Macintosh Operating System X

Version 10.6

TECHNOLOGY OVERVIEW

Version 1, Release 0.1

18 August 2011

Developed by DISA for the DoD

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by DISA FSO or any non-Federal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

This page is intentionally left blank.

1 INTRODUCTION

1.1 Background

This Macintosh Operating System X Version 10.6 Technology Overview (or the Mac OS X 10.6 Technology Overview as it will be referred to from here forth), along with the Mac OS X Security Technical Implementation Guide (STIG) provides the technical security policies, requirements, and implementation details for applying security concepts to the Mac OS X system. With this release of the MAC OS X 10.6 STIG the UNIX Security Requirement Guide (SRG) has been used to enhance the security of the underlying UNIX operating system the Mac OS X runs on. Many new vulnerabilities have been added to the STIG as a result of the UNIX SRG.

1.2 Authority

Department of Defense (DoD) Directive (DoDD) 8500.1 requires "all IA and IA-enabled IT products incorporated into DoD information systems shall be configured in accordance with DoD-approved security configuration guidelines" and tasks Defense Information Systems Agency (DISA) to "develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with Director, NSA". This document is provided under the authority of DoDD 8500.1.

Although the use of the principles and guidelines in these STIGs provide an environment contributing to the security requirements of DoD systems operating at Mission Assurance Categories (MACs) I through III, applicable DoD Instruction (DoDI) 8500.2 Information Assurance (IA) controls need to be applied to all systems and architectures.

The Information Operations Condition (INFOCON) for the DoD recommends actions during periods when a heightened defensive posture is required to protect DoD computer networks from attack. The Information Assurance Officer (IAO) will ensure compliance with the security requirements of the current INFOCON level and will modify security requirements to comply with this guidance.

1.3 Scope

This document is a requirement for all DoD-administered systems and all systems connected to DoD networks. These requirements are designed to assist Security Managers (SMs), Information Assurance Managers (IAMs), IAOs, and System Administrators (SAs) with configuring and maintaining security controls. This guidance supports DoD system design, development, implementation, certification, and accreditation efforts.

1.4 Vulnerability Severity Code Definitions

Severity Category Codes (referred to as CAT) are a measure of risk used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Code of CAT I, II, or III. Each policy is evaluated based on the probability of a realized threat occurring and the expected loss associated with an attack exploiting the resulting vulnerability.

Table 1-1. Vulnerability Severity Category Code Definitions

	DISA/DIACAP Category Code Guidelines	Examples of DISA/DIACAP Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will, directly and immediately result in loss of Confidentiality, Availability or Integrity. An ATO will not be granted while CAT I weaknesses are present. **Note**: The exploitation of vulnerabilities must be evaluated at the level of the system or component being reviewed. A workstation for example, is a stand alone device for some purposes and part of a larger system for others. Risks to the device are first considered, then risks to the device in its environment, then risks presented by the device to the environment. All risk factors must be considered when developing mitigation strategies at the device and system level.	Includes **BUT NOT LIMITED** to the following examples of direct and immediate loss: 1. May result in loss of life, loss of facilities, or equipment, which would result in mission failure. 2. Allows unauthorized access to security or administrator level resources or privileges. 3. Allows unauthorized disclosure of, or access to, classified data or materials. 4. Allows unauthorized access to classified facilities. 5. Allows denial of service or denial of access, which will result in mission failure. 6. Prevents auditing or monitoring of cyber or physical environments. 7. Operation of a system/capability which has not been approved by the appropriate Designated Accrediting Authority (DAA). 8. Unsupported software where there is no documented acceptance of DAA risk.
CAT II	Any vulnerability, the exploitation of which has a potential to result in loss of Confidentiality, Availability or Integrity. CAT II findings satisfactorily mitigated will not prevent an ATO from being granted. **Note**: The exploitation of vulnerabilities must be evaluated at the level of the system or component being reviewed. A workstation for example, is a stand alone device for some purposes and part of a larger system for others. Risks to the device are first considered, then	Includes **BUT NOT LIMITED** to the following examples with a potential to result in loss: 1. Allows access to information possibly leading to a CAT I vulnerability. 2. Could result in personal injury, damage to facilities, or equipment which would degrade the mission. 3. Allows unauthorized access to user or application level system resources. 4. Could result in the loss or compromise of sensitive information. 5. Allows unauthorized access to Government or Contractor owned or leased facilities.

