapackage (`.mpkg`) files. It has a GUI version and a command line version (located at `/usr/sbin/installer`). The package and metapackage files can be used not only to install applications, but also to deploy application updates and application configuration settings.
- **Mac App Store.** The Mac App Store can be used to download and install a variety of applications from Apple and third parties.
- **Application-provided proprietary means.** A third-party application may provide its own proprietary installation method.

- **Third-party application management software.** An organization may use a utility that handles application management or software distribution, such as regulating which versions of software are permitted to be installed on the organization's systems and ensuring that this software is kept fully patched. These third-party utilities might also provide mechanisms for distributing application configuration settings.

While all of these methods may alter security configuration settings as part of their installation processes, note that two of these methods—the Installer application and third-party application management software—can be used outside of the installation process to distribute security configuration settings to OS X systems. This is useful for maintaining settings for already-installed applications.

In addition to the Installer application and third-party application management software, there are other means of altering settings for existing applications, as well as the operating system itself. For example, shell scripts can be run on an OS X system to alter OS configuration settings. There are also a variety of configuration management tools, some supporting the Security Content Automation Protocol (SCAP), which can also be used to alter OS and application settings.

5.4 Security Content Automation Protocol (SCAP)

System security is largely dependent upon staying up to date with security patches, maintaining well-considered configuration settings, and identifying and remediating other security weaknesses as they are identified. Unfortunately, OS X does not provide built-in utilities for assessing its system security, other than basic auditing capabilities. Third-party utilities are needed to verify patch installation, identify security configuration setting weaknesses, and find other security issues on OS X systems.

Configuration management tools are available that can be used to assess the security postures of OS X systems, either periodically or on a continuous basis (continuous monitoring). These tools have a variety of capabilities, such as comparing security settings with baseline settings and identifying missing patches. Some tools can also correct problems that they find by changing settings, installing patches, and performing other actions. Some tools can provide an independent verification that the security controls are implemented as intended and can document this verification for use in demonstrating compliance with laws, regulations, and other security requirements. NIST has been leading the development of SCAP, [33][34] which is a set of specifications for expressing security information in standardized ways. Configuration management tools that support SCAP can use security baselines that are made publicly available by organizations such as NIST, and they can also generate output in standardized forms that can be used by other tools.

---

[33] See NIST SP 800-117, *Guide to Adopting and Using the Security Content Automation Protocol (SCAP) Version 1.0*, at http://dx.doi.org/10.6028/NIST.SP.800-117.

[34] See NIST SP 800-126, *The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2*, at http://dx.doi.org/10.6028/NIST.SP.800-126r2

6. NIST OS X Security Configuration

This section provides an overview of the security configuration options for OS X 10.10 systems and explains how they can provide better security. These configuration options are grouped by the following categories:

- System hardware and firmware (Section 6.1)
- Filesystem security (Section 6.2)
- User accounts and groups (Section 6.3)
- Auditing (Section 6.4)
- Software restriction (Section 6.5)
- Network services (Section 6.6)
- Applications (Section 6.7)
- Other security management options (Section 6.8)

Throughout this section, there are instructions for changing security configuration settings. The instructions may provide multiple values for each setting depending on the profile (Standalone, Managed, SSLF). If only one value is specified, then it should be assumed that all profiles use that value. Some settings are applied to a single user, and a `~` in the directory path represents the path to the current user's home directory that will be modified. In order to modify another user's settings, use `~$USER` instead of `~`.[35] Unless explicitly stated otherwise, it is also assumed in each case that the person making the changes has access to an administrator-level account on the OS X system and uses that account to make the changes. Using an administrator-level account to modify user-level configuration settings in this way may change a file's owner. See Appendix C for a list of tools that can be used to make configuration changes, along with short descriptions of their functionality.

Since most power management settings are not security relevant, they are not discussed here; however, the full set of configuration commands is included in Appendix J.16.

6.1 System Hardware and Firmware

A system is not secured unless the hardware and firmware have been secured. This section describes techniques for restricting access to firmware and disabling unneeded hardware components.

[35] See Appendix F for more information on system variables.

6.1.1 Restricting Access to Firmware

What is known as the BIOS on a PC is known as the Extensible Firmware Interface (EFI) on a Mac (formerly called Open Firmware). The EFI launches the OS and determines whether the OS should boot normally or in single-user mode, which automatically logs in the root account, providing full administrator-level access to the system. Unauthorized booting in single-user mode is a major security weakness, but it can be prevented by setting an EFI password. An EFI password also prevents someone unauthorized from booting the system from another media.

Unfortunately, someone with physical access to the system may be able to circumvent EFI passwords. In systems where memory is removable, a person who changes the physical memory configuration can bypass an EFI password and boot the computer as root, boot from different media, etc. Therefore, organizations should not rely on EFI passwords to provide security unless the physical security of the system is ensured.

6.1.2 Disabling Hardware Components

OS X systems contain many hardware interfaces, for purposes such as wireless networking, data transfer, and multimedia. Each interface creates a potential point of attack on the system. Accordingly, an organization may determine that one or more of these interfaces are unnecessary and should be disabled, particularly in SSLF environments. An example is an organization that prohibits the use of cameras on desktop and laptop systems. Another example is a policy that Bluetooth should be disabled if not being used by the system's keyboard, mouse, or trackpad. Organizations should determine which interfaces may be needed and disable all other interfaces. Organizations should be mindful of accessibility features made available through various hardware interfaces that might otherwise be unused. For example, features such as Dictation and VoiceOver make extensive use of the microphone (or line in) and speakers. Accessibility settings are described in Appendix J.2.

There are two types of methods for disabling selected hardware interfaces. One method involves deleting the associated kernel extensions (files that end with a `.kext` extension), which is only recommended for SSLF systems. Security relevant interfaces include Bluetooth, Wi-Fi, infrared, FireWire, Thunderbolt, USB mass storage, webcam, and audio. When testing kext removal, hardware interfaces did not consistently remain disabled. Therefore, kext removal should not be relied upon to disable hardware interfaces. The second method involves changing configuration settings to disable the interfaces. Note that with this second method, in most cases users are able to override the configuration settings without any administrative privileges, so organizations should not rely on these configuration settings to provide security since users can alter them at will.

However, organizations should also be cautious about the strength of the method involving deleting kernel extensions. These extensions may inadvertently be restored by an administrator or by an OS update (patch). For any OS X host where disabling hardware interfaces is a security prerogative, the host's interfaces should be continuously monitored to detect any restoration of disabled interface functionality.

Both methods for disabling the hardware components can be implemented by running the commands found in Appendix J.1.

6.2 Filesystem Security

This section covers filesystem security for both internal and removable media. Its information is presented in the following categories: general, storage encryption, secure erase, file and folder permissions, and Spotlight.

6.2.1 General

The system's main hard drive partition should be formatted as HFS+. This filesystem supports all the filesystem security features provided by OS X 10.10.

Disk Arbitration determines if new drives should be mounted automatically. Although disabling this prevents inadvertent mounting of drives that may contain malicious content, this also prevents internal disks from being mounted upon system restart. Since OS X would be unable to boot on system restart, it is not recommended to disable disk arbitration.

Finder should be configured to not show hidden files and folders; this is already configured by default. However, administrators with intimate knowledge of the OS X system could notice unusual hidden files and would benefit from their visibility. Consequently, hidden files should be displayed in an SSLF environment. Finder should also be configured to show file extensions, to show a warning before changing a file extension or emptying the trash, and to search this system when performing a search. These options can improve defenses against malware. To configure these options, go to **Finder**, then **Preferences**, and click **Advanced**; then enable the corresponding options as shown in Figure 5. To configure Finder settings through the command line, see Appendix J.3.

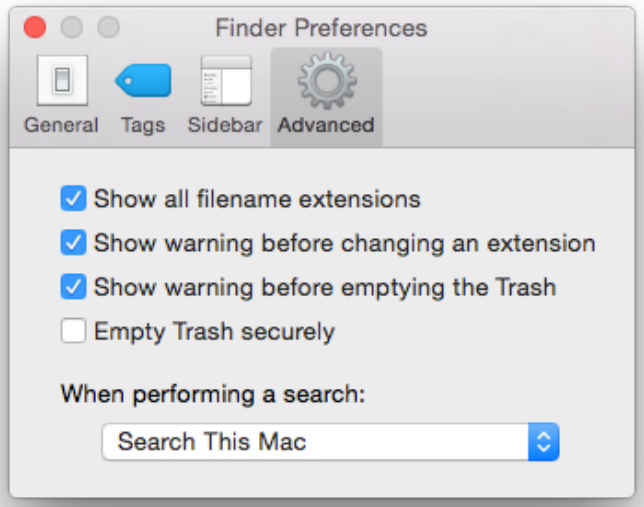

Figure 5: Advanced Finder Preferences

6.2.2 Storage Encryption

As discussed in Section 3.6, OS X provides two mechanisms for storage encryption: FileVault 2 and encrypted disk images.

6.2.2.1 FileVault 2

It is recommended when enabling FileVault 2[36] to log out of the system and log in with an administrator account. After doing so, go to **System Preferences**, then **Security & Privacy**, and select the **FileVault** pane. Select the button marked "Turn On FileVault…" to begin enabling FileVault 2. Designate which users should be allowed to unlock the FileVault encryption (i.e., log on the system after it has been encrypted) and have each user authenticate.[37] OS X will then generate a recovery key[38] and present it on the screen, so that it can be transferred to a secure location (not on the system) for use in case all the passwords on the system are forgotten or otherwise lost. OS X will also provide an option to store the recovery key with Apple; this key is only protected through recovery questions, so it is not recommended that this option be used because of the possibility of the recovery key being retrieved by unauthorized personnel.

After rebooting the OS X system, the encryption process will begin for FileVault 2. This may take several hours, depending on the hardware characteristics of the system and the amount of data that needs to be encrypted. However, this encryption process can take place in the background while other work occurs. When finished, the FileVault 2 settings page should look similar to that of Figure 6.

---

[36] The OS X 10.10 user interface uses the name FileVault to refer to FileVault 2.

[37] If a user is not available to authenticate at this time, it can be skipped. However, the user will need to authenticate within an administrator's session (**System Preferences** / **Security & Privacy** / **FileVault** tab, "Enable Users..." button).

[38] In OS X 10.6 and earlier, there was no recovery key; instead, there was a "master password". The recovery key has replaced the master password in terms of functionality.

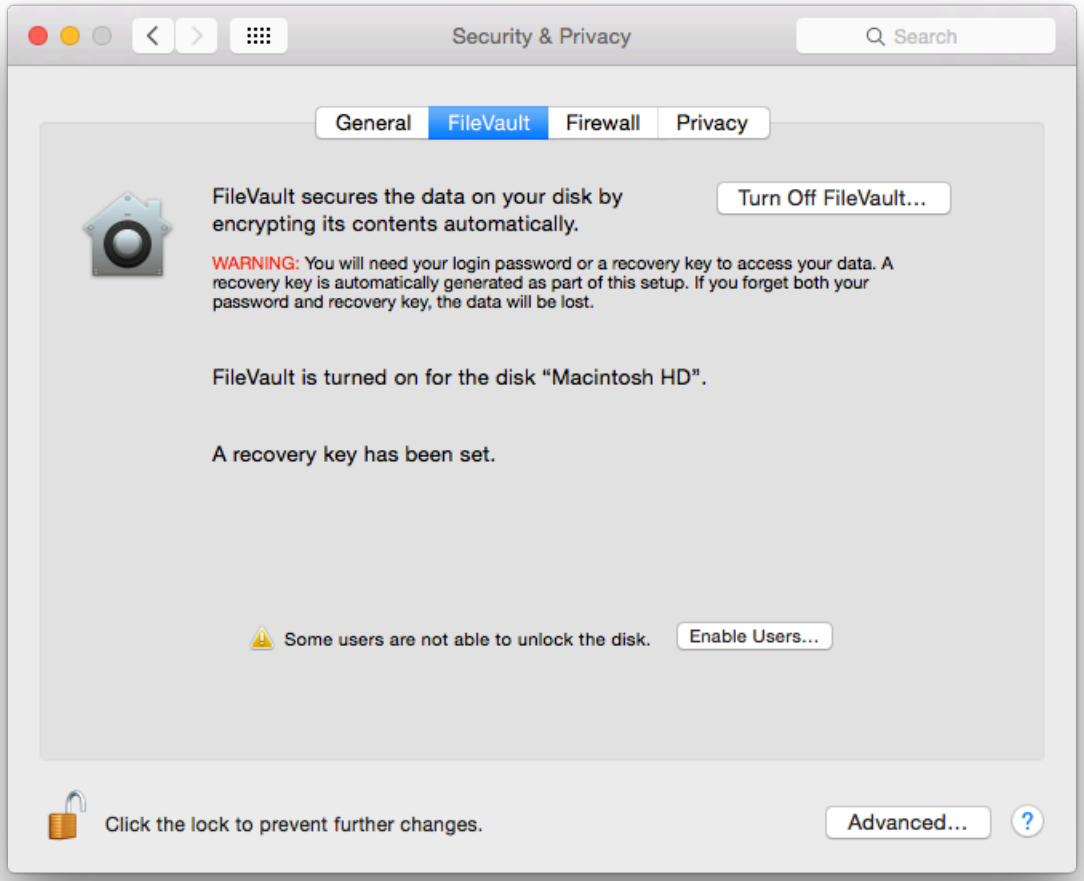

Figure 6: FileVault 2 Settings

For more information on FileVault 2, see the Apple technical white paper titled "Best Practices for Deploying FileVault 2".[39] Of particular interest is that this paper describes additional enterprise tools for FileVault 2 key management and recovery.

6.2.2.2 Encrypted Disk Image

As explained in Section 3.6, an encrypted disk image can be used to safeguard a single file or a group of files, in addition to (or instead of) using FileVault. The encrypted disk image can reside on the OS X system or on removable media. Users and administrators can follow these steps to create an encrypted disk image:

[39] http://training.apple.com/pdf/WP_FileVault2.pdf

1. Run the Disk Utility and select **File**, then **New**, then **Blank Disk Image**.

2. Enter a name and location for the encrypted image to be stored. Set the size to the maximum that you may need (the size can't be changed after the image is created). Set the encryption to either 128-bit AES or 256-bit AES. After adjusting all the necessary settings, click the **Create** button.

3. Enter a password that will be used for decrypting the disk image. The dialog box provides an option to store the password in the user's keychain. When done with the dialog box, click the **OK** button. The encrypted disk image will be created using the designated name and location.

This technique can be very effective at securing individual files containing sensitive information, such as sensitive personally identifiable information (PII). Discussion of securing files in the form of email attachments is outside of the scope of this publication, but more information (e.g., on S/MIME) is available from NIST SP 800-45, *Guidelines on Electronic Mail Security*.[40]

6.2.2.3 FIPS-Enabled System

OS X automatically runs in FIPS Mode without any required setup since version 10.9[41].

6.2.3 Secure Erase

Section 4.1.1 has already discussed the use of Disk Utility to sanitize media. However, there are other OS X features related to media sanitization. For example, an OS X system can be configured to do a secure erase every time it empties the trash. This is set through **Finder** / **Preferences** / **Advanced**, then enabling the "Empty Trash securely" option. This does a seven-pass overwrite of the files being deleted. Note that this is a per-user setting that individual users can alter without administrative privileges. Administrators should also be aware that this option may cause extended periods of system unavailability while securely deleting large files; for example, deleting a large software package securely could take hours. Therefore, many organizations will not enable the "Empty Trash Securely" option for their Standalone and Managed users, requiring its use only on SSLF systems.

When saving a file to disk, one or more distinct instances of the file may be created; these instances may not be visible to the user when using normal tools, e.g., the Finder. Testing showed that not all instances of a file are erased when using the "Empty Trash securely" option. One or more copies of the contents are erased, but old contents of those files may still exist on the disk. Regardless of whether the "Empty Trash securely" option has been enabled, users can manually choose to invoke the "Empty Trash securely" feature by selecting **Finder** / **Secure Empty Trash**. In order to ensure secure deletion of the contents placed in the Trash, it is recommended to use the "Erase Free Space" option in Disk Utility after deleting the desired files.

---

[40] http://csrc.nist.gov/publications/nistpubs/800-45-version2/SP800-45v2.pdf.
[41] https://support.apple.com/library/APPLE/APPLECARE_ALLGEOS/HT205017/APPLEFIPS_GUIDE_CO_OSX10.10.pdf

Depending on disk size, this may take a long time to complete, so this is recommended for SSLF systems only.

6.2.4 File and Folder Permissions

OS X's file and folder permissions have their roots in BSD Unix; although OS X has significant changes from BSD Unix, file and folder permissions should look familiar to Unix-savvy administrators. Examples include requiring certain critical system files (such as `/usr/bin/sudo`) to be owned by root and group-owned by wheel, setting modes (e.g., `644`, `755`) on particular files and folders, and removing the setuid bit from selected system executables.

The NIST baseline settings restrict access to dozens of OS X system files, protecting them from unauthorized access and modification. Additional custom permission settings may be added that are specific to the environment in which the OS X system resides. Changes to the permissions for a specific file or folder can be made using the command prompt with commands such as `chmod`, `chown`, and `chgrp`. OS X also includes extended access control lists (ACLs), which allow for additional control over file permissions. See Appendix I.2 for more information on ACLs.

Certain tools in the directories `/bin`, `/usr/bin`, `/sbin`, and `/usr/sbin` require their setuid bit to be set in order to function. Many of the tools located in these directories can safely have their setid bits[42] cleared; in this case, a user who runs them must already possess admin level access for them to run normally. Critical system tools that must retain their setuid bit are `/usr/bin/login`, `/usr/bin/sudo`, and `/usr/bin/su`. See Appendix I.1 for a list of recommended file permissions.

6.2.5 Spotlight

Spotlight is a system-wide search capability. It indexes files to facilitate fast searches. However, this indexing can inadvertently capture sensitive information, potentially exposing it to unauthorized access. Organizations should evaluate these risks and determine if particular files or groups of files should be omitted from Spotlight indexing and searching, such as files containing sensitive PII. To specify folders to be excluded, go to **System Preferences**, then **Spotlight**, and select the **Privacy** pane. In this pane, add the folders or disks that should not be searched by Spotlight. Note that users can alter these settings without administrative privileges.

6.3 User Accounts and Groups

This section discusses the configuration settings related to user accounts and groups. The discussion is divided into the following categories: user account types, login options, parental controls, password policies, session locking, credential storage, and alternate credentials.

