Administering Your HP-UX Trusted System

HP 9000 Computer Systems

HP Part No. B2355-90121
Printed in USA August 1996

First Edition
E0896

Legal Notices

The information in this document is subject to change without notice.

Hewlett-Packard makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Warranty. A copy of the specific warranty terms applicable to your Hewlett-Packard product and replacement parts can be obtained from your local Sales and Service Office.

Restricted Rights Legend. Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DoD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

HEWLETT-PACKARD COMPANY
3000 Hanover Street
Palo Alto, California 94304 U.S.A.

Use of this manual and flexible disk(s) or tape cartridge(s) supplied for this pack is restricted to this product only. Additional copies of the programs may be made for security and back-up purposes only. Resale of the programs in their present form or with alterations, is expressly prohibited.

Copyright Notices.

©copyright 1996 Hewlett-Packard Company, all rights reserved.

Reproduction, adaptation, or translation of this document without prior written permission is prohibited, except as allowed under the copyright laws.

©copyright 1979, 1980, 1983, 1985-93 Regents of the University of California

This software is based in part on the Fourth Berkeley Software Distribution under license from the Regents of the University of California.

©copyright 1980, 1984, 1986 Novell, Inc.
©copyright 1986-1992 Sun Microsystems, Inc.
©copyright 1985-86, 1988 Massachusetts Institute of Technology.
©copyright 1989-93 The Open Software Foundation, Inc.
©copyright 1986 Digital Equipment Corporation.
©copyright 1990 Motorola, Inc.
©copyright 1990, 1991, 1992 Cornell University
©copyright 1989-1991 The University of Maryland
©copyright 1988 Carnegie Mellon University

Trademark Notices

UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Limited.

X Window System is a trademark of the Massachusetts Institute of Technology.

MS-DOS and Microsoft are U.S. registered trademarks of Microsoft Corporation.

OSF/Motif is a trademark of the Open Software Foundation, Inc. in the U.S. and other countries.

Printing History

The manual printing date and part number indicate its current edition. The printing date will change when a new edition is printed. Minor changes may be made at reprint without changing the printing date. The manual part number will change when extensive changes are made.

Manual updates may be issued between editions to correct errors or document product changes. To ensure that you receive the updated or new editions, you should subscribe to the appropriate product support service. See your HP sales representative for details.

First Edition: August 1996 (HP-UX Release 10.10)

Preface

This manual describes tasks required for configuring and administering an HP- UX system as a C-2 level trusted system. This manual is for system administrators with superuser privilege and should be restricted to those with the proper authority.

This manual is written assuming that you are familiar with HP-UX system administration including using standard system commands, the System Administration Manager (SAM), system and device installation, system configuration, managing users, and performing routine maintenance tasks. This information is covered in *HP-UX System Administration Tasks* (B2355- 90079) and the online HP-UX man pages.

The section "HP-UX C-Level Security Trusted Facility Documentation" in Chapter 1 of this manual describes additional documentation that you may need.

Manual Organization

This manual is organized as follows:

Chapter 1	Description of the HP-UX Trusted System
Chapter 2	Installation and Configuration of an HP-UX Trusted System
Chapter 3	Practices that Enforce the Trustworthiness of the System
Chapter 4	Practices that Compromise the Trustworthiness of the System
Appendix A	Audit Record Format
Appendix B	Commands and System Calls
Appendix C	SFUG Supplement

Conventions Used in this Manual

This manual uses the following typographic conventions:

Boldface	Words in boldface are terms defined for the first time.
`Underlined Computer`	Underlined computer font indicates items you type. For example: `/usr/sbin/newfs`
`Computer`	Computer font within text indicates HP-UX commands, utilities, and SAM menu items.
Italics	Italics indicates manual titles, emphasized words, parameters to an HP-UX command, and entries in the *HP-UX Reference*.
Return	Words or letters in boxes refer to keys on the keyboard or a control button within SAM.
. . .	Ellipses in examples indicate that part or parts of the example might be omitted.