	DISA/DIACAP Category Code Guidelines	Examples of DISA/DIACAP Category Code Guidelines
	risks to the device in its environment, then risks presented by the device to the environment. All risk factors must be considered when developing mitigation strategies at the device and system level.	6. May result in the disruption of system or network resources degrading the ability to perform the mission. 7. Prevents a timely recovery from an attack or system outage. 8. Provides unauthorized disclosure of or access to unclassified sensitive, Personally Identifiable Information (PII), or other data or materials.
CAT III	Any vulnerability, the existence of which degrades measures to protect against loss of Confidentiality, Availability or Integrity. Assigned findings possibly impacting IA posture but are not required to be mitigated or corrected in order for an ATO to be granted. **Note**: The exploitation of vulnerabilities must be evaluated at the level of the system or component being reviewed. A workstation for example, is a stand alone device for some purposes and part of a larger system for others. Risks to the device are first considered, then risks to the device in its environment, then risks presented by the device to the environment. All risk factors must be considered when developing mitigation strategies at the device and system level.	Includes **BUT NOT LIMITED** to the following examples that provide information which could potentially result in degradation of system information assurance measures or loss of data: 1. Allows access to information possibly leading to a CAT II vulnerability. 2. Has the potential to affect the accuracy or reliability of data pertaining to personnel, resources, operations, or other sensitive information. 3. Allows the running of any applications, services or protocols not supporting mission functions. 4. Degrades a defense in depth systems security architecture. 5. Degrades the timely recovery from an attack or system outage. 6. Indicates inadequate security administration. 7. System not documented in the sites C&A Package/System Security Plan (SSP). 8. Lack of document retention by the Information Assurance Manager (IAM) (i.e., completed user agreement forms).

1.5 STIG Distribution

Parties within the DoD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) web site. This site contains the latest copies of any STIG, as well as checklists, scripts, and other related security information. The Non-classified Internet Protocol Router Network (NIPRNet) Uniform Resource Locator (URL) for the IASE web site is http://iase.disa.mil/.

1.6 Document Revisions

Comments or proposed revisions to this document should be sent via email to fso_spt@disa.mil. DISA Field Security Operations (FSO) will coordinate all change requests with the relevant DoD organizations before inclusion in this document.

2 PERFORMING A MAC REVIEW

2.1 General Information

This Mac OS X 10.6 Technology Overview document introduces security concepts and terminology used in the Mac OS X STIG. This document is not a guide to Mac OS X system administration.

The security requirements contained within the Mac OS X STIG are applicable to all DoD-administered systems and all systems connected to DoD networks. The STIG provides requirements and associated procedures to reduce the security vulnerabilities of the Mac OS X system. These requirements are designed to assist SMs, IAMs, IAOs, and SAs with configuring and maintaining security controls in the Mac OS X environment.

An important aspect of computer security is the granting or denying of access permissions (sometimes called access rights). A permission is the ability to perform a specific operation, such as gaining access to data or to execute code. Permissions are granted at the level of folders, subfolders, files, or applications. Permissions are also granted for specific data in files or application functions. Permissions in the Mac OS X are controlled at many levels, from the Mach and Berkeley Software Distribution (BSD) components of the kernel through higher levels of the OS, and—for networked applications—through network protocols.

The STIG currently provides manual checks and fixes for the Mac OS X 10.6. As with many OSs, there are multiple ways to perform the same checks. This document is not intended to provide all command line variations; it is designed to provide a way to check a security setting and provide a fix for that setting. These settings are designed for a desktop system intended for general business use which is connected to a wide-area network. Such systems typically connect to an Active Directory domain or some other Directory Service system for user authentication. These settings are not intended for Mac OS X used as a server system.

Several of the fixes need to be repeated after a system update. A system update is an update to the MAC OS X and not an application software update (for example, updating MAC OS X from 10.6.4 to 10.6.6).

2.2 Access Privileges

The SA should be familiar with both the command line utilities as well as the GUI for securing the system. For many checks, elevated privileges are required; both SU and SUDO commands are used and may require a secondary administrator login for the command to complete. If an "access denied" is returned from the use of a command, it is most likely due to inadequate rights to the objects. When performing the GUI checks, an administrator password may be needed to unlock the "Lock" icon for access to secured options. The SA should also be familiar with the inherent text editors of the Mac OS X for viewing and editing checks.

2.3 Mac OS X Architecture

Mac OS X is built from the BSD UNIX and Mach kernels. Among other things, BSD provides basic file system and networking services and implements user and group identification (ID) schemes. BSD enforces access restrictions to files and system resources based on user and group IDs. Mach provides memory management, thread control, hardware abstraction, and interprocess communication. Mach enforces access by controlling which tasks can send a message to a Mach port. (A Mach port represents a task or another resource.) BSD security policies and Mach access permissions constitute an essential part of security in the Mac OS X, and both are critical to enforcing local security.