6.3.1 User Account Types

There are three general types of accounts for users: administrator, standard, and managed. Administrator accounts can do everything. Administrator accounts should only be used for

[42] The term "setid bits" refers to both the setuid and setgid file permissions.

system administration tasks. At least one non-administrator (standard) account should be created for daily operation of the system. A standard account can do things, including installing software, that affect the account owner but not other users. A managed account is just like a standard account, except there are some additional restrictions available (through Parental Controls), most notably which applications are allowed to run. Each user should be utilizing a unique standard or managed account for daily use of an OS X system. User account settings are accessible under the "Users & Groups" pane of **System Preferences**.

NIST recommends that administrators periodically review user accounts and disable those that have been inactive for 90 days, as well as disabling temporary accounts after 30 days. Organizations should also follow procedures to disable accounts as soon as they are no longer needed (e.g., user leaves the organization, user's responsibilities change). Disabled accounts should be deleted after a specific period to release resources and prevent unneeded accounts from accidentally being re-enabled.

There are some special built-in accounts on OS X systems:

- **Guest.** The Guest account, a special managed account, is considered a security vulnerability in most situations because it has no password associated with it. Once an attacker has gained guest-level access, the attacker can try to elevate privileges to further exploit a system. NIST recommends that the Guest account be disabled on all OS X systems unless there is a clearly demonstrated need to use a Guest account. The Guest account is not allowed to log in to a computer by default. However, guest users can access shared folders remotely by default. This setting is called "Allow guest users to connect to shared folders" and should be disabled. Both of these settings are available after selecting the "Guest User" account in the "Users & Groups" pane. Note that when a guest logs out on an OS X system, the guest's environment is destroyed and reinitialized.

- **Root.** The root account is not to be confused with the administrator accounts; root is a separate account that is disabled by default. Root and administrator accounts have similar privileges, but the root account has considerably less overhead associated with it (for example, the person does not have to authenticate repeatedly to issue administrator-level commands when using the root account). The root account is intended for command line access. NIST recommends that the root account be disabled on all OS X systems and that a separate administrator account be established for each person who will be performing regular administrative tasks. The administrator accounts should then use the `sudo` command to perform actions with root level privileges even if the root account is disabled. An administrator uses the `sudo` command to perform system-wide modifications. The root account is the only account with UID 0.

Other types of users include local, external, network, and mobile, but these classifications only refer to the account's physical location and not the associated privilege levels. It is recommended to have all account types hidden from the login screen so that account names are not visible, but it is also useful to understand the available account types. Local user accounts are the default account type and exist solely on the system on which they are created. External accounts are contained within external/removable media, such as a USB hard drive. Network accounts allow a user to login from any system on the network and the user's files on one system are independent

of all the others. Alternatively, network accounts can be configured to use a centralized home folder, which allows access from any networked system. Mobile accounts are similar to network accounts, but the user's home folder contents are synchronized between the different systems. However, even with all account types hidden, FileVault-enabled systems display usernames at the disk unlock splash screen. Additionally, the username is visible on the lock screen if a user has an active session. With FileVault enabled, usernames are only hidden after a user has authenticated with the system and then logged out.

To configure these accounts through the command line, use the commands provided in Appendix J.4.

6.3.2 Login Options

The Login Options pane within the **System Preferences** / **Users & Groups** screen contains several options related to user login, as shown in Figure 7. Sections 6.3.2.1 through 6.3.2.5 provide additional information on several of these options with security or privacy implications.

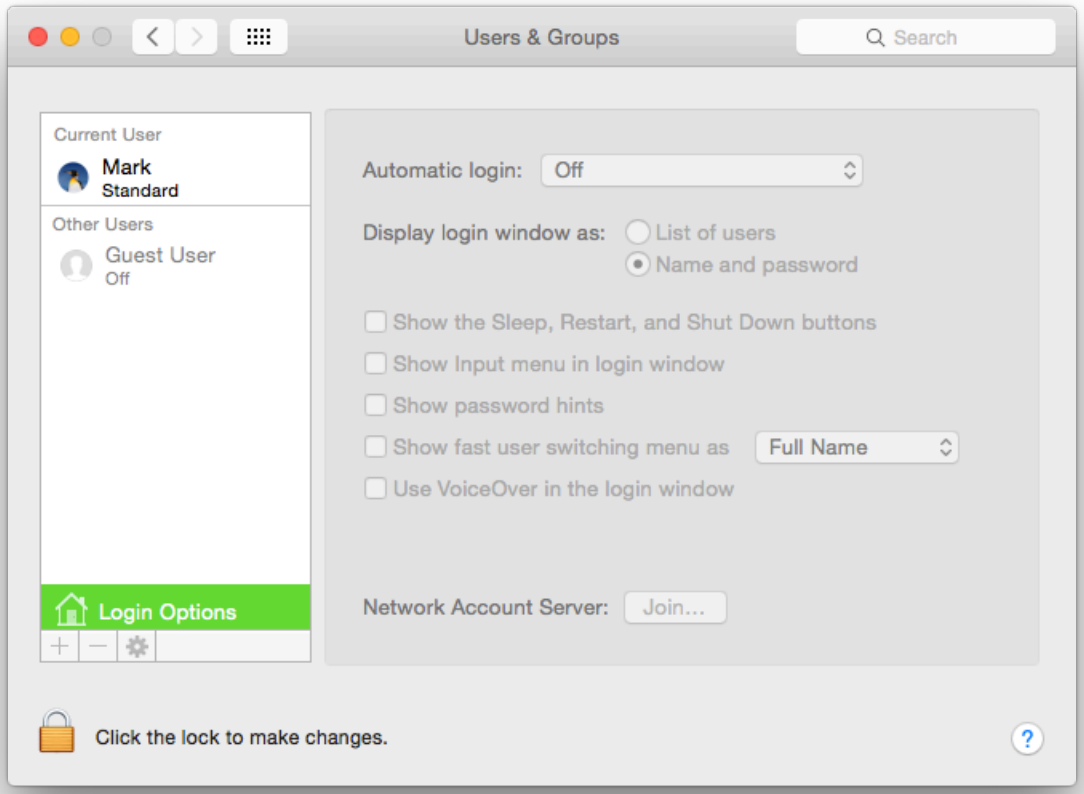

Figure 7: Login Options Pane

The user login options shown in the GUI can also be configured via the command line. The commands for these login-related options can be found in Appendix J.5. Some login window

options are not available to be changed through the GUI. These command line only settings can be configured using the commands in Appendix J.5.

6.3.2.1 Automatic Login

In older versions of OS X, by default the system will automatically log in the administrator every time the system boots. Starting with OS X 10.7, a login is required. The corresponding configuration setting for this is shown at the top of Figure 7, “Automatic login”, and this option is turned off by default. NIST strongly recommends keeping this option disabled.

6.3.2.2 Display Login Window

The second option shown in Figure 7 is “Display login window as”. There are two possibilities: “List of users” or “Name and password”. These refer to what is listed on the screen at login time. Displaying a list of users means that an attacker only needs to recover a password to be authenticated. If name and password boxes are shown instead, an attacker would have to know not only a password, but also the username that corresponds with it. This makes an attack slightly harder, but it also makes login more inconvenient for users. Organizations should weigh the security benefits against the usability impact and decide which setting is best for the circumstances. The NIST baselines set this option to “Name and password”.

6.3.2.3 Restart, Sleep, and Shut Down Buttons

By default, the login window displays buttons to restart, sleep, and shut down the system. This allows someone without an account on the system to alter the system’s state, causing a loss of availability. If this is a concern, the buttons should not be shown in the login window. However, this does not prevent the system from being shut down by any physical power buttons present. NIST recommends removing the buttons, which can be accomplished by unchecking the “Show the Sleep, Restart, and Shut Down Buttons” option shown in Figure 7.

6.3.2.4 Password Hints

One of the options shown in Figure 7 is “Show password hints”. If enabled, this will display password hints that users have created for their accounts to help them remember their passwords. Although this can improve usability, it can also negatively affect security significantly by helping attackers to recover user passwords. As with the Display Login Window option described in Section 6.3.2.2, organizations should consider both security and usability when determining how this option should be set. The NIST baselines disable this option. See Appendix J.5 for the password hint configuration setting.

6.3.2.5 Fast User Switching

The fast user switching feature permits two or more users to be logged into the same OS X system simultaneously. Only one user session is in the foreground at any given time. The usage of fast user switching is beneficial on low-security systems where a user may need brief access to a system that someone else is using, because it preserves security and privacy for both users while minimizing the impact on usability. This is a good alternative to having users share their accounts.

However, on other systems, the risks associated with having multiple users logged in simultaneously may be considered too great, and in such cases the fast user switching capability should be disabled, requiring one user to log out before another user logs in. To disable fast user switching, disable the Figure 7 option involving fast user switching ("Show fast user switching menu"). NIST recommends disabling fast user switching for systems in Managed and SSLF environments that have policies against its use.

6.3.2.6 Network Account Server

The last configuration setting in Figure 7 is for use of an Active Directory domain or an Open Directory server. By clicking on the **"Join…"** button, a computer can be associated with an organization's directory server.

6.3.3 Parental Controls

If Parental Controls are enabled for a user account, a wide variety of restrictions can be placed on what the user can do on the system. This includes restricting which applications may be executed, as described in Section 6.5.2. Other types of restrictions of potential interest for security include the following:

- Which websites the user can visit
- What hours of the day the system can be used by the user
- Whether CDs and DVDs can be burned on the system

6.3.4 Password Policies

In addition to educating users regarding the selection and use of passwords, it is also important to set password parameters so that passwords are sufficiently strong. This reduces the likelihood of an attacker guessing or cracking passwords to gain unauthorized access to the system. The following parameters are specified in the NIST baselines:

- **Maximum password age.** This forces users to change their passwords regularly. The lower this value is set, the more likely users will be to choose poor passwords that are easier for them to remember (e.g., Mypasswd1, Mypasswd2, Mypasswd3). The higher this value is set, the more likely the password will be compromised and used by unauthorized parties.
- **Minimum password length.** This specifies the minimum length of a password in characters. The rationale behind this setting is that longer passwords are more difficult to guess and crack than shorter passwords. The downside is that longer passwords are often more difficult for users to remember and to enter accurately. Organizations that want to set a relatively large minimum password length should encourage their users to use passphrases, which may be easier to remember than conventional passwords.
- **Password complexity requirements.** OS X has several settings that can be used to require a mixture of character types, including uppercase and lowercase letters, digits,

and special characters such as punctuation marks. There is also a setting to ensure that a password does not have a guessable pattern, however informal testing was unable to demonstrate that the setting was effective. These settings can make it more difficult to guess or crack passwords.

- **Enforce password history.** This setting determines how many old passwords the system will remember for each account. Users will be prevented from reusing any of the old passwords. For example, if this is set to 15, then the system will not allow users to reuse any of their last 15 passwords. Old passwords may have been compromised, or an attacker may have invested resources to crack encrypted passwords. Reusing an old password could inadvertently give attackers access to the system.

One of the main challenges in setting account policies is balancing security, functionality, and usability. For example, locking out user accounts after only a few failed logon attempts in a long time period may make it more difficult to gain unauthorized access to accounts by guessing passwords, but may also sharply increase the number of calls to the help desk to unlock accounts accidentally locked by failed attempts from legitimate users. This could also cause more users to write down their passwords or choose easier-to-remember passwords. Organizations should carefully think out such issues before setting OS X account policies.

Note that the OS X 10.10 GUI does not provide any mechanisms for setting password or account lockout policies. Instead, these settings can be accessed via a command prompt using the `pwpolicy` command. Also, some of these settings can be accessed through an OS X server implementation, if that server is managing OS X 10.10 systems. Results were identical between OS X Server via Open Directory and the `pwpolicy` program run on the client workstation.

The `pwpolicy` configuration utility does not appear to apply all of the available password rules typically available in Managed environments. Informal testing was unable to apply the following rules: password cannot contain usernames, minimum age, guessable pattern, failed login reset time, max non-use time before lockout, allow simple value, and invalid login attempts. To deter password guessing attacks, OS X can be configured to lock out (disable) an account when too many failed login attempts occur. Without failed login reset time, a locked account remains inaccessible until an administrator intervenes.

There are two ways to set password policy settings: apply them to specific users or set a global policy. User-specific policies override global policies, so the user policies must either be left unset or be set along with the global policies. Alternatively, on OS X 10.10, existing policies can be cleared on a per-user basis with the command `pwpolicy –u $USER -clearaccountpolicies` before applying global policies to ensure that they affect all users. Use the Terminal commands given in Appendix J.6 to change password policy settings.

6.3.5 Session Locking

It is important to provide protection against unauthorized local access to OS X systems. One such control is to lock the current user's session through automatic or manual means. A screen saver can lock a session automatically after the system has been idle for a certain number of minutes, requiring the user to authenticate before unlocking the system. NIST strongly

recommends using an authentication-enabled screen saver on all OS X systems that need protection from unauthorized physical access. Settings for enabling a screen saver (which is accomplished by setting a "start after" time other than "Never") are located in **System Preferences** under the **Desktop & Screen Saver** icon, in the **Screen Saver** pane. NIST recommends that the screen saver be set to start after 20 minutes of idle time. However, if values other than 1, 2, 5, 10, 20, 30, or 60 are used, the value will be reset to 20 if the **Screen Saver** preferences pane is opened. Depending on the accessibility of the system and its environment, a different value may be more suitable.

Other screen saver options for locking are located under **System Preferences** / **Security & Privacy**, in the **General** pane. To require locking, enable the option to "Require password after sleep or screen saver begins" and set it to "Immediately" or "5 seconds". From a security perspective, these are roughly equivalent; from a system usability perspective, setting it to "5 seconds" may be much more convenient for users than setting it to "Immediately," while not significantly impacting security. There is also an option for the login window screen saver that can be configured through the command line. Note that users can alter any of the screen saver options and that these options are set per user, not per system.

Users can also manually lock their sessions. A user can put the cursor over a designated "hot corner" of the screen to automatically lock the system, if this has been configured (using the **Desktop & Screen Saver** icon under **System Preferences**). In order to improve ease of access, use of a modifier key in conjunction with the start screen saver hot corner is not recommended. Users are cautioned not to designate any of the hot corners as "Disable Screen Saver" or "Put Display to Sleep", because this could inadvertently reduce security.

There is another option that only administrators can set related to session locking. Under **System Preferences** / **Security & Privacy**, click the "Advanced…" button and uncheck the option to "Log out after x minutes of inactivity". If checked, this option could cause users' work in progress to be lost. It is more user friendly to have a password-protected screen saver instead of the inactivity log out option.

Session-locking settings can also be configured through the command prompt. See Appendix J.7 for NIST recommendations on the Standalone, Managed, and SSLF profiles for session locking settings.

6.3.6 Credential Storage

Section 3.4 has already described the OS X feature known as keychains. Although keychains are a valuable security feature, by default they are not configured as securely as they should be.

By default, the user account and primary keychain have the same password set. Additionally, the primary keychain is unlocked when the user logs in (since the passwords are the same). To set a different password for the primary keychain, run the **Keychain Access** utility, and choose the primary keychain from the list of keychains. Click on **Edit**, then **Change Password for Keychain**, and change the keychain's password. Note that this may impact some core services that use the keychain, such as the caching of the encryption passphrases for wireless networks. NIST recommends separating daily-use passwords from those used for sensitive information

access. Creating a separate keychain can be accomplished by clicking the "+" icon at the bottom of the **Keychain Access** window.

By default, keychains do not automatically lock when a system sleeps. This increases the risk of unauthorized disclosure or modification of keychain data. To correct this, run the **Keychain Access** utility and choose the primary keychain from the list of keychains. Click on **Edit**, then **Change Settings for Keychain**, and select the "Lock when sleeping" option. A related setting found on the same menu, "Lock after x minutes of inactivity", causes the keychain to lock after it has not been used for a certain number of minutes. NIST recommends that the keychain locks when the screen saver starts.

6.3.7 Alternate Credentials

OS X supports the use of alternate credentials for logical user authentication; examples include token-based authentication, biometric-based authentication, and Personal Identity Verification (PIV) cards[43]. As shown at the bottom of Figure 7, there is a **Network Account Server** option in the **Users & Groups** window. Clicking on the **Join…** button opens a window for specifying the Open Directory or Active Directory server that should be used for alternate credentials. If the server name is not known, or additional options are needed, click on the **Open Directory Utility…** button to run the Directory Utility application.

If alternate credentials are not being supported and there is no other reason to enable directory services, then directory services should be disabled to prevent their possible abuse and exploitation. A common example is Standalone systems, which often do not bind to any directories.

6.3.8 Sudo

The `sudo` program allows an account with administrator privileges to perform an action as the super user (root). This is very powerful functionality and its use needs to be controlled. Options related to `sudo` are located in `/private/etc/sudoers` and can be modified using the `visudo` command. NIST recommends requiring user authentication for each invocation of the `sudo` command. Additionally, `sudo` authentications should be restricted to a single Terminal session. These settings can be found in Appendix J.4.

The `su` command is similar to the `sudo` command. If it is not passed any parameters, it prompts for login to the root user account, and gives root access. The command also allows login to other users by passing in the desired username as a parameter.

6.4 Auditing

This section discusses OS X 10.10's configuration settings related to auditing (logging). Systemwide security auditing is enabled by default and testing did not reveal a method for disabling it.

---

[43] The support for PIV card readers on OS X is still evolving.

6.4.1 Audit Policies and Tools

OS X 10.10's auditing capabilities are based on `syslogd`. OS X logs contain error messages, audit information, and other records of activity on the system, which can be graphically displayed using the Console utility built into OS X and via the `praudit` command line utility. Only administrators can use these tools to read log files.

The Audit control file, `/etc/security/audit_control`, contains the policies for system auditing. Audit logs must be maintained for a sufficient amount of time—30 days—and must record all security-relevant events. The max recommended size per audit file is 80 MB. The audit event flags in Table 1 are recommended:

Table 1: `audit_control` Flags

`audit_control` Flag	Flag Description
`lo`	Login and logout events
`ad`	Administrative events
`-all`	All failed events
`fd`	File deletion events
`fm`	File attribute modify events
`^-fa`	Do not log failed file attribute access events
`^-fc`	Do not log failed file creation events
`^-cl`	Do not log failed file closure events

The logs on each system should be reviewed on a regular basis; the logs can be used not only to identify suspicious and malicious behavior and investigate security incidents, but also to assist in troubleshooting system and application problems. Therefore, it is important to enable logging and to specify the log retention time for various system logs for all environments. If the log retention time is very low, the system will not store as much information on system activity. Some organizations may have a logging policy and central log servers, so the baseline settings may need to be adjusted so they comply with the policy.

For more information on `syslogd`, including its own security, see NIST SP 800-92, *Guide to Computer Security Log Management.*[44]

6.4.2 Date and Time Setting

It is important to configure OS X systems to synchronize their clocks on a regular basis with accurate time sources. If audit logs contain evidence of an attack and the system's clock is inaccurate, it makes the analysis of the attack more difficult and may also weaken the evidentiary value of the logs. Time synchronization is also convenient because users do not need to manually adjust the clock to compensate for inaccuracies in the system's timekeeping. OS X uses the Network Time Protocol (NTP) for time synchronization.