Contents

Tables

1

Description of the HP-UX Trusted System

The Hewlett-Packard C2-level trusted system consists of the HP-UX Release 10.10 operating system configured in trusted mode and its commands, utilities, and subsystems along with supported hardware. This results in a system designed to meet the criteria of a C2-level trusted system, as described in Section 2.2 of the *Department of Defense Trusted Computer System Evaluation Criteria*, DOD 5200.28-STD, December 1985, and the E3/FC2 security level as definded by the Information Technology Security Evaluation Criteria (ITSEC) established by the European Community.

This chapter defines a trusted system. It introduces fundamental security terms and concepts and summarizes the major security features enforced by the HP-UX C2-level system. It provides an overview of the HP-UX C2-level system and outlines administrative roles and functions necessary to maintain a trusted system. It also discusses background for planning system security including a section on developing a security policy for your department.

Note This chapter is written for system administrators whose responsibility it is to maintain the system. When this chapter refers to "you," it is directed towards such system administrators, presumably those having superuser (root) privilege on the HP-UX C2-level system.

Background Required

To effectively use this manual and to be able to ensure your system's security, you should be familiar with HP-UX system administration as described in *HP-UX System Administration Tasks*. You should have experience with

- Installing and configuring HP-UX and peripherals
- Changing system parameters
- Managing user accounts
- Disk management
- File systems
- Backing up data
- Solving system problems

What is a Trusted System?

A *trusted system* is one that can be relied upon to perform correctly in two important ways:

- The system's operational features—in particular, its application interface—work correctly and satisfy the computing needs of the system users.
- The system's security features provide the mechanisms necessary to enforce the site's security policy and provide protection from threats.

A *security policy* is a statement of the rules and practices that regulate how an organization manages, protects, and distributes sensitive information. HP-UX C2-level security expands on existing HP-UX security mechanisms. Organizations need to make the following procedures and guidelines described in this manual part of their security policy.

What is C2-Level Trusted Mode?

You can configure HP-UX in either the C2-level trusted mode or the untrusted mode. For the purposes of this chapter, the HP-UX trusted system being defined is one which is configured in the C2-level trusted mode.

In the untrusted mode, HP-UX offers the security mechanisms available in the standard UNIX environment. When configured in the trusted mode, HP-UX provides additional security features such as a more stringent password and authentication system, auditing, terminal access control, and time-base access controls.

C2-level trusted HP-UX protects the system and its users against a variety of threats and system compromises. A *threat* is any event that might cause users at a site to lose the use of computing resources or any of the information stored on them.

The Trusted Computing Base (TCB) is the totality of hardware and software protection mechanisms designed to enforce the system's security policy. It includes all the code that runs with hardware privilege (that is, the operating system or kernel) and all code running in processes that cooperate with the operating system to enforce the security policy.

The TCB oversees and monitors interactions between *subjects* (active entities such as processes) and *objects* (passive entities such as files, devices, and interprocess communication mechanisms). The TCB is protected from unauthorized modification and provides mechanisms that support the authentication and accountability requirements of a C-2 level system.

Parts of the TCB

The TCB includes the following:

- A modified HP-UX kernel
- Trusted commands and utilities
- Trusted hardware and firmware

The TCB consists of hardware and software components that enforce the correct operation of the system's security policies while the system is running

in secure multiuser mode. This includes both the trusted and untrusted portions of the HP-UX operating system.

Some of the trusted commands and utilities in the TCB can cause the system to leave its secure state (for example, to shutdown or reboot the system). The TCB also includes *sam*(1M), HP's System Administration Manager. Refer to "System Administration Tasks" later in this chapter for more information on SAM. Security-related commands and system roles are listed in Appendixes B and C.

Excluded from the TCB

The TCB does not include the following:

- Compilers
- Configuration management tools
- System debugging and diagnostic tools
- System generation utilities
- Networking
- X11 or Motif Windows
- Journaled File Systems (JFS or VxFS)
- Other untrusted commands and utilities

Although these tools are trusted to work correctly to configure the system, they play no role in enforcing security policies while the system is in operation.