3 OPEN SOURCE SOFTWARE (OSS) POLICY

Mac OS X security services are built on two open source standards:

- A *Berkeley Software Distribution (BSD).* BSD is a form of UNIX providing fundamental services, including the UNIX file system and file access permissions.
- A *Common Data Security Architecture (CDSA).* CDSA provides a wide array of security services, including more specific access permissions, authentication of user identities, encryption, and secure data storage.

DoD has clarified policy on the use of OSS to take advantage of the capabilities available in the Open Source community, as long as certain prerequisites are met. DoD no longer requires that OS software be obtained through a valid vendor channel and have a formal support path if the source code for the OS is publicly available for review.

From the DoD Chief Information Officer (CIO) Memo, Open Source Software (OSS) in Department of Defense (DoD), 28 May 2003:

"DoD Components acquiring, using or developing OSS must ensure that the OSS complies with the same DoD policies that govern Commercial-Off-The-Shelf (COTS) and Government-Off-The Shelf (GOTS) software. This includes, but is not limited to, the requirements that all information assurance (IA) or IA-enabled IT hardware, firmware and software components or products incorporated into DoD information systems whether acquired or originated within DoD;

- Comply with the evaluation and validation requirements of National Security Telecommunications and Information Systems Security Policy Number 11 and;
- Be configured in accordance with DoD-approved security and configuration guidelines at http://iase.disa.mil/ and http://www.nsa.gov/."

OSS takes several forms and may be acceptable or unacceptable depending on the form:

1. A utility with a publicly available source code is acceptable.
2. A commercial product incorporating OSS is acceptable because the commercial vendor provides a warranty.
3. Vendor-supported OSS is acceptable.
4. A utility that comes compiled and has no warranty is not acceptable.

The DoDD 8500.1 states: "Public domain software products, and other software products with limited or no warranty, such as those commonly known as freeware or shareware, shall only be used in DoD information systems to meet compelling operational requirements. Such products shall be thoroughly assessed for risk and accepted for use by the responsible DAA."

This page is intentionally left blank.

APPENDIX A. ACRONYMS

ATO	Authority To Operate
BSD	Berkeley Software Distribution. A version of UNIX
C&A	Certification and Accreditation
CAT	Category Codes (for Mission Assurance Category)
CDSA	Common Data Security Architecture
CIO	Chief Information Officer
CNDSP	Computer Network Defense Service Provider
COTS	Commercial Off The Shelf
CTO	Communication Tasking Order
CYBERCOM	Cyber Command
DAA	Designated Accrediting Authority
DIACAP	Department of Defense (DoD) Information Assurance Certification and Accreditation (C&A) Process
DISA	Defense Information Systems Agency
DoD	Department of Defense
DoDD	DoD Directive
DoDI	DoD Instruction
FSO	Field Security Operations
GOTS	Government Off The Shelf
GUI	Graphical User Interface
IA	Information Assurance
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IASE	Information Assurance Support Environment
IAVM	Information Assurance Vulnerability Management
ID	Identification
INFOCON	Information Operations Condition
IT	Information Technology
JTF-GNO	Joint Task Force - Global Network Operations
Mac	Macintosh
MAC	Mission Assurance Category
NIPRNet	Non-classified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OS	Operating System
OSS	Open Source Software
PII	Personally Identifiable Information
SA	System Administrator
SM	Security Manager
SRG	Security Requirement Guide
STIG	Security Technical Implementation Guide
SU/SUDO	Super User- Super User Do
URL	Uniform Resource Locator
WARNORDs	Warning Orders

This page is intentionally left blank.

APPENDIX B. RELATED PUBLICATIONS

Government Publications

Department of Defense, DoD Directive (DoDD) 8500.1, "Information Assurance (IA)", 24 October 2002.

Department of Defense, DoD Instruction (DoDI) 8500.2, "Information Assurance (IA)", 6 February 2003.

Executive Office of the President, Office of Management and Budget Memorandum, "Protection of Sensitive Agency Information", 23 June 2006.

National Security Agency (NSA), "Hardening Tips For Default Installation of Mac OS X 10.6 Leopard"

Technical Publications

Mac OS X Security Configuration For Mac OS X Version 10.6 Snow Leopard
Apple Inc. © 2010 Apple Inc.

Common Criteria Configuration and Administration Guide
Apple Computer, Inc. © 2005 Apple Computer, Inc. All rights reserved.

This page is intentionally left blank.