[44] http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf

To configure a OS X host to use NTP, choose **System Preferences**, then **Date & Time**. Enable the "Set date & time automatically" option and enter the name of the organization's designated NTP server (or select one of the Apple-provided default time servers). If there is more than one designated NTP server, their names can be entered as a list, separating each entry from the others with a space. Figure 8 below shows the Date & Time settings panel.

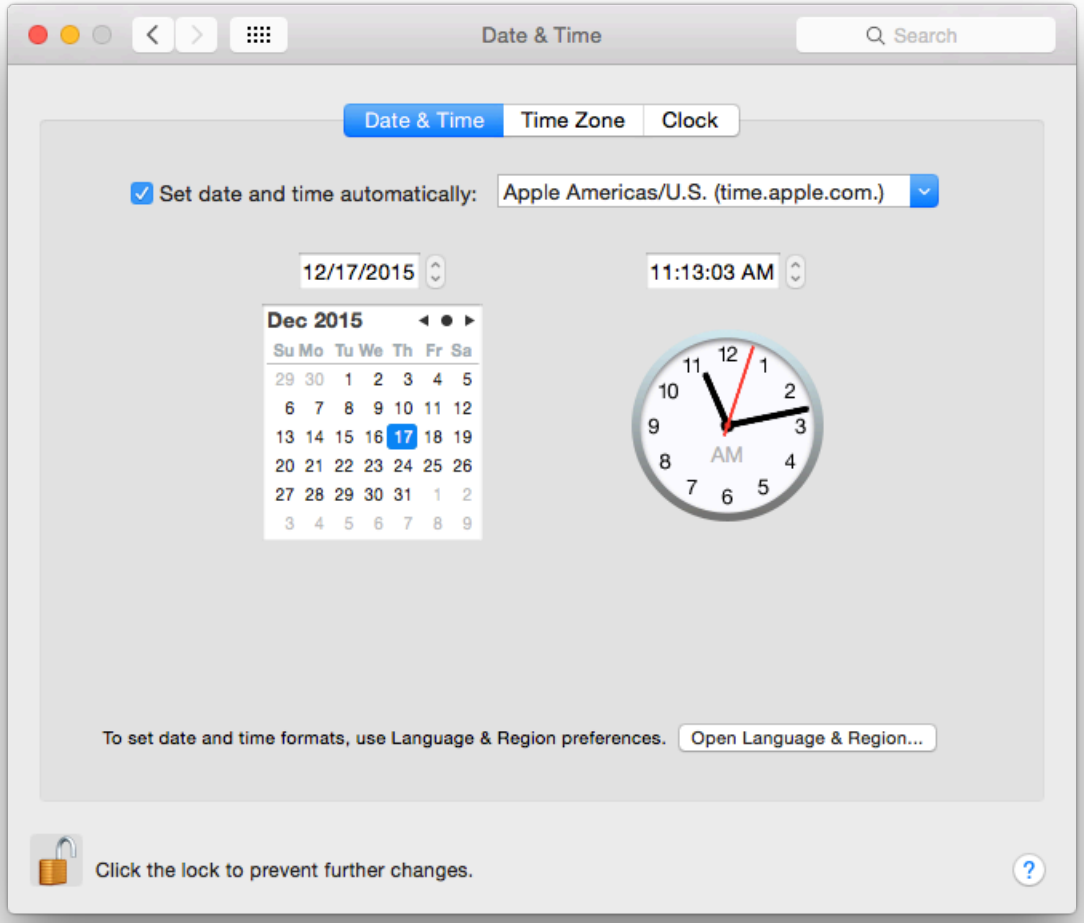

Figure 8: Setting the NTP Servers

To set a time server and to enable automatic updating of time, use the commands in Appendix J.12.

6.4.3 System Crash and Panic Reporting

Crash and panic reports should be monitored to prevent potentially sensitive data from being written to unencrypted files. These reports are meant to provide diagnostic information regarding

system crashes and panics. The reports are located in `/Library/Logs/DiagnosticReports`. If an organization does not plan to use the files for diagnostic purposes, the files should be periodically deleted to conserve disk space and limit the possibility of exposing sensitive information. OS X does not seem to allow these to be disabled.

6.5 Software Restriction

OS X offers multiple ways of restricting the execution of software; see Section 3.1 for additional information. This section briefly looks at two methods of limiting software execution: Gatekeeper and Parental Controls. Gatekeeper restricts which applications may be installed onto a system, while Parental Controls restricts which applications already installed on a system may be run by a user.

6.5.1 Gatekeeper

Gatekeeper's configuration options are not marked as pertaining to Gatekeeper, but rather are all bundled in the **System Preferences** / **Security & Privacy** / **General** pane. This pane has three options related to "Allow applications downloaded from", as described in Section 3.1. By default, the option to limit downloads to "Mac App Store and identified developers" is enabled. To disable Gatekeeper, select the "Anywhere" option. To use the strictest Gatekeeper controls, select the "Mac App Store" option. These options are shown in Figure 9 below.

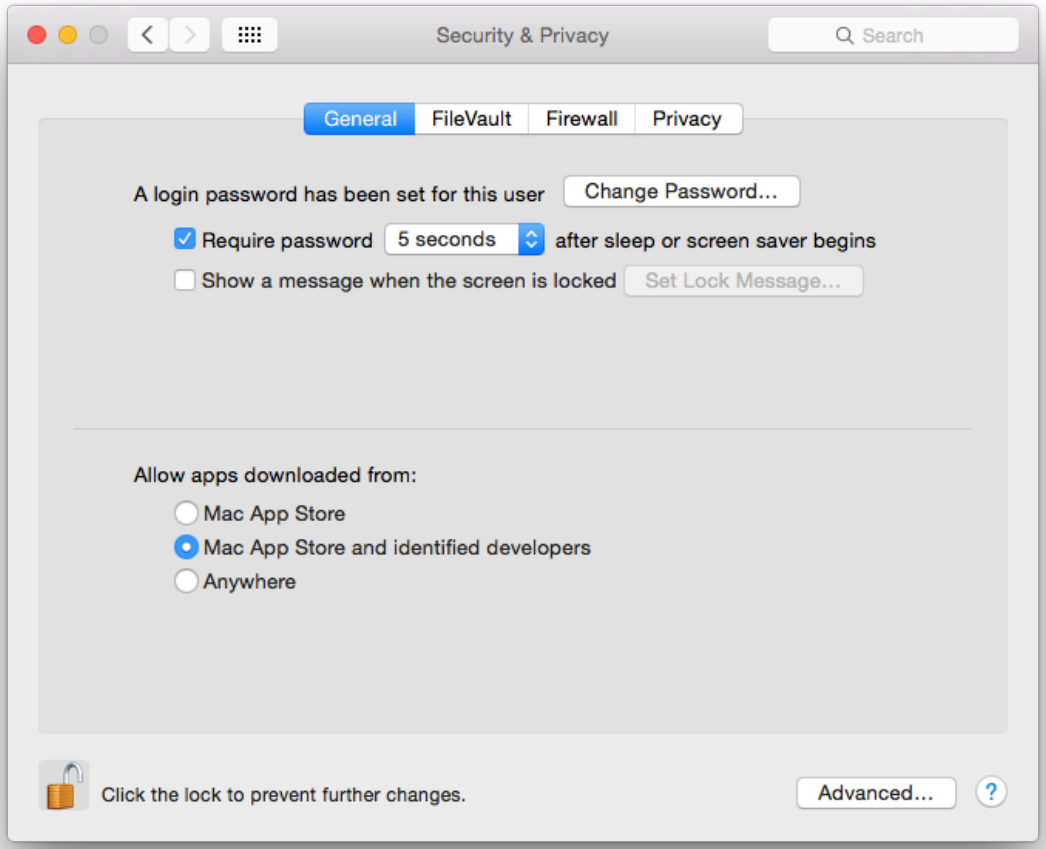

Figure 9: Gatekeeper Options

6.5.2 Parental Controls

Parental Controls can be used to specify which installed applications may be executed through the "Limit Applications" option in the **System Preferences** / **Parental Controls** window. If the Limit Applications option is enabled, a user will be unable to run an application unless an administrator has added it to the list of permitted applications for that user. The administrator can also configure each user account so that it can or cannot use apps from the Mac App Store, either altogether or based on age ratings.

6.6 Network Services

This section discusses security issues related to network services. The information is organized into the following categories: firewalls, sharing, IPv6, the SSH daemon, wireless networking, and Bonjour. For network service configuration commands, see Appendix J.12.

6.6.1 Firewalls

Both built-in firewalls, the application firewall and the stateful inspection firewall, are disabled by default. To enable the application firewall, go to **System Preferences**, then **Security & Privacy**, and select the **Firewall** pane. Click the "Turn On Firewall" button. There are four additional options under the "Firewall Options..." button:

- **Block all incoming connections.** This blocks all incoming traffic except for a few protocols, such as DHCP, that may be needed for basic system services to function. This setting provides a high level of network security while possibly negatively impacting functionality. Before using this setting in production, perform testing to determine how this setting affects all major applications on the system.

- **Enable selected applications.** Once the user has authenticated as an administrator (by clicking the lock and providing the username and password), specific applications can be authorized to accept incoming connections (subject to also being allowed by the `pf` firewall described below).

- **Automatically allow signed software to receive incoming connections.** This option is only available if "Block all incoming connections" is disabled.

- **Enable stealth mode.** This option is only available if "Block all incoming connections" is disabled. This option prevents the system from responding to pings, traceroutes, and other similar diagnostic tools.

Enabling the stateful inspection firewall (`pf`; see the `pfctl` man page) is ineffective unless its ruleset has been configured, because by default the `pf` ruleset does not block any network traffic. A detailed explanation of how to configure a `pf` ruleset is outside the scope of this publication. Table 2 presents a recommended `pf` ruleset. This ruleset should be altered depending on an organization's networking service needs.

Table 2: `pf` Firewall Services and Ports

Service Name	TCP Port(s)	UDP Port(s)	Direction
FTP	20, 21	20, 21	Incoming
SSH	22	22	Incoming
telnet	23	23	Incoming
rexec	512	512	Both
RSH	514	514	Both
TFTP	69	69	Both
finger	79		Both
HTTP	80	80	Incoming
NFS	2049		Both
Remote Apple Events	3031		Incoming

SMB	139, 445	137, 138	Both
Apple File Server	548		Incoming
UUCP	540		Both
Screen Sharing	5900		Incoming
ICMP	7	7	Incoming
SMTP	25		Incoming
POP3	110		Incoming
POP3S	995		Incoming
SFTP	115		Incoming
IMAP	143		Incoming
IMAPS	993		Incoming
Printer Sharing	631		Incoming
Bonjour		1900	Both
mDNSResponder		5353	Both
iTunes Sharing	3689		Both
Optical Drive Sharing	49152		Both

The various application firewall settings can be changed via the command line with the commands given in Appendix J.8.

6.6.2 Sharing

By default, all sharing is disabled. There are several different types of sharing, as shown in Figure 10, including screen, file[45], printer, Internet, and Bluetooth. Other systems may have slightly different lists of sharing, based on their hardware characteristics (for example, systems with optical drives will have a "DVD or CD Sharing" option). For all the sharing services, there may be names or directories listed; however, this does not imply that the service is enabled. Note that this list also includes three options for remote access to an OS X system:

- **Remote Login.** The Remote Login feature allows Secure Shell (SSH) and Secure FTP (SFTP) connections to be made to the OS X system from other systems. By default, SSH and SFTP are disabled, and organizations should not enable them unless they are needed for system maintenance, access, etc. because they are additional attack vectors into a system.

- **Remote Management and Screen Sharing.** Remote Management and Screen Sharing both allow remote operation of a computer. These services would be required for a technical support person to remotely see an OS X system's screen from another system. Since both settings allow external control of a system, they should be disabled unless

[45] File sharing includes options for sharing files and folders using the Apple Filing Protocol (AFP), File Transfer Protocol (FTP), or Server Message Block (SMB) protocol.

needed.

- **Remote Apple Events** (logging of events from other OS X systems on this system). This feature is intended to be used when a system is acting as a server, not a desktop or laptop. In most cases, it should be disabled.

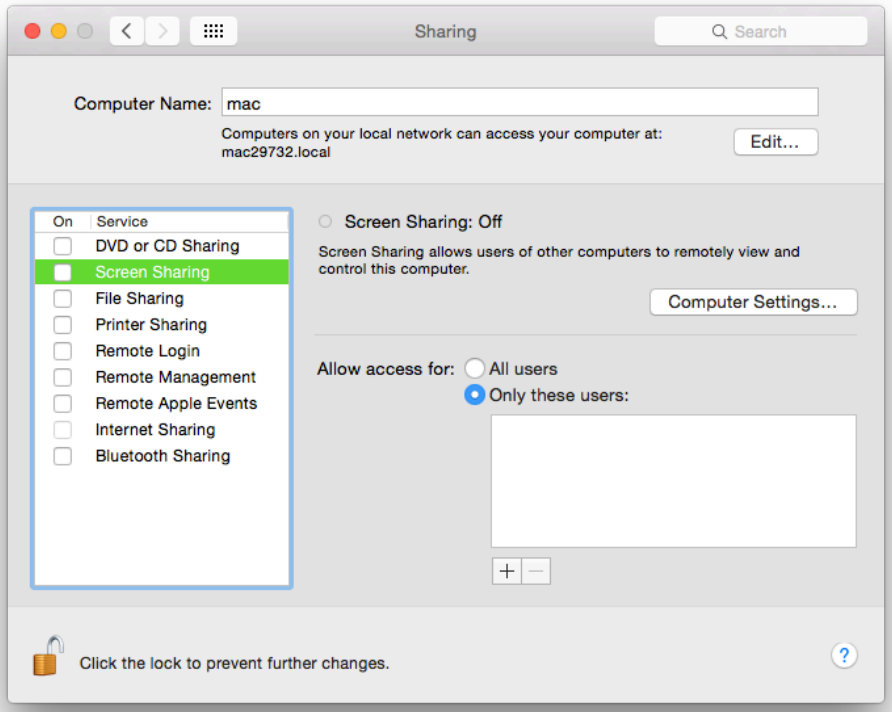

Figure 10: Sharing Options

To reduce the number of attack vectors against a system, all sharing and remote access services should be disabled unless explicitly needed. To enable a needed service, go to **System Preferences**, then **Sharing**, and enable (turn on) the appropriate service. Computer names are used for networking purposes, and are helpful for users to differentiate between machines. Computer names should not have content that identifies any of its users. To configure computer name settings, see Appendix J.12.

Sharing will only work if the firewall or firewalls are configured to permit it. For example, the built-in application firewall has an option called “Block all incoming connections”. If enabled, this will disable all sharing. To alter the setting for this option, go to **System Preferences**, then **Security & Privacy**, and select the **Firewall** pane. Click the “Firewall Options…” button and change the setting as appropriate for the “Block all incoming connections” option.

OS X also has individual configuration settings for sharing each local printer. If a system has local printers, these printers should not be shared remotely unless they need to provide printing services to other systems. To disable sharing for a printer, choose **System Preferences**, then

Printers & Scanners, and for each local printer, deselect the "Share this printer on the network" option. Note that when the "Share this printer on the network" option is enabled, this also enables the Printer Sharing option in the **Sharing** window of **System Preferences**.

There is another form of OS X sharing that is not included in the Figure 10 menu: AirDrop. AirDrop is a peer-to-peer file sharing service. AirDrop is only available on certain Apple hardware that supports it, and it requires the use of Wi-Fi. AirDrop is only enabled when the user specifically has it open (**Finder**/**Go**/**Airdrop**). When open, AirDrop automatically scans for other AirDrop-enabled systems with Wi-Fi range. However, files are not transferred unless a user specifically authorizes the transfer.

NIST recommends that if any sharing services are enabled, they should be protected by another layer (such as a host-based firewall) that restricts access to the service. Allowing global access to any form of sharing is not recommended.

To disable sharing services via the command line, use the commands provided in Appendix J.9.

6.6.3 IPv6

If IPv6 is not needed, it should be disabled to reduce the possible attack vectors into the system. To effectively disable IPv6, go to **System Preferences**, then **Network**. For each network interface that should not be using IPv6, perform the following steps: Click on the "Advanced…" button. Go to the TCP/IP pane, then the "Configure IPv6" popup menu, and choose the "Link-local only" option. Technically this does not completely disable IPv6, but it configures it in such a way that it is not accessible from other systems.

6.6.4 SSH Daemon

NIST recommends that the Secure Shell (SSH) daemon (`sshd`) be disabled in all environments unless specifically needed. The NIST baselines also contain several settings to make `sshd` more secure; these settings should be applied whether or not `sshd` is enabled just in case it becomes enabled inadvertently or is needed in the future.

The table in Appendix J.10 lists some of the possible settings that can be configured for the SSH daemon. This is not a comprehensive list of all changes that should be made to secure SSH. The settings exist in the `/etc/sshd_config` file as key-value pairs in the format of "key value."

For additional information on SSH security, see NIST IR 7966, *Security of Interactive and Automated Access Management Using Secure Shell (SSH)*.[46]

6.6.5 Wireless Networking

Any wireless networking services (e.g., Wi-Fi, Bluetooth) that are not needed should be disabled. See Section 6.1.2 for more information on disabling hardware interfaces. For wireless networking services that are enabled, NIST recommends reviewing their configuration options

[46] http://dx.doi.org/10.6028/NIST.IR.7966

and locking them down to the greatest extent possible. Recommendations for these services can be found in Appendix J.11.

Configurable Bluetooth settings include: Bluetooth devices can wake the computer, Bluetooth assistant for mouse and keyboard, toggled state on menu bar, and file sharing. For example, the Bluetooth option "Allow Bluetooth devices to wake this computer" is beneficial if the system is using Bluetooth input devices (keyboard, mouse), but otherwise poses risk without providing benefit. The Bluetooth discoverability by other devices setting is not manually configured through the **System Preferences** or the command line. The setting automatically toggles to "on" when the Bluetooth pane is opened under **System Preferences**.

Wireless settings can also be configured, and these settings include: preferred networks, toggled state on menu bar, and AirDrop. One setting that can be configured through the **System Preferences** is "Require administrator authorization to: Create computer-to-computer networks". Such an option should be enabled unless users specifically require this privilege and do not have administrator-level access. This type of setting is located under the **Network** pane of **System Preferences**.

For additional information on wireless networking security, see NIST SP 800-153, *Guidelines for Securing Wireless Local Area Networks (WLANs)*[47] and NIST SP 800-121 Revision 1, *Guide to Bluetooth Security*[48].