TCB Interface

Processes (or users interacting with a process at a terminal) request services from the TCB in the following ways:

- A process can execute unprivileged hardware instructions
- A process can execute system calls
- A user or process can interact with non-kernel TCB trusted program and trusted library interfaces

Note Users can write programs that bypass the system call interface and invoke trap instructions directly. All system security policy decisions are made in kernel code that is accessible only through invocation of the trap instruction. All user actions that involve policy decisions must eventually go through the trap interface. Therefore, system security policy cannot be violated or bypassed.

Trusted System Administration

The administration of a C2-level HP-UX system is your responsibility as system administrator.

HP-UX generally supports two types of users:

- Regular users, given limited access to the system
- Superusers, given unlimited access to the system

HP-UX provides C2-level security in a multiuser environment. Users can authorize or restrict access to files they own. This is accomplished by means of a discretionary access control (DAC) policy which is enforced through Access Control Lists (ACLs) and traditional UNIX access controls specified using protection bits.

The superuser can customize SAM to meet specific system needs and needs of individual users. SAM supports separate operator and administrative functions by allowing the superuser to enable or disable access to specific task menus.

Administering an HP-UX system and its users is normally done using *sam*(1M), a menu-driven interface program.

System Administration Manager

HP's System Administration Manager, *sam*(1M), is included as part of the TCB in a C2-level trusted HP-UX system. SAM provides an easy-to-use interface for performing setup and other essential system administration tasks.

Note SAM can only be used in character mode in a trusted system.

By default, only the superuser can use *sam*(1M). The superuser may optionally set up a restricted *sam*(1M) to allow particular users to administer specific functional areas of *sam*(1M). The *sam*(1M) main menu is the list of functional areas. In addition, *sam*(1M) maintains a log of actions taken by system administrators including actions that change the system configuration.

Trusted Computer System Evaluation Criteria

With the National Computer Security Center (NCSC) of the National Security Agency (NSA), the US Government sets standards for trusted systems and performs evaluations of systems submitted by vendors. During the evaluation process, the systems are subjected to detailed analysis and testing of both operational features and security features.

The Department of Defense's *Trusted Computer System Evaluation Criteria (TCSEC)* describes a graded classification of trusted systems (levels A, B, C, and D) and specifies the criteria that distinguishes each class. Each class offers increased security features so that level D is the least strict and level A assures maximum, verified protection.

Systems are evaluated using the criteria specified in the *TCSEC*. Based on the result of the evaluation, a system earns an overall rating showing the degree of trust that can be placed in the evaluated system.

The *TCSEC* defines two types of requirements for each of the classes defined: *features* and *assurance.* These requirements have to be addressed during the design, implementation, and testing of a trusted system.

- Features are visible functions that carry out the security policy of a system.
- Assurances are tasks that the system implementor must complete to guarantee that the system meets specifications.

HP-UX complies with (and in many instances exceeds) the TCSEC requirements for the C2 class. Table 1-1 summarizes the TSCEC features and assurances that must be satisfied by a C2-level trusted system. The sections that follow describe each of these requirements in greater detail and summarize the impact of these requirements on administrator responsibilities.

Table 1-1. TCSEC C2-Level System Features

Requirement	Description
Discretionary access control (DAC)	An owner of an object containing data must be able to allow or deny access to that object based on a need-to-know basis.
Object reuse	When an object is initially assigned, allocated, or reallocated to a subject, that object must not contain any data that the subject is not authorized to access.
Identification and authentication	Individuals must identify themselves to the system to use it, and the system must be able to authenticate users' identities.
Audit	Users must be accountable for their actions. The system records an audit trail of each security-related event and who caused the event.
System architecture	The system must isolate areas that require protection via access control and auditing.
System integrity	The system needs to include features that allow periodic validation of the hardware and firmware.

Discretionary Access Control

Using discretionary access control (DAC), owners of objects containing data can allow or deny access to these objects at their own discretion, on a need- to-know basis. Objects are things such as files, devices, or interprocess communications mechanisms that another user or the user's process is attempting to access.