6.6.6 Bonjour

Bonjour multicast advertisements should be disabled in all environments except Standalone. Bonjour advertises the system's capabilities, which opens it to attack. It allows other systems running Bonjour to detect a system and any services that it provides. By disabling Bonjour multicast advertisements, only the service announcements are being disabled and not the services themselves. For information on disabling Bonjour advertisements, go to Appendix J.12.

6.6.7 DNS Servers

NIST recommends that systems be configured to use at least two DNS servers. This provides redundancy in the event of a failure. A failure in name resolution could lead to the failure of security functions requiring name resolution, which may include time synchronization, centralized authentication, and remote system logging. Command line configuration is available in Appendix J.12.

6.7 Applications

This section provides basic information on securing commonly used built-in OS X applications, namely Mail (email client) and Safari (web browser).

---

[47] http://dx.doi.org/10.6028/NIST.SP.800-153
[48] http://dx.doi.org/10.6028/NIST.SP.800-121r1.

6.7.1 Mail

Email has become a popular means for malware propagation. Careful configuration of email clients is important not only to protect a given system, but also to prevent the propagation of malware from the system to other systems.

Examples of security-related settings for the built-in Mail client are listed below. Note that the validity of these settings will vary from organization to organization, depending on the email server infrastructure and the security needs versus functionality needs.

- Under **Mail**, select **Preferences**, then go to the **Accounts** pane. Under the **Advanced** tab, enable the "Use SSL" option. This will protect the POP or IMAP (incoming) email communications with the SSL/TLS protocol. Note that this option will not protect SMTP (outgoing) email communications; to protect them as well, go to the **Accounts** pane and set up the **Outgoing Mail Server (SMTP)** to **Use Secure Sockets Layer (SSL)**.

- Under **Mail**, select **Preferences** and choose the **Junk Mail** pane. Enable the "Enable junk mail filtering" option. There are other options available that support junk mail filtering, such as defining what actions should be performed when junk mail is received and determining which categories of messages should not be flagged as being junk mail (e.g., from certain senders).

- Under **Mail**, select **Preferences** and go to the **Viewing** pane. Security-related options in this pane include **Use Smart Addresses**, which if disabled will show email addresses instead of names, and the **Display remote images in HTML messages** option, which if disabled will prevent possibly objectionable or malicious images from being displayed in HTML-based email messages.

6.7.2 Safari

Web browsing is a common way for malware to infect systems and otherwise take advantage of systems. It is important to configure web browsers with security in mind, particularly in higher-security environments (e.g., SSLF), otherwise the web browser may provide an easy way for malware to infiltrate a system.

Examples of security-related settings for the built-in Safari web browser are listed below. Note that the validity of these settings will vary from organization to organization depending on security needs versus functionality needs.

- Under **Safari**, select **Preferences** and choose the **General** pane. There is an option titled **Open "safe" files after downloading**, which is enabled by default. The intention of this option is to allow automatic opening of file types that are unlikely to include malicious content; however, the list of file formats includes PDFs, which have been known to contain malicious content. This option should be disabled unless all downloads are being scanned by antivirus software.

- Under **Safari**, select **Preferences** and choose the **AutoFill** pane. One of the options is for autofilling **User names and passwords**. AutoFill should be disabled.

- Under **Safari**, select **Preferences** and click on the **Security** pane. There are several security-related options under this pane, including the following:
  - **Warn when visiting a fraudulent website** will do as the name implies, so it should typically be enabled.
  - The option to **Block pop-up windows** should generally be enabled because of the frequency with which pop-up windows have been used to transmit malicious content. In some cases, however, a mission-critical web application will use popup windows; in this case, pop-up windows should be temporarily allowed only while the critical web application is being used.
  - There are options to **Enable plug-ins** and **Enable JavaScript**. Under the **Plug-in Settings** menu, there is a checkbox to enable Java. Organizations should consider disabling some or all of these options for high-security needs (e.g., systems in SSLF environments).
- Under **Safari**, select **Preferences** and open the **Privacy** pane. There are several privacy-related options, as shown in Figure 11.

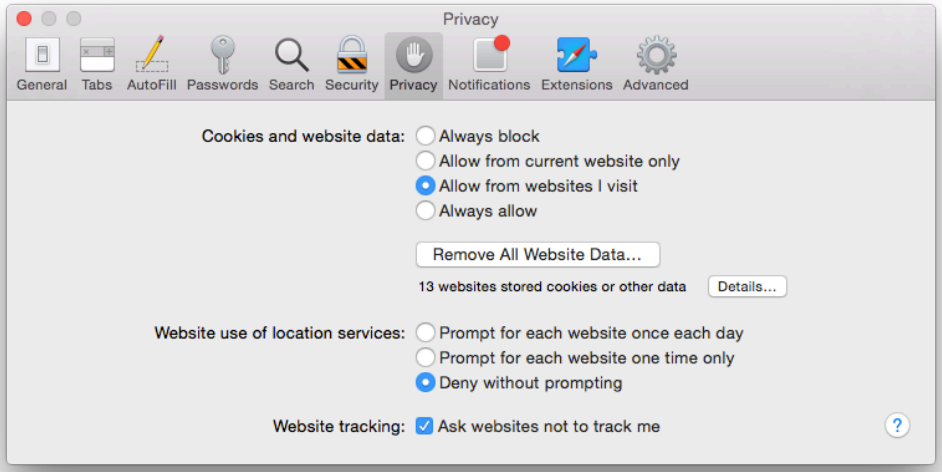

Figure 11: Privacy Options

Safari can be configured to show its status bar, and the command-line option is located in Appendix J.17. This is useful for confirming the underlying web address for a hyperlink.

6.7.3 Configuring Software Updates

Many software update settings can be configured using a command prompt. Available system updates can be displayed and applied using the `softwareupdate` tool in a similar manner to the Mac App Store GUI. These settings are described in Appendix J.13.

6.8 Other Security Management Options

This section discusses security management options not covered in the other parts of Section 6, such as configuring CD and DVD preferences, login banners, privacy settings, and virtualization.

6.8.1 CD and DVD Preferences

There can be security risks in automatically performing actions when a CD or DVD is placed into an OS X system. If the CD or DVD contains malicious content, that content could be automatically run. Automatic options can be disabled through the **CDs & DVDs** icon under **System Preferences** by choosing the "Ignore" option for each type of media. Note that the settings are not visible if there is no optical drive, but will appear if a supported external drive is attached. These settings can also be configured through the command line using the commands described in Appendix J.14.

6.8.2 Login Banners

Login banners are often used to warn people of the possible legal consequences of misuse of a system. There are two ways to set up login banners for OS X:

- Set the text for the login window access warning. This option is best suited for short login banners (three lines or less). See http://help.apple.com/securityguide/mac/10.7/#apdC3C3745F-3036-4531-9697-D24F6FB5EC3C for instructions on implementing this option.

- Create a policy banner file that contains the text of the banner. The file must be located at `/Library/Security`, and it must be named `PolicyBanner` with a file extension of `.txt`, `.rtf`, or `.rtfd`.[49]

There may also be a need to set up a warning banner for command line access (both remote and local). For instructions on setting up such a banner, see http://help.apple.com/securityguide/mac/10.7/#apdA5B369D5-9A06-421D-8DB2-B086BA657BDA.

6.8.3 Privacy

General privacy settings are available through the **Privacy** pane under **System Preferences** / **Security & Privacy**. These settings are divided into three categories:

- **Location Services.** The "Enable Location Services" option will enable or disable the use of location services. To preserve privacy, it is generally recommended to disable location services unless there is a specific reason to have them enabled. If location services are enabled, only the necessary applications should have access to location information. This can be configured through the same menu.

[49] http://help.apple.com/securityguide/mac/10.7/#apd07CB9812-3682-4522-9F9D-147774DF4733

- **Contacts.** This setting is comprised of a list of applications that have requested access to the Contacts information. Contacts access can be revoked by unchecking the permission box for a specific application. Only the necessary applications should have access to contact information, in order to protect it from unintended disclosure.

- **Diagnostics & Usage.** This category holds two configuration settings: "Send diagnostic & usage data to Apple" and "Share crash data with app developers". According to the descriptions presented to the user, all data is anonymized before being sent to Apple and app developers. By default, these settings are disabled, and the NIST baselines agree. These settings require administrator-level credentials to enable.

Privacy settings can be configured through the command line as described in Appendix J.15.

6.8.4 Virtualization

An OS X "system" can be run as a virtual machine instance (a guest operating system). This can provide additional isolation for activities occurring within the virtual OS X system. For more information on the use of full virtualization, see NIST SP 800-125, *Guide to Security for Full Virtualization Technologies*[50].

6.8.5 Other System Preferences

This section discusses additional settings including administrator access for preferences, dock auto-hide, and Dashboard.

6.8.5.1 Administrator Access for Preferences

Not all system preferences require an administrator password to be changed. In particular, all systemwide settings should require administrator authentication. This setting is found in the **System Preferences** / **Security & Privacy** pane, after clicking the **Advanced…** button at the bottom of the window. This is shown in Figure 12 below.

[50] http://dx.doi.org/10.6028/NIST.SP.800-125.

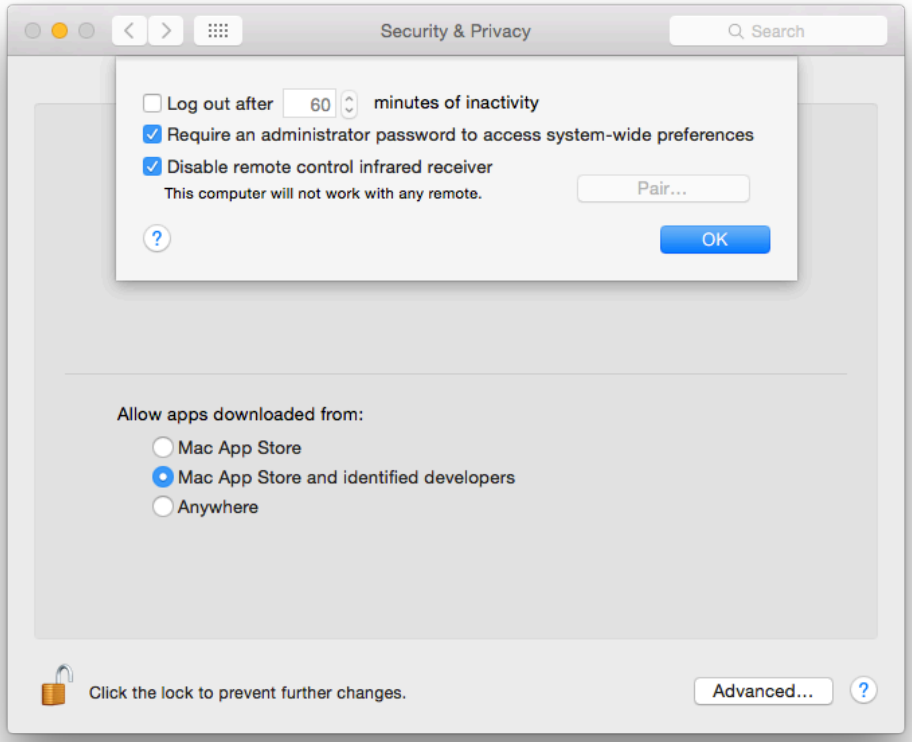

Figure 12: Administrator Access for Systemwide Preferences

This can be changed by using the `security` tool. Making the change through the command line requires the use of a temp file. The process is described below:

1. Run the command `security authorizationdb read system.preferences > $tmp_file` to get the `.plist` file associated with the setting in the database.

2. Run `defaults write $tmp_file shared -bool false` to modify the setting value to require the administrator password for system-wide preferences.

3. Write the `.plist` file contents back into the database by running `security authorizationdb write system.preferences < $tmp_file`.

6.8.5.2 Dock

To change Dock preferences, go to the **Dock** pane under **System Preferences**. The terminal command to configure Dock auto-hide is available in Appendix J.17.

6.8.5.3 Dashboard

The Dashboard is disabled by default on OS X 10.10. Updates to Dashboard widgets may pose a security risk, so NIST recommends that the Dashboard remains disabled. However, enabling it

does not require administrator permission. The terminal commands for the Dashboard are available in Appendix J.17.

6.9 Summary of Recommendations

- Each hardware interface creates a potential point of attack, so an organization may determine that one or more of these interfaces are unnecessary and therefore should be disabled. However, the available methods of disabling hardware interfaces are not foolproof, so on such hosts the disabled interfaces should be continuously monitored to detect any restoration.

- Only rely on EFI passwords to provide security if the physical security of the system is assured.

- Use FileVault 2 full disk encryption on system drives and use Disk Utility to encrypt disk images on removable media.

- Periodically use the Disk Utility to securely erase the system's free space.

- Make sure to properly sanitize storage media before disposal.

- Only use administrator accounts for system administration tasks. Each user should utilize a unique standard or managed account for daily use of OS X systems.

- Administrators should periodically review user accounts and disable those that have been inactive for 90 days, as well as disabling temporary accounts after 30 days. Organizations should also follow procedures to disable accounts as soon as they are no longer needed. Disabled accounts should be deleted after a specific period of time to release resources and prevent unneeded accounts from accidentally being re-enabled.

- Disable the guest user account.

- The Root account should be disabled on all OS X systems and a separate administrator account should be established for each person who will be performing regular administrative tasks.

- NIST strongly recommends keeping the "Automatic login" option disabled.

- Implement and enforce a strong password policy.

- Use an authentication-enabled screen saver on all OS X systems.

- Carefully think out usability issues before setting OS X account policies.

- Configure and monitor logs for undesired system activity.

- Configure OS X systems to synchronize their clocks on a regular basis with accurate time sources.

- Configure firewalls to block undesired traffic.
- If IPv6 is not needed, disable it to reduce the possible attack vectors into the system.
- Disable any unneeded sharing services. Protect active sharing services with restrictive access measures, such as a host-based firewall.

7. Putting It All Together

This publication covers many topics related to the security of OS X systems. The purpose of this section is to put it all together by describing the basic process that IT professionals should follow to use this publication and the accompanying baselines. The primary steps are as follows:

1. Read the entire publication, including the appendices. As needed, review the additional reference material listed throughout the publication and in Appendix D.

2. As discussed in Section 4, install and patch the OS and applications on test systems, and create and test plans for system backups and restores.

3. Refer to Section 2 to review the system threats, then select the appropriate operating environment. Review the security baseline and the settings spreadsheet columns corresponding to that environment. Refer to Section 6 as needed for more information on the different regions and values within the baseline.

4. Modify the baseline to reflect local policy and apply it to test systems using the appropriate deployment tool, as described in Section 5. Create multiple versions of the baseline if necessary to address multiple system roles or environments. Refer to Appendix C and Appendix D for other tools that may be useful for deployment.

5. Augment the baseline with additional controls presented in Section 6, as well as any others that are required based on the local environment. Also, apply application-specific security configuration changes.

6. Verify that the controls have been deployed properly by testing system functions and security controls, as described in Sections 2.6 and 5.4. Modify and document any changes made to the baseline security controls (e.g., altering a setting so a particular application can function properly). Modify the baselines as necessary to incorporate changes that apply to all systems.

7. Perform another round of testing in a test environment before deploying the baselines and other changes to production systems.

8. Deploy the baselines and additional controls to production systems. Verify that the controls have been deployed properly by testing system functions and security controls.

9. Maintain the systems, as described in Section 2.7 This includes keeping systems updated (Section 4.3), monitoring the system's primary security controls (Section 5.4), performing periodic or continuous vulnerability assessments (Section 5.4), and monitoring the various logs described throughout the publication.

Appendix A. NIST Security Configurations

Appendix A briefly discusses the NIST security baselines and settings spreadsheets.

NIST produced a list of settings that are important for ensuring the security of an OS X system. These settings correspond to three different environments—Standalone, Managed, and SSLF. All of these settings are documented in a spreadsheet with the following columns:

- **Grouping in the Script.** The group numbering of this particular setting. Similar settings typically share a group.
- **Function.** The category of the setting as seen in Figure 13.
- **Setting Name.** Combines with the CCE ID to produce the function name in the script.
- **Description.** A user-friendly explanation of the setting.
- **CCE IDv5.** The unique Common Configuration Enumeration (CCE) ID value assigned to each setting.
- **Security Baseline.** The human-readable setting value for each environment profile.
- **Technical Mechanism.** The in-depth explanation of how to apply the setting.
- **Read Setting State. A** command-line statement used to read the current state of the setting.
- **Write Setting State.** A command-line statement used to write the new value for the setting.
- **Standalone, Managed, and SSLF (Environment-Specific Value).** Specifies the setting baseline value for Standalone, Managed, and SSLF.
- **STIG ID.** Corresponding setting in the 10.10 DISA STIG.[51]
- **Rationale.** Security considerations that this setting addresses.
- **Reference.** Any references providing more information for the setting.

The spreadsheet and other associated materials can be found in Appendix D.

Figure 13 gives an illustrative overview of the setting categories covered by this guide. The number of settings for a category does not imply increased importance of one category over another.

[51] http://iase.disa.mil/stigs/os/mac/Pages/index.aspx

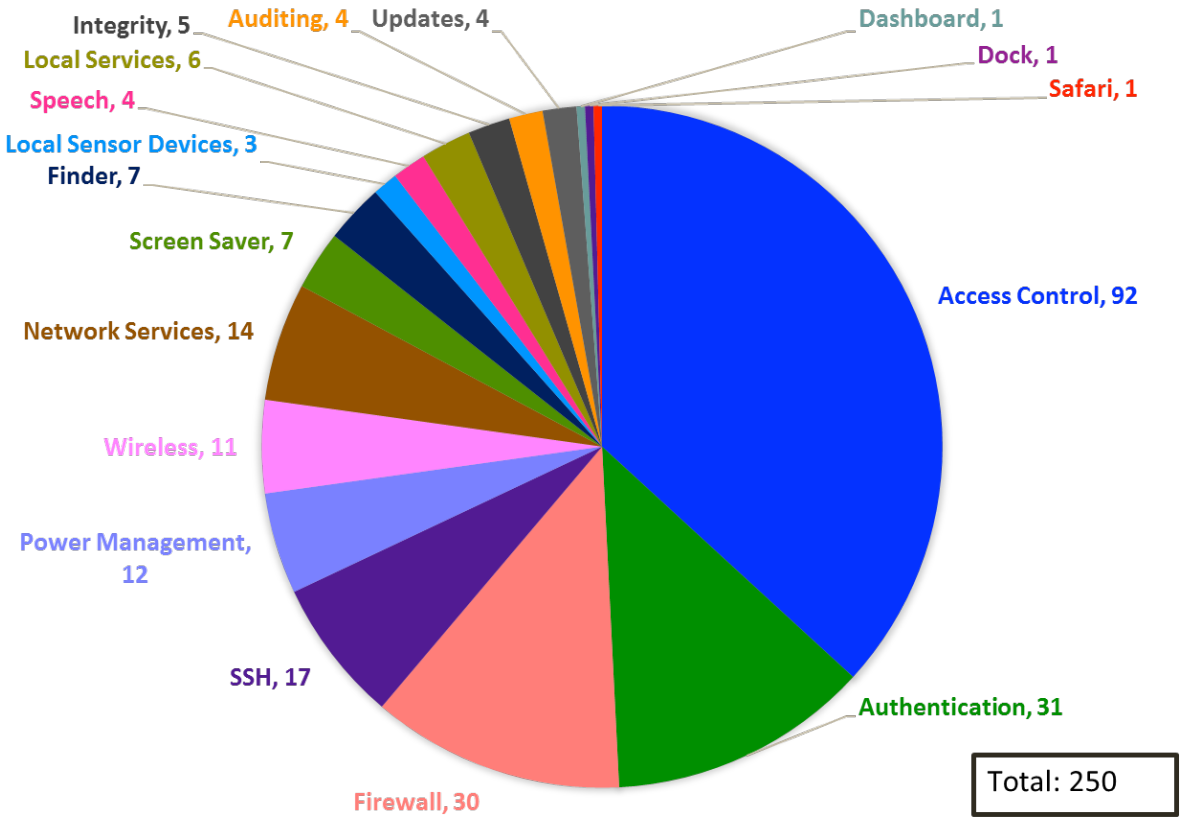

Figure 13: Distribution of Security Controls

Appendix B. Mapping OS X Controls to NIST SP 800-53 Rev 4

Appendix B maps many of the security controls and baseline settings referenced throughout this document to their corresponding controls in NIST Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. The list of controls and mapping is not intended to be fully comprehensive or authoritative, and it omits SP 800-53 controls that are not directly related to individual OS X 10.10 systems. Note that a mapping does not imply full satisfaction of a given security control's requirements. If an organization were to follow the guidance in sections 6.3.1 and 6.3.2.5, additional steps might still be required to fully satisfy control AC-2 requirements. The mappings are listed according to the control family categories established in SP 800-53. Each category has a separate table, with three columns containing the following information for each mapping:

- Number and name of the control from SP 800-53
- The sections of this publication that map to the SP 800-53 control, and a brief description of the content within those sections that corresponds to the SP 800-53 control
- The settings within this publication and its corresponding spreadsheet that map to the SP 800-53 control, if any.

The tables include the requirements and control enhancements that apply to low, moderate, and high impact systems. (Section 2.2 contains definitions for the impact categories.) After determining the impact level of a system, administrators can select the SP 800-53 controls that correspond to that impact level, and then identify the sections of this document and baseline settings that match those SP 800-53 controls. This would provide a starting point for identifying all of the security controls needed to secure the system.

Table 3: Access Control (AC) Family Controls

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
AC-2: Account management	• Section 6.3.1 (Disabling unneeded accounts) • Section 6.3.2.5 (Disabling Fast User Switching)	CCE_79678_9_fast_user_switching
AC-3: Access enforcement	• Section 6.2.4 (Setting file and folder permissions)	Refer to Table 20 for permission settings
	• Section 6.2.5 (Setting Spotlight permissions)	N/A

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
	• Section 6.3.1 (Having separate accounts for use and administration)	N/A
	• Section 6.3.6 (Storing credentials securely)	N/A
	• Section 6.6.2 (Restricting use of shares and remote access tools)	CCE_79828_0_ssh_restrict_users CCE_79875_1_restrict_screen_sharing_to_specified_users CCE_79753_0_bluetooth_disable_file_sharing CCE_79922_1_disable_remote_management
AC-4: Information flow enforcement	• Section 2.3.2.1 (Using a firewall to limit network access to a host) • Section 3.5 (Using a host-based firewall to restrict network traffic) • Section 4.2 (Disabling iCloud) • Section 6.1.2 (Disabling unneeded hardware components, including network interfaces) • Section 6.6.1 (Using a host-based firewall to restrict network traffic) • Section 6.6.2 (Disabling sharing) • Section 6.6.3 (Disabling IPv6) • Section 6.6.4 (Disabling sshd) • Section 6.6.5 (Disabling wireless networking) • Section 6.6.6 (Disabling Bonjour multicast advertisements)	CCE_79843_9_enable_firewall_logging CCE_79845_4_allow_signed_sw_receive_connections CCE_79846_2_turn_on_firewall See Table 21 for `pf` rules CCE_79889_2_disable_remote_login CCE_79779_3_disable_bonjour_advertising CCE_79834_8_disable_location_services CCE_79866_0_ssh_disable_x11_forwarding CCE_79800_9_disable_airdrop CCE_79858_7_unload_uninstall_infrared_receiver CCE_79859_5_disable_infrared_receiver
AC-6: Least privilege	• Section 2.2 (Assigning user rights based on least privilege) • Section 6.3.1 (Assigning user rights based on least privilege)	CCE_79845_4_allow_signed_sw_receive_connections CCE_79921_3_sbin_route_no_setid_bits CCE_79923_9_usr_libexec_dumpemacs_no_setid_bits CCE_79924_7_usr_libexec_rexecd_no_setid_bits CCE_79925_4_usr_sbin_vpnd_no_setid_bits CCE_79926_2_preferences_install_assistant_no_setid_bits CCE_79927_0_iodbcadmintool_no_setid_bits CCE_79928_8_extensions_webdav_fs_no_setid_bits CCE_79929_6_appleshare_afpLoad_no_setid_bits CCE_79930_4_appleshare_check_afp_no_setid_bits
AC-7: Unsuccessful logon attempts	• Section 6.3.4 (Locking out accounts after too many failed login attempts)	N/A
AC-8: System use notification	• Section 2.3.1.2 (Presenting a warning banner when a user attempts to log on) • Section 2.3.2.1 (Presenting a warning banner when a user attempts to log on)	CCE_79939_5_add_login_banner

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
	• Section 6.8.2 (Presenting a warning banner when a user attempts to log on)	
AC-11: Session lock	• Section 2.3.1.2 (Using a password-protected screen saver) • Section 6.3.5 (Using a password-protected screen saver, manually locking user sessions)	CCE_79736_5_screensaver_grace_period CCE_79737_3_require_password_after_screensaver CCE_79738_1_start_screen_saver_hot_corner CCE_79739_9_no_put_to_sleep_corner CCE_79740_7_no_modifier_keys_for_screen_saver_start CCE_79743_1_no_prevent_screensaver_corner CCE_79754_8_desktop_idle_time CCE_79793_6_sleep_on_power_button
AC-17: Remote access	• Section 2.3.2.1 (Using industry-standard strong protocols for remote access)	CCE_79818_1_ssh_remove_non_fips_140_2_ciphers CCE_79819_9_ssh_remove_cbc_ciphers CCE_79820_7_ssh_remove_non_fips_140_2_macs CCE_79865_2_ssh_use_protocol_version_2 CCE_79781_1_use_network_time_protocol
	• Section 6.6.2 (Disabling built-in remote access services that are not needed)	CCE_79852_0_disable_remote_apple_events CCE_79889_2_disable_remote_login CCE_79922_1_disable_remote_management
AC-18: Wireless access	• Section 6.1.2 (Disabling hardware components) • Section 6.6.2 (Disabling Bluetooth file sharing) • Section 6.6.5 (Not connecting to any wireless network automatically, using wireless security features)	CCE_79763_9_remove_all_preferred_wireless_networks CCE_79748_0_bluetooth_disable_wake_computer CCE_79745_6_bluetooth_turn_off_bluetooth CCE_79756_3_bluetooth_unload_uninstall_kext CCE_79753_0_bluetooth_disable_file_sharing CCE_79746_4_show_bluetooth_status_in_menu_bar CCE_79768_8_show_wifi_status_in_menu_bar CCE_79801_7_wifi_unload_uninstall_kext CCE_79800_9_disable_airdrop CCE_79858_7_unload_uninstall_infrared_receiver CCE_79859_5_disable_infrared_receiver

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
AC-20: Use of external information systems	• Section 4.2 (iCloud settings)	N/A

Table 4: Awareness and Training (AT) Family Controls

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
AT-2: Security awareness training	• Section 2.3.2.3 (Educating users on avoiding malware infections) • Section 2.5 (Having security awareness and training for end users and administrators)	N/A
AT-3: Role-based security training	• Section 2.5 (Having security awareness and training for end users and administrators)	N/A

Table 5: Audit and Accountability (AU) Family Controls

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
AU-2: Audit events	• Section 6.4 (Configuring system auditing)	CCE_79862_9_ssh_set_log_level_verbose CCE_79912_2_set_audit_control_flags
AU-4: Audit storage capacity	• Section 6.4.1 (Enabling logging and specifying log retention time)	CCE_79843_9_enable_firewall_logging CCE_79941_1_audit_log_retention CCE_79940_3_audit_log_max_file_size
AU-6: Audit review, analysis, and reporting	• Section 2.7 (Monitoring logs) • Section 6.4.1 (Reviewing logs)	CCE_79870_2_do_not_send_diagnostic_info_to_apple
AU-8: Time stamps	• Section 6.4.2 (Performing clock synchronization)	CCE_79781_1_use_network_time_protocol

Table 6: Security Assessment and Authorization (CA) Family Controls

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
CA-7: Continuous monitoring	• Section 2.7 (Monitoring security controls and configuration changes)	N/A

Table 7: Configuration Management (CM) Family Controls

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
CM-1: Configuration management policy and procedures	• Section 2.5 (Having a configuration management policy, plan, and procedures) • Section 4 (Having a configuration management policy and user guidance for operating system and application installation and changes) • Section 5 (Managing security configurations)	N/A
CM-2, Baseline configuration	• Section 2 (Having effective and well-tested security configurations)	All settings
CM-3: Configuration change control	• Section 2.6 (Documenting changes to default security baselines and settings) • Section 2.7 (Logging all hardware maintenance activities)	N/A
CM-4: Security impact analysis	• Section 2.6 (Testing changes to security controls) • Section 5 (Determine the effect of applying security baselines for a particular user or computer) • Section 6 (Considering the effect each decision made regarding a system might have on its security)	N/A
CM-6: Configuration settings	• Section 2.5 (Having a security configuration guide) • Section 5 (Using security baselines to set security-relevant system settings	N/A

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
	and to compare actual settings to required settings)	
CM-7: Least functionality	• Section 2.3.1.3 (Disabling unused local services)	CCE_79834_8_disable_location_services CCE_79835_5_disable_auto_actions_on_blank_CD_insertion CCE_79836_3_disable_auto_actions_on_blank_DVD_insertion CCE_79837_1_disable_auto_music_CD_play CCE_79838_9_disable_auto_picture_CD_display CCE_79839_7_disable_auto_video_DVD_play CCE_79745_6_bluetooth_turn_off_bluetooth CCE_79753_0_bluetooth_disable_file_sharing CCE_79774_6_login_window_disable_voiceover CCE_79800_9_disable_airdrop CCE_79813_2_disable_dictation CCE_79814_0_disable_voiceover CCE_79868_6_disable_printer_sharing CCE_79852_0_disable_remote_apple_events CCE_79889_2_disable_remote_login CCE_79922_1_disable_remote_management
	• Section 2.3.2.1 (Disabling unused network services)	CCE_79799_3_disable_bonjour_advertising CCE_79852_0_disable_remote_apple_events CCE_79868_6_disable_printer_sharing CCE_79889_2_disable_remote_login CCE_79875_1_restrict_screen_sharing_to_specified_users CCE_79922_1_disable_remote_management CCE_79753_0_bluetooth_disable_file_sharing CCE_79800_9_disable_airdrop
	• Section 3.9 (Application whitelisting)	N/A
	• Section 6.1.2 (Disabling unneeded hardware components)	CCE_79756_3_bluetooth_unload_uninstall_kext CCE_79801_7_wifi_unload_uninstall_kext CCE_79857_9_unload_uninstall_isight_camera CCE_79858_7_unload_uninstall_infrared_receiver
	• Section 6.5 (Restricting the installation and execution of applications)	N/A

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
	• Section 6.6.1 (Using firewalls to restrict network traffic)	CCE_79843_9_enable_firewall_logging CCE_79845_4_allow_signed_sw_receive_connections CCE_79846_2_turn_on_firewall See Table 21 for `pf` rules
	• Section 6.6.2 (Disabling sharing and remote access utilities)	CCE_79753_0_bluetooth_disable_file_sharing CCE_79771_2_no_guest_access_to_shared_folders CCE_79868_6_disable_printer_sharing CCE_79875_1_restrict_screen_sharing_to_specified_users CCE_79852_0_disable_remote_apple_events CCE_79889_2_disable_remote_login CCE_79922_1_disable_remote_management CCE_79799_3_disable_bonjour_advertising CCE_79800_9_disable_airdrop
	• Section 6.6.3 (Disabling IPv6 support)	N/A
	• Section 6.6.4 (Disabling sshd support)	CCE_79828_0_ssh_restrict_users CCE_79889_2_disable_remote_login CCE_79844_7_ssh_disable_root_login CCE_79944_5_pf_rule_ssh
	• Section 6.6.5 (Disabling wireless networking)	CCE_79745_6_bluetooth_turn_off_bluetooth CCE_79753_0_bluetooth_disable_file_sharing CCE_79756_3_bluetooth_unload_uninstall_kext CCE_79763_9_remove_all_preferred_wireless_networks CCE_79801_7_wifi_unload_uninstall_kext
	• Section 6.6.6 (Disabling Bonjour multicast advertisements)	CCE_79799_3_disable_bonjour_advertising
CM-11: User-installed software	• Section 2.3.2.3 (Not installing or using non-approved applications) • Section 3.1 (Using Gatekeeper to limit which applications can be installed on a system) • Section 6.5 (Using Gatekeeper and Parental Controls to limit which	N/A

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
	applications can be executed on a system)	

Table 8: Contingency Planning (CP) Family Controls

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
CP-2: Contingency plan	• Section 2.3 (Performing contingency planning) • Section 2.5 (Having IT contingency plans)	N/A
CP-9: Information system backup	• Section 2.3 (Performing backups, storing them in a safe and secure location, and testing them regularly) • Section 4.2 (Performing backups and restores; testing backups)	N/A

Table 9: Identification and Authentication (IA) Family Controls

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
IA-1: Identification and authentication policy and procedures	• Section 2.3.1.2 (Having a password policy) • Section 2.3.2.1 (Having a password policy)	CCE_79770_4_require_admin_password_for_system_prefs CCE_79747_2_password_enforce_password_history_restriction CCE_79749_8_password_complex_passwords_alphabetic_char CCE_79750_6_password_complex_passwords_numeric_char CCE_79751_4_password_complex_passwords_symbolic_char CCE_79759_7_password_uppercase_and_lowercase CCE_79761_3_password_minimum_length CCE_79762_1_password_maximum_age
IA-2: Identification and authentication (organizational users)	• Section 2.3.1.2 (Requiring valid username and password authentication) • Section 2.3.1.3 (Requiring strong passwords for administrator accounts) • Section 2.3.2.1 (Requiring strong authentication for using network services)	CCE_79672_2_users_list_on_login CCE_79673_0_other_users_list_on_login CCE_79676_3_retries_until_hint CCE_79678_9_fast_user_switching CCE_79679_7_console_login CCE_79681_3_admin_accounts_visibility CCE_79682_1_local_user_accounts_visibility CCE_79683_9_mobile_accounts_visibility

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
	• Section 2.3.2.3 (Using a daily use account for normal system operations; using an administrator-level account only when needed for specific tasks) • Section 6.3.1 (Having an individual user account for each person)	CCE_79684_7_network_users_visibility CCE_79736_5_screensaver_grace_period CCE_79737_3_require_password_after_screensaver CCE_79738_1_start_screen_saver_hot_corner CCE_79739_9_no_put_to_sleep_corner CCE_79740_7_no_modifier_keys_for_screen_saver_start CCE_79743_1_no_prevent_screensaver_corner CCE_79754_8_desktop_idle_time CCE_79767_0_disable_guest_user CCE_79770_4_require_admin_password_for_system_prefs CCE_79771_2_no_guest_access_to_shared_folders CCE_79817_3_ssh_login_grace_period CCE_79821_5_ssh_challenge_response_authentication_disallowed CCE_79826_4_ssh_enable_password_authentication CCE_79827_2_ssh_disable_pub_key_authentication CCE_79828_0_ssh_restrict_users CCE_79830_6_ssh_set_client_alive_300_seconds CCE_79831_4_ssh_max_auth_tries_4_or_less CCE_79844_7_ssh_disable_root_login CCE_79863_7_ssh_disallow_empty_passwords CCE_79864_5_ssh_turn_off_user_environment CCE_79865_2_ssh_use_protocol_version_2 CCE_79866_0_ssh_disable_x11_forwarding CCE_79893_4_ssh_keep_alive_messages CCE_79848_8_no_netrc_files_on_system CCE_79781_1_use_network_time_protocol CCE_79908_0_sudo_restrict_to_single_terminal CCE_79910_6_sudo_timeout_period_set_to_0 CCE_79770_4_require_admin_password_for_system_prefs CCE_79747_2_password_enforce_password_history_restriction CCE_79749_8_password_complex_passwords_alphabetic_char CCE_79750_6_password_complex_passwords_numeric_char CCE_79751_4_password_complex_passwords_symbolic_char CCE_79759_7_password_uppercase_and_lowercase CCE_79761_3_password_minimum_length

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
		CCE_79762_1_password_maximum_age
	• Section 6.3.2.1 (Not permitting system login to be bypassed)	CCE_79938_7_disable_automatic_system_login
	• Section 6.3.2.5 (Disabling Fast User Switching)	CCE_79678_9_fast_user_switching
	• Section 6.3.2.6 (Using Active Directory services for authentication)	N/A
IA-4: Identifier management	• Section 6.3.1 (Creating a separate daily use account for each user) • Section 6.3.4 (Having strong passwords for each user account)	CCE_79749_8_password_complex_passwords_alphabetic_char CCE_79750_6_password_complex_passwords_numeric_char CCE_79751_4_password_complex_passwords_symbolic_char CCE_79759_7_password_uppercase_and_lowercase CCE_79761_3_password_minimum_length
IA-5: Authenticator management	• Section 2.3.2.2 (Using a secure user identification and authentication system)	N/A
	• Section 6.3.4 (Setting minimum and maximum password ages; ensuring password strength; preventing password reuse through password history)	CCE_79747_2_password_enforce_password_history_restriction CCE_79762_1_password_maximum_age CCE_79749_8_password_complex_passwords_alphabetic_char CCE_79750_6_password_complex_passwords_numeric_char CCE_79751_4_password_complex_passwords_symbolic_char CCE_79759_7_password_uppercase_and_lowercase CCE_79761_3_password_minimum_length