Users of standard HP-UX systems protect objects, such as files, by establishing read, write, and access permissions to these objects. The owner can set permissions on objects so that the owner of the object is allowed different accesses from other group members; group members can have different access to an object than the rest of the user community. The owner can change these protection attributes so they are more restrictive (controlled access) or more permissive (open access).

The *TCSEC* requires the C2-level of trust to have discretionary controls on an object that are *capable of including or excluding access to the granularity of a single user.* In other words, the owner of a file must be able to specify that one user is authorized to access a file in a certain way, or that one user is denied access to a file while all others are allowed access.

Access control lists (called ACLs), used with standard HP-UX protections make it possible to define a highly customized access to specify objects. The ACL of an object contains entries that control types of access permitted. Individual users create and maintain ACLs at their own discretion using the *chacl*(1), *lsacl*(1), and *getaccess*(1) commands.

For more information on ACLs, refer to the *chacl*(1), *lsacl*(1), and *getaccess*(1) man pages and to "Managing Access to Files and Directories" in Chapter 12 of *HP-UX System Administration Tasks.*

Object Reuse

The system ensures that an object that is assigned, allocated, or reallocated does not contain data (from a previous use) that the new user is not authorized to access. Object reuse security prevents information from being disclosed inadvertently when storage is released by one user and made available to another.

The C2-level of trusted HP-UX uses standard HP-UX mechanisms to clear newly allocated disk blocks and memory pages. It extends standard mechanisms for authentication to clear buffers containing passwords immediately after they are encrypted.

Identification and Authentication

The *TCSEC* requires users to identify themselves to the TCB before performing any actions that the TCB must mediate. The TCB will maintain data to verify the identity of individual users, thus authenticating each user. Stringent identification and authentication requirements are necessary on a trusted system. The purpose of these requirements is to ensure users are held accountable for their actions.

On a standard HP-UX system, the user logs in by entering a user name and password. The system searches `/etc/passwd` for the user name and authenticates the user by comparing the entered password with the encrypted version of the password in `/etc/passwd`. HP-UX includes more stringent password authentication through a password management mechanism that is designed to meet the objectives and recommendations of the DoD *Password Management Guideline*, CSC-STD-002-85. Several security databases protect and control the following:

- Passwords
- Terminal access
- System defaults
- Device assignments

You and the entire administrative staff must take responsibility for maintaining the authentication information stored by the system for each user. Tasks include creating new user accounts and changing account information as users enter and leave the HP-UX system.

Audit

In a trusted system, all users are held accountable for their actions. That is, any security-relevant action must be traceable to a particular responsible user. Some features of standard HP-UX make accountability difficult because some actions (such as those performed by pseudo-user accounts like *lp* or *cron*) cannot be traced to a specific user.

The HP-UX C2-level auditing subsystem logs security-related events to ensure user accountability. An audit trail records security-relevant events, such as instances of access by subjects to objects, and allows detection of any attempts to bypass the protection mechanism. You can examine the audit trail to identify the users responsible for system changes. You can also selectively audit the actions of any user.

You must perform the following tasks for auditing maintenance:

- Configure the audit subsystem and control the events and users that are audited
- Set auditing parameters appropriately for reliable, efficient performance.
- Determine how much information to collect in the audit trail and maintain the information once it has been collected
- Analyze the audit trail to monitor system activities.

You can administer the auditing subsystem in two ways:

- Using the "Auditing and Security" window in *sam*(1M), the System Administration Manager. Only the character version of *sam*(1M) can be used.
- Using several HP-UX commands including *audsys*(1M), *audusr*(1M), *audevent*(1M), *audisp*(1M), and *audomon*(1M).

In summary, the auditing subsystem acts as a deterrent against system abuses and exposes potential security weaknesses in the system. However, it is still your responsibility as the system administrator to turn on auditing, monitor appropriate system activities, detect, and report any unauthorized or suspect activity.

System Architecture

The system needs to be organized in such a way that the areas requiring protection can be isolated from the rest of the system. In this way, access to these areas can be controlled, monitored, audited, and protected from unauthorized access.

System Integrity

The enforcement of security must be extended to system hardware and software features so that correct operation of the system can be verified. This provides an assurance that the security policy is implemented correctly and that the system security features accurately enforce the control objectives.