Table 10: Incident Response (IR) Family Controls

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
IR-1: Incident response policy and procedures	• Section 2.7 (Having an organization incident response policy)	N/A
IR-4: Incident handling	• Section 2.7 (Having a formal incident response capability)	N/A

Table 11: Maintenance (MA) Family Controls

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
MA-1: System maintenance policy and procedures	• Section 2.3.2.3 (Creating a plan for maintaining OS X 10.10 systems)	N/A
MA-2: Controlled maintenance	• Section 2.7 (Performs regular security maintenance)	N/A
MA-4: Nonlocal maintenance	• Section 2.7 (Providing remote system administration and assistance)	N/A

Table 12: Media Protection (MP) Family Controls

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
MP-4: Media storage	• Section 2.3.1.2 (Physically securing removable media) • Section 2.7 (Protecting media) • Section 4.2 (Storing and protecting backup media)	N/A
MP-6: Media sanitization	• Section 2.7 (Sanitizing media) • Section 4.1.1 (Sanitizing media) • Section 6.2.3 (Securely erasing trash)	CCE_79802_5_secure_erase_trash

Table 13: Physical and Environmental Protection (PE) Family Controls

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
PE-1: Physical and environmental protection policy and procedures	• Section 2.3.1.1 (Having a physical and environmental protection policy)	N/A
PE-3: Physical access control	• Section 2.3.1.1 (Implementing physical securing measures to restrict access to systems) • Section 2.3.2.3 (Restricting physical access to systems)	N/A

Table 14: Planning (PL) Family Controls

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
PL-2: System security plan	Section 2.5 (Having a security configuration guide and other security-related documentation)	N/A
PL-4: Rules of behavior	• Section 2.5 (Having a rules of behavior document)	N/A

Table 15: Personnel Security (PS) Family Controls

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
PS-4: Personnel termination	• Section 2.3.1.2 (Disabling accounts as soon as employees leave the organization) • Section 2.3.2.1 (Disabling accounts as soon as employees leave the organization) • Section 6.3.1 (Disabling accounts as soon as they are no longer needed, such as an employee leaving the organization)	N/A
PS-5: Personnel transfer	• Section 6.3.1 (Disabling accounts as soon as they are no longer needed, such as an employee whose responsibilities change)	N/A

Table 16: Risk Assessment (RA) Family Controls

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
RA-2: Security categorization	• Section 2.2 (Describes FIPS 199 security categories and their relationship to SP 800-53 controls)	N/A
RA-3: Risk assessment	• Section 2.3 (Defining threats, conducting risk assessments, performing risk mitigation)	N/A
RA-5: Vulnerability scanning	• Section 2.7 (Performing vulnerability assessments to assess the security posture of the system) • Section 5.4 (Using vulnerability scanners to identify security issues)	N/A

Table 17: System and Services Acquisition (SA) Family Controls

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
SA-5: Information system documentation	• Section 2.5 (Having a security configuration guide and other security-related documentation)	N/A

Table 18: System and Communications Protection (SC) Family Controls

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
SC-4: Information in shared resources	• Section 3.8 (Encrypting virtual memory)	CCE_79833_0_encrypt_system_swap_file
SC-8: Transmission confidentiality and integrity	• Section 2.3.2.2 (Encrypting network communications) • Section 6.6.4 (SSH Daemon)	CCE_79818_1_ssh_remove_non_fips_140_2_ciphers CCE_79819_9_ssh_remove_cbc_ciphers CCE_79820_7_ssh_remove_non_fips_140_2_macs
SC-13: Cryptographic protection	• Section 6.2.2.3 (Using FIPS-approved encryption algorithms)	CCE_79818_1_ssh_remove_non_fips_140_2_ciphers CCE_79819_9_ssh_remove_cbc_ciphers CCE_79820_7_ssh_remove_non_fips_140_2_macs
SC-18: Mobile code	• Section 2.3.2.3 (Configuring systems so that default file associations prevent automatic execution of active content files)	N/A
SC-28, Protection of information at rest	• Section 2.3.1.1 (Encrypting local files to prevent access) • Section 2.3.1.3 (Encrypting sensitive data) • Section 3.6 (Encrypting files to prevent access) • Section 3.8 (Encrypting virtual memory) • Section 4.2 (Encrypting Time Machine backups) • Section 6.2.2 (Encrypting files to prevent access)	CCE_79833_0_encrypt_system_swap_file

Table 19: System and Information Integrity (SI) Family Controls

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
SI-2: Flaw remediation	• Section 2.3.1.3 (Installing application and OS updates) • Section 2.3.2.1 (Testing and installing application and OS updates) • Section 2.7 (Acquiring and installing software updates) • Section 4.3 (Acquiring and installing security updates; configuring software update features) • Section 5.3 (Installing applications and application updates) • Section 5.4 (Checking the patch status of computers)	CCE_79777_9_install_system_data_updates CCE_79778_7_install_security_updates CCE_79876_9_update_apple_software CCE_79776_1_updates_download_in_background
SI-3: Malicious code protection	• Section 2.3.2.3 (Protecting systems from malicious payloads; using antivirus and antispyware software; configuring server and client software to reduce exposure to malware) • Section 3.7 (Using code execution protection features) • Section 6.2.1 (Displaying full filenames to identify suspicious extensions used by malware) • Section 6.5 (Restricting the execution of software) • Section 6.6.1 (Using personal firewalls to block outbound communications from malware)	CCE_79783_7_display_file_extensions CCE_79778_7_install_security_updates CCE_79783_7_display_file_extensions
SI-4: Information system monitoring	• Section 2.7 (Monitoring event logs to identify problems and suspicious activity)	N/A
SI-5: Security alerts, advisories, and directives	• Section 2.3.2.3 (Monitoring mailing lists for relevant security bulletins) • Section 2.7 (Subscribing to and monitoring vulnerability notification mailing lists)	N/A
SI-6: Security function verification	• Section 5.4 (Performing central monitoring of security controls)	N/A
SI-7: Software, firmware, and information integrity	• Section 2.7 (Monitoring changes to OS and software settings) • Section 3.1 (Preventing unwanted executables from being installed) • Section 6.5.2 (Using Parental Controls to prevent unwanted executables from running)	N/A
SI-8: Spam protection	• Section 2.3.2.3 (Protecting systems from malicious payloads; using e-mail clients that support spam filtering) • Section 6.7.1 (Configuring e-mail clients to use anti-spam features; configuring e-mail clients not to load remote images automatically) • Section 6.7.2 (Limiting Web browser cookies, including tracking cookies)	N/A
SI-16, Memory protection	• Section 3.7 (Code execution protection)	N/A

File permission settings are grouped together in Table 20 below.

Table 20: File Permissions

CCE_79685_4_bash_init_files_owner	CCE_79886_8_etc_hosts_permissions
CCE_79686_2_bash_init_files_group	CCE_79887_6_etc_hosts_owner
CCE_79687_0_bash_init_files_permissions	CCE_79888_4_etc_hosts_group
CCE_79688_8_csh_init_files_owner	CCE_79890_0_var_run_resolv_conf_permissions
CCE_79689_6_csh_init_files_group	CCE_79891_8_var_run_resolv_conf_owner
CCE_79690_4_csh_init_files_permissions	CCE_79892_6_var_run_resolv_conf_group
	CCE_79894_2_etc_openldap_ldap_conf_permissions
CCE_79698_7_ipcs_owner	CCE_79895_9_etc_openldap_ldap_conf_owner
CCE_79699_5_ipcs_group	CCE_79896_7_etc_openldap_ldap_conf_group
CCE_79700_1_ipcs_permissions	CCE_79897_5_etc_passwd_permissions
CCE_79701_9_rcp_owner	CCE_79898_3_etc_passwd_owner
CCE_79702_7_rcp_group	CCE_79899_1_etc_passwd_group
CCE_79703_5_rcp_permissions	
CCE_79704_3_rlogin_owner	CCE_79900_7_usr_sbin_traceroute_permissions
CCE_79705_0_rlogin_group	CCE_79901_5_usr_sbin_traceroute_owner
CCE_79706_8_rlogin_permissions	CCE_79902_3_usr_sbin_traceroute_group
CCE_79707_6_rsh_owner	CCE_79903_1_etc_motd_permissions
CCE_79708_4_rsh_group	CCE_79904_9_etc_motd_owner
CCE_79709_2_rsh_permissions	CCE_79905_6_etc_motd_group
	CCE_79907_2_var_at_at_deny_owner
CCE_79710_0_aliases_acl	CCE_79909_8_var_at_permissions
CCE_79711_8_group_acl	CCE_79913_0_private_var_at_cron_allow_group
CCE_79712_6_hosts_acl	CCE_79916_3_private_var_at_cron_deny_group
CCE_79713_4_ldap_conf_acl	CCE_79917_1_global_preferences_plist_permissions
CCE_79714_2_passwd_acl	CCE_79919_7_etc_aliases_group
CCE_79715_9_services_acl	
CCE_79716_7_syslog_conf_acl	CCE_79918_9_system_command_files_permissions
CCE_79717_5_cron_allow_acl	CCE_79920_5_usr_lib_sa_sadc_permissions
CCE_79718_3_cron_deny_acl	CCE_79921_3_sbin_route_no_setid_bits
CCE_79719_1_traceroute_acl	CCE_79923_9_usr_libexec_dumpemacs_no_setid_bits
CCE_79720_9_resolve_conf_acl	CCE_79924_7_usr_libexec_rexecd_no_setid_bits
	CCE_79925_4_usr_sbin_vpnd_no_setid_bits
CCE_79721_7_services_owner	CCE_79926_2_preferences_install_assistant_no_setid_bits
CCE_79722_5_services_group	CCE_79927_0_iodbcadmintool_no_setid_bits
CCE_79723_3_services_permissions	

CCE_79724_1_syslog_conf_owner CCE_79725_8_syslog_conf_group CCE_79726_6_audit_logs_owner CCE_79727_4_audit_logs_group CCE_79728_2_audit_logs_permissions CCE_79730_8_audit_config_permissions CCE_79729_0_audit_logs_acl CCE_79731_6_audit_tool_executables_acl CCE_79779_5_all_files_in_a_users_home_dir_are_owned_by_that_user CCE_79780_3_files_in_home_dir_group_owned_by_owners_group CCE_79861_1_no_acls_system_command_executables CCE_79867_8_crontab_files_no_acls CCE_79869_4_etc_shells_no_acls CCE_79877_7_library_files_permissions CCE_79878_5_system_log_files_permissions CCE_79879_3_files_in_user_home_directories_no_ACLs CCE_79880_1_user_home_directories_no_ACLs CCE_79881_9_etc_shells_permissions CCE_79882_7_etc_shells_owner CCE_79883_5_etc_group_file_permissions CCE_79884_3_etc_group_file_owner CCE_79885_0_etc_group_file_group	CCE_79932_0_system_files_and_directories_no_uneven_permissions CCE_79911_4_library_files_no_acls CCE_79928_8_extensions_webdav_fs_no_setid_bits CCE_79929_6_appleshare_afpLoad_no_setid_bits CCE_79930_4_appleshare_check_afp_no_setid_bits CCE_79931_2_user_home_directories_permissions CCE_79933_8_remote_management_ARD_agent_permissions

Firewall rules for the `pf` firewall are grouped together in Table 21.

Table 21: `pf` Firewall Rules

CCE_79942_9_pf_enable_firewall CCE_79943_7_pf_rule_ftp CCE_79944_5_pf_rule_ssh CCE_79945_2_pf_rule_telnet CCE_79946_0_pf_rule_rexec CCE_79947_8_pf_rule_rsh	CCE_79956_9_pf_rule_screen_sharing CCE_79957_7_pf_rule_icmp CCE_79958_5_pf_rule_smtp CCE_79959_3_pf_rule_pop3 CCE_79960_1_pf_rule_pop3s CCE_79961_9_pf_rule_sftp

CCE_79948_6_pf_rule_tftp	CCE_79962_7_pf_rule_imap
CCE_79949_4_pf_rule_finger	CCE_79963_5_pf_rule_imaps
CCE_79950_2_pf_rule_http	CCE_79964_3_pf_rule_printer_sharing
CCE_79951_0_pf_rule_nfs	CCE_79965_0_pf_rule_bonjour
CCE_79952_8_pf_rule_remote_apple_events	CCE_79966_8_pf_rule_mDNSResponder
CCE_79953_6_pf_rule_smb	CCE_79967_6_pf_rule_itunes_sharing
CCE_79954_4_pf_rule_apple_file_service	CCE_79968_4_pf_rule_optical_drive_sharing
CCE_79955_1_pf_rule_uucp	

Appendix C. Tools

Appendix C lists tools that may be helpful in configuring, managing, and monitoring the security of OS X systems.

The following table briefly describes a variety of commands that can be used to make configuration changes on OS X. This is not an exhaustive list of all tools available to make configuration changes. In order to fully automate some settings, other commands may be required in addition to those listed below. For more information on these commands, view the Manual pages by using the `man` command.

Table 22: Built-in Commands Used to Write OS X Configuration Data

Command Name	Description
`chgrp`	This is used to change the group ownership on a file or directory.
`chmod`	This command is used to change a file's permission bits. Modifications can be made to read, write, execute, and extended ACLs on a file or directory.
`chown`	This command is used to modify the owner and group owner on a file or directory.
`cupsctl`	This command is used to configure settings for CUPS (Common Unix Printing System). In this guide, the `cupsctl` command is used to disable printer sharing.
`defaults`	The defaults command is used to modify or read OS X `.plist` configuration files. Modifying configuration files with defaults has a side-effect of resetting permissions and changing ownership metadata to the user who executed the command.
`dscl`	This command is used to modify and read Directory Service data. In this guide, `dscl` is used to modify and read user properties.
`kickstart`	This program is used for modifying remote management settings. This can be used to turn remote management off entirely, or to limit access to specific users.
`networksetup`	Changes the specified network adapter's settings.
`pfctl`	Modifies the `pf` firewall rules and behaviors.
`PlistBuddy`	Alternate method for reading and editing `.plist` files. Allows for modification of nested keys.
`pmset`	Changes power management settings for OS X.
`praudit`	Tool that allows reading of BSM formatted log files, such as the ones located in `$AUDIT_LOG_PATH`.
`pwpolicy`	This is used to change password policy requirements for a specific user, or for an entire system.
`scutil`	This command is used to modify and read many system settings. In this guide, the command is used to modify the system's name.
`security`	Command line interface allowing administrator access to the security framework.

Command Name	Description
`socketfilterfw`	This command controls a variety of software firewall settings. It is used for actions such as disabling the firewall, or configuring what applications are allowed through the firewall.
`softwareupdate`	This is the command line equivalent program for viewing available updates and choosing which updates to install.
`systemsetup`	The `systemsetup` command can be used to modify many of the settings found in the System Preferences GUI application. This command is used to modify network time settings in this guide.
`system_profiler`	Tool that returns information about the host system.
`visudo`	This program is used to edit the `/etc/sudoers` file while ensuring the file's proper format.

Appendix D. Resources

Appendix D lists resources that may be useful OS X security references.

Table 23: OS X Security Resources

Online Resource	URL
NIST OS X 10.10 Setting Baselines	https://github.com/usnistgov/applesec
Apple's OS X 10.8 security page	https://web.archive.org/web/20121202050221/http://www.apple.com/osx/what-is/security.html
Apple's OS X 10.9 security page	https://web.archive.org/web/20131223153413/http://www.apple.com/osx/what-is/security.html
Apple's OS X 10.10 security page	https://web.archive.org/web/20150201073654/http://www.apple.com/osx/what-is/security/
Apple Security Updates	http://support.apple.com/kb/HT1222
OS X Security Configuration (for 10.7)	http://help.apple.com/securityguide/mac/10.7/#
CIS OS X 10.8 Benchmark	http://und.edu/cio/it-security/policy/_files/docs/cis-apple-osx-10.8-benchmark-v1-0-0.pdf
DISA STIG for OS X	http://iase.disa.mil/stigs/os/mac/Pages/mac-os.aspx
TCP and UDP ports used by Apple software products	http://support.apple.com/kb/TS1629

Bathurst, Robert et al., *The Hacker's Guide to OS X: Exploiting OS X from the Root Up*, Syngress, 2012.

Beighley, Lynn, *OS X Mountain Lion*, Peachpit Press, 2012.

Dreyer, Arek and Greisler, Ben, *Apple Pro Training Series: OS X Server Essentials: Using and Supporting OS X Server on Mountain Lion*, Peachpit Press, 2012.

Edge, Charles et al., *Enterprise Mac Security: Mac OS X Snow Leopard*, Apress, 2010.

Edge, Charles, *Using Mac OS X Lion Server: Managing Mac Services at Home and Office*, O'Reilly Media, 2012.

Gruman, Galen, *OS X Mountain Lion Bible*, Wiley, 2012.

Kissell, Joe, *Mac Security Bible*, Wiley, 2010.

Kite, Robert et al., *Apple Training Series: Mac OS X Security and Mobility v10.6*, Peachpit Press, 2010.

Levin, Jonathan, *Mac OS X and iOS Internals: To the Apple's Core*, Wrox, 2012.

McFedries, Paul, *Teach Yourself VISUALLY OS X Mountain Lion*, Visual, 2012.

Pogue, David, *OS X Mountain Lion: The Missing Manual*, O'Reilly Media, 2012.

Seibold, Chris, *Mac Hacks: Tips & Tools for Unlocking the Power of OS X*, O'Reilly Media, 2013.

Seibold, Chris, *OS X Mountain Lion Pocket Guide*, O'Reilly Media, 2012.

Taylor, Dave, *Learning Unix for OS X Mountain Lion: Going Deep with the Terminal and Shell*, O'Reilly Media, 2012.

White, Kevin M. and Davisson, Gordon, *Apple Pro Training Series: OS X Support Essentials*, Peachpit Press, 2012.

Appendix E. Acronyms and Abbreviations

Selected acronyms and abbreviations used in the guide are defined below.