Planning System Security

The key to running a secure trusted system is planning and developing a security policy. This section provides some general guidelines on HP-UX system security.

However, realize that establishing and implementing a security policy is an extensive and complicated process. Complete coverage of system security is beyond the scope of this document. You should consult computer security trade books and adopt security measures that suit your business needs. One useful book to refer for additional information is *Practical UNIX Security (Second Edition)* by S. Garfinkel and G. Spafford. This book is available from your local computer bookstore or by ordering ISBN 1-56592-148-8 from O'Reilly & Associates, Inc. at 1-800-998-9938 or via email at ORDER@ORA.COM.

This book is required for administration of your trusted system.

System Security Policy

The system enforces a security policy which is a combination of mode permission bits and access control lists. The policy can be stated, in real world terms, as follows:

> A person may read a document if: (1) the person owns the document, (2) if the document's owner allows him or her to, (3) if the person is a member of a group which owns the document and group read permission is set, or (4) if read permission of the document is universally granted.
>
> A person may alter or modify a document if: (1) the person owns the document, (2) if the document's owner allows him or her to, (3) if the person is a member of a group that owns the document and group write permission is set, or (4) if write permission of the document is universally granted.
>
> A person may execute a document if: (1) the person owns the document, (2) if the document's owner allows him or her to, (3) if the person is a member of a group that owns the document and group execute permission is set, or (4) if execute permission of the document is universally granted.

Developing a Security Policy

Before you convert your system to a trusted system, your security policy should consider the following aspects of a computer system:

- Protecting information from unauthorized access
- Protecting information from being deleted or altered
- Keeping the system and the information on it available
- Keeping the system running consistently
- Preventing unauthorized access to the system
- Auditing or tracking system activity

Establishing your security policy should be a joint effort between the technical staff and senior management. Your security policy should conform to your organization's laws and regulations.

Approaching System Security

Following are steps to perform as a general approach to system security:

- Identify what you need to protect. These are your assets such as employees, system hardware, data (onsite and offsite), and documentation.
- Identify potential threats to your assets. These include threats from nature (floods, earthquakes), ignorance and lack of training, and intentional security breaches.
- Implement measures that will protect your assets in a cost effective manner.

Securing System Users

Maintaining system security involves securing system users as follows:

- **Identification of Users.** All users must have a unique login identity (ID) consisting of an account name and password.
- **Authentication of Users.** When a user logs in, the system authenticates the password by checking for its existence in the password database.
- **Authorization of Users.** At a system level, HP-UX provides two kinds of authorized computer use—regular and superuser. Individual users also may be granted or restricted access to system files through traditional file permissions, access control lists, and Restricted SAM.

HP-UX C-Level Security Trusted Facility Documentation

One of the requirements specified in the Department of Defense's *Trusted Computer System Evaluation Criteria (TCSEC)* is for documentation that must include specific information about the C2-level System being evaluated.

The following manuals are required:

- *Security Features User's Guide* describes the protection mechanisms provided by the TCB for system users.
- *Trusted Facility Manual* presents administrative considerations including which functions and privileges should be controlled on a trusted system,

procedures for examining and maintaining audit trails, and other system administration tasks.

Security Features User's Guide

The information required for the *Security Features User's Guide* is aimed at end users. Information must describe system protection mechanisms such as those for file and account protection and provide general security guidelines. The following documents provide the information required for the *Security Features User's Guide*.

For Series 700 systems: *Using Your HP-UX Workstation*

For Series 800 systems: *Using HP-UX*

Note Additional security information is available via HP-UX release 10.10 security patches. This information is in the *SFUG Supplement*. You must print this supplementary security documentation and provide a copy to each of your users to meet C-2 level government requirements.

Printing the SFUG Supplement

There are two ways you can obtain the *SFUG Supplement* to provide copies to your users:

1. Appendix C of this manual contains the *SFUG Supplement*. Simply make copies for your users.
2. You, or your users, can obtain a copy from HP SupportLine on the World Wide Web by following these steps:
   a. Open the URL - http://us.external.hp.com
   b. Click on "Search Problem Solving DBS".
   c. Type "SFUG30" into the Document ID window.
   d. Click "Get Document".