ACL	Access Control List
AES	Advanced Encryption Standard
ARD	Apple Remote Desktop
ASLR	Address Space Layout Randomization
BIOS	Basic Input/Output System
DNS	Domain Name System
DoS	Denial of Service
EFI	Extensible Firmware Interface
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GB	Gigabyte
GUI	Graphical User Interface
HFS	Hierarchical File System
ICMP	Internet Control Message Protocol
IM	Instant Messaging
IP	Internet Protocol
IPsec	Internet Protocol Security
IPv6	Internet Protocol version 6
IT	Information Technology
ITL	Information Technology Laboratory
LAN	Local Area Network
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OMB	Office of Management and Budget
OS	Operating System
OVAL	Open Vulnerability and Assessment Language
P2P	Peer-to-Peer
PC	Personal Computer
PII	Personally Identifiable Information
POP3	Post Office Protocol 3
SCAP	Security Content Automation Protocol
SFTP	Secure File Transfer Protocol
S/MIME	Secure/Multipurpose Internet Mail Extensions
SMTP	Simple Mail Transfer Protocol
SOHO	Small Office/Home Office
SP	Special Publication
SSH	Secure Shell
SSLF	Specialized Security-Limited Functionality
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol

USB	Universal Serial Bus
XD	Execute Disable

Appendix F. Terminal Command Variables

Many terminal commands explained in this document use variables, which are described below. They must be replaced with a value in order for them to have the desired effect.

Table 24: Terminal Command Variable Descriptions

Variable	Description
`$AUDIT_LOG_PATH`	Location of the path to audit logs specified in the `/etc/security/audit_control` file. It is located on the line beginning with `dir:`
`$DEVICE_NAME`	This variable is used for configuring wireless network settings and represents the Wi-Fi adapter to be configured. It can be retrieved from the system by running this command: `networksetup -listnetworkserviceorder`
`$HOST_ID`	This should be replaced with a non-identifying name that will be used for each type of name for a single computer. The different names are `LocalHostName`, `HostName`, `ComputerName`, and `NetBIOSName`.
`$HW_UUID`	This is the unique hardware-based identifier for the system. This value can be obtained by using this command: `system_profiler SPHardwareDataType 2> /dev/null | grep 'Hardware UUID' | awk ' { print $3 }'`
`$PROFILE_VALUE`	Since not all security configurations use the same values, this variable is a placeholder for the actual profile's value. The values for the Standalone, Managed, and SSLF profiles are given in the table along with the terminal command.
`$SHELL_FILES_PATH`	Location of the shell files are specified in the `/etc/shells` file.
`$USER`	For some settings that require a specific username to run, this variable is used. Replace this variable with the short username in which the setting should be applied to.
`$USER_GROUP`	This variable should be replaced with the group name in which the corresponding user resides.

Appendix G. Special Files

Below is a list of files that must be edited manually because there are no provided tools.

Table 25: Files Requiring Manual Editing

File name	Description
`/etc/sudoers`	This file is modified in order to set restrictions on the `sudo` command. NIST recommends that authentication should be required for each `sudo` command, and `sudo` sessions should not persist across Terminal windows. Editing the `/etc/sudoers` file manually can lead to mistakes that may make the file unreadable to the system. To make changes to this file, edit it using the `visudo` command. An administrator can type `sudo visudo` into Terminal to begin editing `/etc/sudoers`. When saving changes to the file, `visudo` will validate that all additions are formatted properly. See Appendix J.4 for enhancing `sudo` security.
`/etc/sshd_config`	This file contains configuration information and security settings for the SSH daemon (server).
`/etc/security/audit_control`	This file contains the values for configuring audit logs, which includes log retention, log size, and the type of information that is recorded.

Appendix H. Process Restarting

Some settings may require certain processes to be restarted in order for the desired result to be achieved. In most cases, restarting processes causes the setting changes to take effect immediately, rather than after restarting the system. OS X 10.10 uses preferences caching, which can prevent changed preferences from taking effect properly without restarting the `cfprefsd` process. The table below gives the names of processes and the settings related to those processes.

Table 26: Settings Requiring Process Restart

Setting	Related Process Names
Show filename extensions	`cfprefsd, Finder`
Show hidden files	
Empty trash securely	
Search scope: Search this Mac	
Warn before changing file extension	
Warn before emptying trash	
Disable AirDrop	
Disable blank CD actions	`cfprefsd, SystemUIServer`
Disable blank DVD actions	
Disable music CD actions	
Disable picture CD actions	
Disable video DVD actions	
Show Wi-Fi status in menu bar	
Show Bluetooth status in menu bar	
Disallow Bluetooth devices to wake the computer	`cfprefsd, UserEventAgent`
Disable Bluetooth file sharing	
Disable application alert announcements	`cfprefsd`
Show Safari status bar	
Restrict screen sharing to no users	
Disable Bonjour advertising	
Disable Dictation	
Run firewall automatically on system startup	
Disable remote Apple events for specific users	
Prevent saving windows when quitting app	
Disable Mission Control Dashboard	`cfprefsd, Dock`
Screen saver grace period	
Require password after screen saver ends	
Start screen saver hot corner	
No put to sleep hot corner	
No modifier keys for start screen saver hot corner	
No prevent screen saver hot corner	
Desktop idle time	
Auto hide Dock	
Turn off Speakable Items	`cfprefsd, SpeakableItems, SpeechRecognitionServer,`

Setting	Related Process Names
	`SpeechFeedbackWindow`
Disable VoiceOver per user	`cfprefsd, VoiceOver`
Disable speak selected text	`cfprefsd, SpeechSynthesis`
Enable firewall logging	`socketfilterfw`
Automatically allow signed software to receive incoming connections	
Turn on firewall	
Turn on firewall and block all incoming connections	

As a convenience, all of the above processes are listed below:

- `cfprefsd`
- `Dock`
- `Finder`
- `socketfilterfw`
- `SpeakableItems`
- `SpeechFeedbackWindow`
- `SpeechRecognitionServer`
- `SpeechSynthesis`
- `SystemUIServer`
- `UserEventAgent`
- `VoiceOver`

Appendix I. File Attributes

I.1. Permissions and Ownership

In order to secure key system files, the permissions must be modified. These files' properties can be modified using programs such as `chmod`, `chown`, and `chgrp`. Generally, all system files and folders should have uneven permissions resolved, meaning that owner permissions should at least be equal to group and other. System files and directories include, but are not limited to, those found in `/etc`, `/bin`, `/usr/bin`, `/sbin`, and `/usr/sbin`. Note that all files and folders must belong to a valid owner and group. Typically, a user or group becomes invalid when it is deleted from the system, and files they owned were not removed.

The following table lists the recommended permissions and ownership information for a variety of OS X files. A "-" represents no recommended change from the default value for that column. A "`*`" in the path means all files in the directory should have the specified permissions and ownership values applied to them. In the permissions column, "`a`" is a shorthand for all users (`ugo`). See the man page for `chmod` for more details. Note that permissions can be reduced below the recommended values, but may cause loss of functionality. Unless specified below, files should have a mode of 0755 or more restrictive in these directories: `/bin`, `/usr/bin`, `/sbin`, and `/usr/sbin`.

Table 27: Recommended File Permissions and Ownership

File/Directory Name	Permission	Owner	Group
/etc/bashrc	a-wxs	root	wheel
/etc/profile	a-wxs	root	wheel
/etc/csh.cshrc	a-xs,go-w	root	wheel
/etc/csh.logout	a-xs,go-w	root	wheel
/etc/csh.login	a-xs,go-w	root	wheel
/usr/bin/ipcs	a-ws,go-r	root	wheel
/bin/rcp	a-ws	root	wheel
/usr/bin/rlogin	a-ws	root	wheel
/usr/bin/rsh	a-ws	root	wheel
/etc/services	a-xs,go-w	root	wheel
/etc/syslog.conf	-	root	wheel
$AUDIT_LOG_PATH/*	a-xs,go-w,o-r	root	wheel
/etc/security/audit_class	a-ws	-	-

File/Directory Name	Permission	Owner	Group
/etc/security/audit_control	a-ws	-	-
/etc/security/audit_event	a-ws	-	-
/etc/security/audit_warn	a-ws	-	-
/etc/security/audit_user	a-ws	-	-
~/*	-	$USER	$USER_GROUP
Files listed in the /etc/shells file	a-s,go-w	root	-
/etc/group	a-xs,go-w	root	wheel
/etc/hosts	a-xs,go-w	root	wheel
/var/run/resolv.conf	a-xs,go-w	root	daemon
/etc/openldap/ldap.conf	a-xs,go-w	root	wheel
/etc/passwd	a-xs,go-w	root	wheel
/usr/sbin/traceroute	a-w,go-rs	root	wheel
/etc/motd	a-xs,go-w	root	wheel
/var/at/at.deny	-	root	-
/var/at	a-s,go-w	-	-
/private/var/at/cron.allow	-	-	wheel
/private/var/at/cron.deny	-	-	wheel
/Library/Preferences/.GlobalPreferences.plist	a-xs,go-w	-	-
/etc/aliases	-	-	wheel
/usr/bin/login	go-ws	-	-
/usr/bin/sudo	go-ws	-	-
/usr/bin/su	go-ws	-	-
/usr/lib/sa/sadc	a-ws	-	-
/sbin/route	a-s	-	-
/usr/libexec/dumpemacs	a-s	-	-
/usr/libexec/rexecd	a-s	-	-
/usr/sbin/vpnd	a-s	-	-

File/Directory Name	Permission	Owner	Group
`/Applications/System Preferences.app/Contents/Resources/installAssistant`	`a-s`	-	-
`/Applications/Utilities/ODBCAdministrator.app/Contents/Resources/iodbcadmintool`	`a-s`	-	-
`/System/Library/Extensions/webdav_fs.kext/Contents/Resources/load_webdav`	`a-s`	-	-
`/System/Library/Filesystems/AppleShare/afpLoad`	`a-s`	-	-
`/System/Library/Filesystems/AppleShare/check_afp.app/Contents/MacOS/check_afp`	`a-s`	-	-
Home directories	`go-rwx`	-	-
`/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/MacOS/ARDAgent`	`a-s,go-w`	-	-
`/var/log/*`	`a-xs,go-w`	-	-
`/Library/Logs/*`	`a-xs,go-w`	-	-
`$AUDIT_LOG_PATH/*`	`a-xs,g-w,o-rw`	-	-
`.a`, `.so`, and `.dylib` files inside `/System/Library/Frameworks` `/Library/Frameworks` `/usr/lib` `/usr/local/lib` and their subdirectories	`a-s,go-w`	-	-

I.2. Access Control Lists

Extended access control lists (ACLs) must also be removed from files. Since these ACLs are difficult to view for most users, these special permissions can sometimes go unnoticed. They should be removed to prevent unauthorized access or modification of files. The following command can be used to find all files with ACLs on the system:

```
find / -name \* -acl
```

To find and remove all ACLs from the files, use this command:

```
find / -name \* -acl -exec chmod -N '{}' +
```

NIST recommends removing ACLs from the files and directories in the following list if removing ACLs from all files is not practical for the target system. Use the command `chmod -N $FILE_NAME` to remove all ACLs from a file.

- `/etc/aliases`
- `/etc/group`
- `/etc/hosts`

- `/etc/openldap/ldap.conf`
- `/etc/passwd`
- `/etc/services`
- `/etc/syslog.conf`
- `/private/var/at/cron.allow`
- `/private/var/at/cron.deny`
- `/usr/sbin/traceroute`
- `/etc/resolv.conf`
- `$AUDIT_LOG_PATH/*`
- `/usr/sbin/auditd`
- `/usr/sbin/audit`
- `/usr/sbin/auditreduce`
- `/usr/sbin/praudit`
- Executables files in:
    - `/bin`
    - `/sbin`
    - `/usr/bin`
    - `/usr/sbin`
- `/usr/sbin/cron`
- `/usr/lib/cron`
- `/usr/bin/crontab`
- `/private/var/at/cron.deny`
- `$SHELL_FILES_PATH`
- Files and folders in `~$USER` for each username
- Home directory for each user
- Files in the following directories with the extensions `.a`, `.so`, `.dylib`:
    - `/System/Library/Frameworks`
    - `/Library/Frameworks`
    - `/usr/lib`
    - `/usr/local/lib`

Appendix J. Terminal Configuration Commands

This appendix provides the terminal commands needed to configure a system through an automated process. The appendix is broken into sections based on the categories of the settings.

J.1. Disabling Hardware Components

Note that kernel extension (`kext`) removal is only recommended for SSLF systems.

Table 28: Disabling Hardware Components

Device Name	Disable Through Configuration	Remove Kernel Extension
Bluetooth	`defaults write /Library/Preferences/com.apple.Bluetooth.plist ControllerPowerState -bool $PROFILE_VALUE` Where `$PROFILE_VALUE` is one of the following SOHO=Enterprise=`true`, SSLF=`false`	`rm -rf /System/Library/Extensions/IOBluetoothFamily.kext /System/Library/Extensions/IOBluetoothHIDDriver.kext`
Wi-Fi[52]	`networksetup -setairportpower en1 off` Where `en1` is the Wi-Fi adapter name This setting is only recommended for SSLF systems.	`rm –rf /System/Library/Extensions/IO80211Family.kext`
Infrared (IR)	`defaults write /Library/Preferences/com.apple.driver.AppleIRController.plist DeviceEnabled -bool false`	`rm -rf /System/Library/Extensions/AppleIRController.kext`

Built-in camera	-	`rm -rf /System/Library/Extensions/IOUSBFamily.kext/Contents/Plugins/AppleUSBVideoSupport.kext`
		
		`rm -rf /System/Library/Extensions/Apple_iSight.kext`
		
		`rm -rf /System/Library/Frameworks/CoreMediaIO.framework/Versions/A/Resources/VDC.plugin`

[52] Run the command `networksetup -listnetworkserviceorder` to view the short device names.

J.2. Accessibility Settings

Accessibility settings are designed to improve ease-of-use and may be required for some users. These settings include text-to-speech, auditory alerts, and the ability to control the system through voice commands. Accessibility settings may negatively affect security by causing information leakage, but this effect can be partially mitigated with modifications to the operating environment. The majority of these settings rely on the audio hardware interface. When configuring systems for accessible use, organizations should consider the hardware interfaces needed to promote accessibility. Table 29 describes the commands used to configure accessibility on a system.

Table 29: Accessibility Settings

Setting Name	Terminal Command
*Disable Dictation	`defaults write ~/Library/Preferences/com.apple.speech.recognition.AppleSpeechRecognition.prefs.plist DictationIMMasterDictationEnabled -bool $PROFILE_VALUE` Where `$PROFILE_VALUE` is one of the following: SOHO=Enterprise=unchanged, SSLF=`false`
Disable VoiceOver on login window	`defaults write /Library/Preferences/loginwindow.plist UseVoiceOverAtLoginwindow -bool $PROFILE_VALUE` Where `$PROFILE_VALUE` is one of the following: SOHO=Enterprise=unchanged, SSLF=`false`
*Disable application alert announcements	`defaults write ~/Library/Preferences/com.apple.speech.synthesis.general.prefs.plist TalkingAlertsSpeakTextFlag -bool $PROFILE_VALUE` Where `$PROFILE_VALUE` is one of the following: SOHO=Enterprise=unchanged, SSLF=`false`
*Disable speak selected text	`defaults write ~/Library/Preferences/com.apple.speech.synthesis.general.prefs.plist SpokenUIUseSpeakingHotKeyFlag -bool $PROFILE_VALUE` Where `$PROFILE_VALUE` is one of the following: SOHO=Enterprise=unchanged, SSLF=`false`
*Disable VoiceOver per user	`defaults write ~/Library/Preferences/com.apple.universalaccess.plist voiceOverOnOffKey -bool $PROFILE_VALUE` Where `$PROFILE_VALUE` is one of the following: SOHO=Enterprise=unchanged, SSLF=`false`

* See Appendix H to determine what processes should be restarted for the setting to take effect.

J.3. Finder Preferences

Table 30: Finder Preferences

Setting Name	Terminal Commands
*Show filename	`defaults write ~/Library/Preferences/.GlobalPreferences.plist`

Setting Name	Terminal Commands
extensions	`AppleShowAllExtensions -bool true`
*Warn before changing file extension	`defaults write ~/Library/Preferences/com.apple.finder.plist FXEnableExtensionChangeWarning -bool true`
*Warn before emptying trash	`defaults write ~/Library/Preferences/com.apple.finder.plist WarnOnEmptyTrash -bool true`
*Empty trash securely	`defaults write ~/Library/Preferences/com.apple.finder.plist EmptyTrashSecurely -bool $PROFILE_VALUE` Where `$PROFILE_VALUE` is one of the following SOHO=Enterprise=`false`, SSLF=`true`
*Search scope: Search this Mac	`defaults write ~/Library/Preferences/com.apple.finder.plist FXDefaultSearchScope -string SCev`
*Show hidden files	`defaults write ~/Library/Preferences/com.apple.finder.plist AppleShowAllFiles -bool $PROFILE_VALUE` Where `$PROFILE_VALUE` is one of the following SOHO=Enterprise=`false`, SSLF=`true`
*Prevent saving windows when quitting app	`defaults write ~/Library/Preferences/.GlobalPreferences.plist NSQuitAlwaysKeepsWindows -bool false`

* See Appendix H to determine what processes should be restarted for the setting to take effect.

J.4. User Account Types

Table 31: User Account Settings

Setting Name	Terminal Commands

Disable guest user account	`dscl . -create /Users/Guest AuthenticationAuthority ";basic;"`
	
	`dscl . -create /Users/Guest passwd "*"`
	
	`dscl . -create /Users/Guest UserShell "/sbin/nologin"`
	
	`defaults write /Library/Preferences/com.apple.loginwindow.plist GuestEnabled -int 0`

Disable guest access to shared folders	`defaults write /Library/Preferences/com.apple.AppleFileServer.plist guestAccess -bool false`
	
	`defaults write /Library/Preferences/SystemConfiguration/com.apple.smb.server.plist AllowGuestAccess -bool false`

Restrict sudo authentication to single Terminal	`echo “Defaults tty_tickets” >> /etc/sudoers`
Set sudo authentication	`echo “Defaults timestamp_timeout=0” >> /etc/sudoers`

Setting Name	Terminal Commands
frequency	Change the value if the line already exists.
Only root has UID 0	Run this command for all non-root users with UID 0. `dscl . -change "~$USER" UniqueID 0 $UNUSED_UID`

J.5. Login Window

Table 32: Login Window GUI Settings

Setting Name	Terminal Commands
Disable automatic login	`defaults delete "/Library/Preferences/com.apple.loginwindow autoLoginUser"`
Hide users list	`defaults write /Library/Preferences/com.apple.loginwindow.plist SHOWFULLNAME -bool true`
Show sleep, restart, and shut down buttons[53]	`defaults write /Library/Preferences/com.apple.loginwindow.plist PowerOffDisabled -bool $PROFILE_VALUE` Where `$PROFILE_VALUE` is one of the following: SOHO=`false`, Enterprise=SSLF=`true`
Disable input menu in login window	`defaults write /Library/Preferences/loginwindow.plist showInputMenu -bool false`
Disable password hints	`defaults write /Library/Preferences/com.apple.loginwindow.plist RetriesUntilHint -int 0`
Disable fast user switching	`defaults write /Library/Preferences/.GlobalPreferences MultipleSessionEnabled -bool false`
Disable VoiceOver on login window	See the Accessibility table in Appendix J.2 for this command

Table 33: Login Window Terminal Settings

Setting Name	Terminal Commands
Disable inactivity logout	`defaults write /Library/Preferences/.GlobalPreferences`

[53] The three buttons can be toggled individually through Terminal commands using the keys `SleepDisabled`, `RestartDisabled`, and `ShutDownDisabled` in the `/Library/Preferences/com.apple.loginwindow.plist` configuration file.

Setting Name	Terminal Commands
	`com.apple.autologout.AutoLogOutDelay -int 0`
Set login window screen saver idle time	`defaults write /Library/Preferences/com.apple.screensaver.plist loginWindowIdleTime -int 900`
Disable console login	`defaults write /Library/Preferences/com.apple.loginwindow.plist DisableConsoleAccess -bool true`
Disable external accounts	`defaults write /Library/Preferences/com.apple.loginwindow.plist EnableExternalAccounts -bool false`
Hide non-local users on login window user list	`defaults write /Library/Preferences/com.apple.loginwindow.plist SHOWOTHERUSERS_MANAGED -bool false`
Hide admin accounts on login window	`defaults write /Library/Preferences/com.apple.loginwindow.plist HideAdminUsers -bool true`
Hide local user accounts on login window	`defaults write /Library/Preferences/com.apple.loginwindow.plist HideLocalUsers -bool true`
Hide mobile users on login window	`defaults write /Library/Preferences/com.apple.loginwindow.plist HideMobileAccounts -bool true`
Hide network users on login window	`defaults write /Library/Preferences/com.apple.loginwindow.plist IncludeNetworkUser -bool false`

J.6. Password Policy

The pwpolicy program uses a plist file for policy configuration. The NIST recommended password policy as a plist is available on the GitHub repository listed in in the resources in Table 23.

The plist policy file is applied for all users with the following command:

```
pwpolicy setaccountpolicies /full/path/to/policyTempFile
```

The policy temp file can be removed after it is applied.

Alternatively, the pwpolicy plist can be generated and customized using the following process. First, the plist array needs to be created a single time for each of the following policy categories. These commands do not need to be run on a per-setting basis.

```
/usr/libexec/PlistBuddy –c “Add :policyCategoryPasswordContent array”
/full/path/to/policyTempFile

/usr/libexec/PlistBuddy –c “Add :policyCategoryPasswordChange array”
```

```
/full/path/to/policyTempFile

/usr/libexec/PlistBuddy –c “Add :policyCategoryAuthentication array”
/full/path/to/policyTempFile
```

Each setting needs to have an array index different than the others, in increasing order, starting with index 0. These commands must be run for each setting, with the values from Table 34 substituted in.

```
/usr/libexec/PlistBuddy –c “Add :$policy_category:$index:policyContent string $
policy_content” /full/path/to/policyTempFile

/usr/libexec/PlistBuddy –c “Add :$policy_category:$index:policyIdentifier string
$policy_identifier” /full/path/to/policyTempFile

/usr/libexec/PlistBuddy –c “Add :$policy_category:$index:policyParameters dict”
/full/path/to/policyTempFile

/usr/libexec/PlistBuddy –c “Add
:$policy_category:$index:policyParameters:$parameter_name integer  $parameter_value”
/full/path/to/policyTempFile
```

Table 34: Password Policy Settings

Password Rule	Policy Variable Substitutions

Maximum age	`$policy_category = policyCategoryPasswordChange`
	
	`$policy_content = policyAttributeCurrentTime > policyAttributeLastPasswordChangeTime + (policyAttributeExpiresEveryNDays * 24 * 60 * 60)`
	
	`$policy_identifier = com.apple.policy.legacy.maxMinutesUntilChangePassword`
	
	`$parameter_name = policyAttributeExpiresEveryNDays`
	
	`$parameter_value = 60`

Minimum length	`$policy_category = policyCategoryPasswordContent`
	
	`$policy_content = policyAttributePassword matches \’(.){12,}\’`
	
	`$policy_identifier = com.apple.policy.legacy.minChars`
	
	`$parameter_name = minimumChars`
	
	`$parameter_value = 12`

Require alphabetic character	`$policy_category = policyCategoryPasswordContent`
	
	`$policy_content = policyAttributePassword matches \’(.*[a-zA-Z].*)\’`
	
	`$policy_identifier = com.apple.policy.legacy.requiresAlpha`

Password Rule	Policy Variable Substitutions

	`$parameter_name = minimumAlphaCharacters`
	
	`$parameter_value = 1`

Require numeric character	`$policy_category = policyCategoryPasswordContent`
	
	`$policy_content = policyAttributePassword matches \'(.*[0-9].*)\'`
	
	`$policy_identifier = com.apple.policy.legacy.requiresNumeric`
	
	`$parameter_name = minimumNumericCharacters`
	
	`$parameter_value = 1`

Require symbolic character	`$policy_category = policyCategoryPasswordContent`
	
	`$policy_content = policyAttributePassword matches \'(.*[^0-9a-zA-Z].*)\'`
	
	`$policy_identifier = com.apple.policy.legacy.requiresSymbolic`
	
	`$parameter_name = minimumSymbolicCharacters`
	
	`$parameter_value = 1`

Failed login lockout duration	This setting did not work as documented during informal testing.
Invalid login attempts before lockout	This setting did not work as documented during informal testing.

Password history restriction	`$policy_category = policyCategoryPasswordContent`
	
	`$policy_content = none policyAttributePasswordHashes in policyAttributePasswordHistory`
	
	`$policy_identifier = com.apple.policy.legacy.usingHistory`
	
	`$parameter_name = policyAttributeHistoryDepth`
	
	`$parameter_value = 15`

Upper and lowercase characters	`$policy_category = policyCategoryPasswordContent`
	
	`$policy_content = policyAttributePassword matches \'(.*[a-z].*[A-Z].*)| (.*[A-Z].*[a-z].*)\'`
	
	`$policy_identifier = com.apple.policy.legacy.requiresMixedCase`
	
	`$parameter_name = minimumMixedCaseInstances`
	
	`$parameter_value = 1`

Password cannot	This setting did not work as documented during informal testing.

Password Rule	Policy Variable Substitutions
contain username	
Password cannot contain any guessable patterns	This setting did not work as documented during informal testing.

J.7. Session Locking

Table 35: Session Locking Settings

Setting Name	Terminal Command
*Require password after screen saver ends	`defaults write ~/Library/Preferences/ByHost/com.apple.screensaver.$HW_UUID.plist askForPassword -int 1`
*Screen saver grace period	`defaults write ~/Library/Preferences/ByHost/com.apple.screensaver.$HW_UUID.plist askForPasswordDelay -int 5`
*Start screen saver hot corner[54]	`defaults write ~/Library/Preferences/com.apple.dock.plist wvous-$CORNER-corner -int 5`
*No put to sleep hot corner[54]	If any corner puts the display to sleep, run the following command: `defaults write ~/Library/Preferences/com.apple.dock.plist wvous-$CORNER-corner -int 1`
*No modifier keys for start screen saver hot corner[54]	If a start screen saver corner requires a modifier key to be pressed, run the following command for that corner: `defaults write ~/Library/Preferences/com.apple.dock.plist wvous-$CORNER-modifier -int 0`
*No prevent screen saver hot corner[54]	For any corner that would prevent the screen saver, run the following command for that corner: `defaults write ~/Library/Preferences/com.apple.dock.plist wvous-$CORNER-corner -int 1`
*Desktop idle time	`defaults write ~/Library/Preferences/com.apple.dock.plist idleTime -int 1200`

* See Appendix H to determine what processes may need to be restarted for the setting to take effect.

[54] Use one of the codes "`bl`," "`br`," "`tl`," or "`tr`" in place of `$CORNER`; where "bl" is bottom left, "tr" is top right, etc.

J.8. Firewalls

Table 36: Application Firewall Settings

Setting Name	Terminal Command
Turn on firewall	`/usr/libexec/ApplicationFirewall/socketfilterfw --setglobalstate on`
Turn on firewall and block all incoming connections	`/usr/libexec/ApplicationFirewall/socketfilterfw --setblockall on`
Automatically allow signed software to receive incoming connections	`/usr/libexec/ApplicationFirewall/socketfilterfw --setallowedsigned on`
*Enable firewall logging	`/usr/libexec/ApplicationFirewall/socketfilterfw --setloggingmode on`

* See Appendix H to determine what processes may need to be restarted for the setting to take effect.

The `pf` firewall is separate from the application firewall, and offers finer-grained controls. Before making changes to `pf` settings, be sure to back up the `/etc/pf.conf` file. The `pf` firewall must be configured to run automatically on system startup in order to maintain persistence. The `pf` firewall needs to be directed to a configuration file with the desired anchor points. An anchor point allows a set of firewall rules to be loaded from another file. An anchor is first defined, and then loaded in from a specified file.

Firewall rules must be constructed and placed in a custom anchor file specified in `/etc/pf.conf`. For example, incoming SSH connections can be blocked with the following rule: `block in proto { tcp udp } to any port 22`. This instructs `pf` to block incoming traffic using the TCP or UDP protocols destined for any IP address on port 22. The full set of recommendations for `pf` firewall rules is available in Table 2. The Terminal configuration commands are available below in Table 37.

Table 37: pf Firewall Settings

Action	Terminal Command
Turn on firewall	`pfctl –e`
*Run firewall automatically on system startup	`defaults write /System/Library/LaunchDaemons/com.apple.pfctl ProgramArguments '(pfctl, -f, /etc/pf.conf, -e)'`

Define and add custom anchor to config file	`echo 'anchor "sam_pf_anchors"' >> /etc/pf.conf`
	
	`echo 'load anchor "sam_pf_anchors" from "/etc/pf.anchors/sam_pf_anchors"' >> /etc/pf.conf`

Load a `pf` configuration	`pfctl –f /etc/pf.conf`

* See Appendix H to determine what processes may need to be restarted for the setting to take effect.

J.9. Sharing Services

Table 38: Sharing Settings

Setting Name	Terminal Command
*Disable Bluetooth file sharing	`defaults write ~/Library/Preferences/ByHost/com.apple.Bluetooth.$HW_UUID.plist PrefKeyServicesEnabled -bool false`
Disable printer sharing	`cupsctl --no-share-printers`
Disable remote login	`systemsetup -f -setremotelogin off`
Disable remote Apple events	`systemsetup -setremoteappleevents off`

*Disable remote Apple events for specific users	`defaults write /private/var/db/dslocal/nodes/Default/groups/com.apple.access_remote_ae.plist users –array "";`
	
	`defaults delete /private/var/db/dslocal/nodes/Default/groups/com.apple.access_remote_ae.plist groupmembers;`
	
	`defaults delete /private/var/db/dslocal/nodes/Default/groups/com.apple.access_remote_ae.plist nestedgroups`

* See Appendix H to determine what processes may need to be restarted for the setting to take effect.

J.10. SSH Daemon

In the table below, the italicized text in the "Value" column is not the actual value to input in the configuration file, but rather a suggested restriction of values.

Table 39: SSH Settings

Key Name	Value
`LoginGraceTime`	`30`
`Ciphers`	*Required: cipher names that begin with "3des" or "aes"* *Disallowed: ciphers with names ending in "cbc"*
`MACs`	`hmac-sha1`
`ChallengeResponseAuthentication`	`no`
`PasswordAuthentication`	`yes`
`PubkeyAuthentication`	`no`
`DenyUsers`	`*`

Key Name	Value
`ClientAliveInterval`	`300`
`maxAuthTries`	`4`
`PermitRootLogin`	`no`
`LogLevel`	`VERBOSE`
`PermitEmptyPassword`	`no`
`PermitUserEnvironment`	`no`
`Protocol`	`2`
`X11Forwarding`	`no`
`ClientAliveCountMax`	`0`

J.11. Wireless Networking

Table 40: Wireless Networking Settings

Setting Name	Terminal Command
Don't open Bluetooth setup assistant if no keyboard detected	`defaults write /Library/Preferences/com.apple.Bluetooth.plist BluetoothAutoSeekKeyboard -bool false`
Don't open Bluetooth setup assistant if no mouse or trackpad detected	`defaults write /Library/Preferences/com.apple.Bluetooth.plist BluetoothAutoSeekPointingDevice -bool false`
*Show Bluetooth status in menu bar	`defaults write ~/Library/Preferences/com.apple.systemuiserver.plist menuExtras -array-add "/System/Library/CoreServices/Menu\ Extras/Bluetooth.menu"`
*Disallow Bluetooth devices to wake the computer	`defaults write ~/Library/Preferences/ByHost/com.apple.Bluetooth.$HW_UUID.plist RemoteWakeEnabled -bool false`
Remove preferred wireless networks	`networksetup -removeallpreferredwirelessnetworks $DEVICE_NAME` *This setting is only recommended for SSLF systems.*
*Show Wi-Fi status in menu bar	`defaults write ~/Library/Preferences/com.apple.systemuiserver.plist menuExtras -array-add /System/Library/CoreServices/Menu\ Extras/AirPort.menu`
*Disable AirDrop	`defaults write ~/Library/Preferences/com.apple.NetworkBrowser.plist`

Setting Name	Terminal Command
	`DisableAirDrop -bool true`

* See Appendix H to determine what processes may need to be restarted for the setting to take effect.

J.12. Network Services

Table 41: Network Services Settings

Setting Name	Terminal Command
Change LocalHostName	`scutil --set LocalHostName $HOST_ID`
Change HostName	`scutil --set HostName $HOST_ID`
Change ComputerName	`scutil --set ComputerName $HOST_ID`
Change NetBIOSName	`defaults write /Library/Preferences/SystemConfiguration/com.apple.smb.server.plist NetBIOSName $HOST_ID`
*Disable Bonjour advertising	`defaults write /System/Library/LaunchDaemons/com.apple.mDNSResponder.plist ProgramArguments -array-add "-NoMulticastAdvertisements"`
Remove all .netrc files	`find / -name .netrc 2> /dev/null -exec srm {} +`
Use 2 DNS servers[55]	`networksetup -setdnsservers [networkservice] server1, server2`

Use Network Time Protocol (NTP)	`systemsetup -setnetworktimeserver $ADDRESS`
	
	`systemsetup -setusingnetworktime on`

*Restrict screen sharing to no users	`defaults write /private/var/db/dslocal/nodes/Default/groups/com.apple.access_screensharing.plist users -array ""`
	
	`defaults delete /private/var/db/dslocal/nodes/Default/groups/com.apple.access_screensharing.plist groupmembers`
	
	`defaults delete /private/var/db/dslocal/nodes/Default/groups/com.apple.access_screensharing.plist nestedgroups`

Disable remote management	`/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/Resources/kickstart -quiet -deactivate -stop`
Restrict remote management to specific users	`/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/Resources/kickstart –quiet –configure -allowAccessFor –specifiedUsers –access -off`

[55] [network service] is one of the services listed from running the command `networksetup –listallnetworkservices`

* See Appendix H to determine what processes may need to be restarted for the setting to take effect.

J.13. Software Updates

Table 42: Software Update Settings

Setting Name	Terminal Command
Update Apple software	`softwareupdate -ia`
Enable updates download in background	`defaults write /Library/Preferences/com.apple.SoftwareUpdate.plist AutomaticDownload -bool true`
Enable system data updates	`defaults write /Library/Preferences/com.apple.SoftwareUpdate.plist ConfigDataInstall -bool true`
Enable system security updates	`defaults write /Library/Preferences/com.apple.SoftwareUpdate.plist CriticalUpdateInstall -bool true`

J.14. CD and DVD Preferences

Table 43: CD and DVD Settings

Setting Name	Terminal Command
*Disable blank CD actions	`defaults write ~/Library/Preferences/com.apple.digihub.plist com.apple.digihub.blank.cd.appeared -dict action -int 1`
*Disable blank DVD actions	`defaults write ~/Library/Preferences/com.apple.digihub.plist com.apple.digihub.blank.dvd.appeared -dict action -int 1`
*Disable music CD actions	`defaults write ~/Library/Preferences/com.apple.digihub.plist com.apple.digihub.cd.music.appeared -dict action -int 1`
*Disable picture CD actions	`defaults write ~/Library/Preferences/com.apple.digihub.plist com.apple.digihub.cd.picture.appeared -dict action -int 1`
*Disable video DVD actions	`defaults write ~/Library/Preferences/com.apple.digihub.plist com.apple.digihub.dvd.video.appeared -dict action -int 1`

* See Appendix H to determine what processes should be restarted for the setting to take effect.

J.15. Privacy

Table 44: Privacy Settings

Setting Name	Terminal Command
Disable location services	`defaults write /private/var/db/locationd/Library/Preferences/ByHost/com.apple.locationd.$HW_UUID.plist LocationServicesEnabled -bool false`
Disable sending of diagnostic data to Apple	`defaults write ~/Library/Preferences/ByHost/com.apple.SubmitDiagInfo.$HW_UUID.plist AutoSubmit -bool false`

J.16. Power Management

Although most power management settings do not directly affect security, they are still important for effective system use. The one important setting to note is “Display sleep idle time,” which must have a value greater than or equal to the “Desktop idle time” setting in Appendix J.7. If the screen goes to sleep before the session locks, it creates a false sense of security.

Table 45: Power Management Settings

Setting Name	Terminal Command
Sleep computer when power button pressed	`pmset -a powerbutton 1`
Disable computer sleep	`pmset -a sleep 0`
Prevent idle sleep if remote login session is active	`pmset -a ttyskeepawake 1`
Disable wake for network access	`pmset -a womp 0`
Disable hibernate	`pmset -a hibernatemode 0`
Dim display when switched to battery	`pmset -b lessbright 1`
Wake when power source changes	`pmset -a acwake 1`
No auto restart after power failure	`pmset -a autorestart 0`
Hard disk sleep idle time	`pmset -a disksleep 10`
Display sleep idle time	`pmset -a displaysleep 20`

Setting Name	Terminal Command
Enable dimming before display sleep	`pmset -a halfdim 1`
Wake when lid opened	`pmset -a lidwake 1`
Park disk heads on sudden motion	`pmset –a sms 1`

J.17. Miscellaneous Settings

Table 46: Miscellaneous Settings

Setting Name	Terminal Command
*Show Safari status bar	`defaults write ~/Library/Preferences/com.apple.Safari.plist ShowStatusBar -bool true`
*Auto hide Dock	`defaults write ~/Library/Preferences/com.apple.dock.plist autohide -bool true`
*Disable Mission Control Dashboard	`defaults write ~/Library/Preferences/com.apple.dashboard.plist mcx-disabled -bool true` *This setting is only configured on SSLF systems.*

* See Appendix H to determine what processes should be restarted for the setting to take effect.