Trusted Facility Manual

This manual, *Administering Your HP-UX Trusted System*, is part of a set of HP-UX manuals that provide the information required in the *Trusted Facility Manual.*

This manual is a pointer to other documents that make up the TFM. The information is all of these documents should be consistent, however, if differences exist this manual contains the most current information.

Hewlett-Packard provides seven documents (including this one) that contain the information needed for the *Trusted Facility Manual*:

- *Administering Your HP-UX Trusted System*
- *Practical UNIX Security* by S. Garfinkel and G. Spafford, Second Edition, O'Reilly & Associates
- *Configuring HP-UX for Peripherals* B2355-90053
- *HP-UX System Administration Tasks* B2355-90079
- *HP-UX Reference* (4 volumes) B2355-90052 (These man pages are available online using the *man* command)
- *Managing HP-UX Software with SD-UX* B2355-90089
- *Read Me Before Installing or Upgrading to HP-UX 10.10* B3782-90074

Table 1-2 specifies the security-relevant topics covered in the documents and indicates their locations in each book.

Table 1-2. Trusted Facility Manual Information Mapping

Manual	Content Relevant to the *Trusted Facility Manual*
Administering Your Trusted System	■ Configuring and installing secure systems (Chapters 1, 2) ■ Operating a system in a secure manner (Chapters 3, 4) ■ Effective use of system privileges and protection mechanisms (Chapters 1, 3, 4) ■ Warnings about possible misuse of authority (Chapters 3, 4) ■ Use of security-related information and additional references (Chapter 1) ■ Limitations of security scope (Chapter 1) ■ Threats to system security (Chapter 4) ■ Security policy and accountability countermeasures (Chapter 2) ■ Security assumptions (Chapter 1) ■ Administrative and routine system vulnerabilities (Chapters 3, 4) ■ Discretionary access control (Chapter 3) ■ Security-relevant operations (Chapter 3, 4) ■ Security-irrelevant procedures (Chapters 2, 3) ■ TCB generation (Chapter 2) ■ TCB vulnerabilities (Chapters 3, 4) ■ Configuration management (Chapters 1, 2) ■ Ratings maintenance plan (Chapter 1) ■ TCB hardware installation (Chapters 1, 2), s ■ Security vulnerabilities of TCB generation, installation, maintenance, and distribution (Chapters 2, 3, 4) ■ *TCSEC* requirements (Chapter 1)

Table 1-2.
Trusted Facility Manual Information Mapping (continued)

Manual	Content Relevant to the *Trusted Facility Manual*
Practical UNIX Security, Second Edition	■ Configuring and installing secure systems (Chapters 1, 5, 19) ■ Operating a system in a secure manner (Chapters 1, 5, 6, 8, 15, 16, 18, 19) ■ Effective use of system privileges and protection mechanisms (Chapters 2, 3, 4, 7, 18) ■ Warnings about possible misuse of authority (Chapters 2, 3, 4, 7, 18) ■ Threats to system security (Chapters 1, 5, 6, 8, 15, 16, 19) ■ Security policy and accountability countermeasures (Chapters 5, 6, 8, 15, 16) ■ Security assumptions (Chapter 19) ■ Administrative and routine system vulnerabilities (Chapters 1, 5, 6, 8, 15, 16, 19) ■ Discretionary access control (Chapters 2, 3, 4) ■ Group membership and object ownership (Chapter 3) ■ User account management (Chapter 3) ■ Identification and authentication (Chapters 2, 3) ■ Security-relevant operations (Chapter 1) ■ TCB file protection (Chapter 4)
Configuring HP-UX for Peripherals	■ Installing, configuring, testing, and managing devices on secure systems (Whole book)

Table 1-2.
Trusted Facility Manual Information Mapping (continued)

Manual	Content Relevant to the *Trusted Facility Manual*
HP-UX System Administration Tasks	■ Configuring and installing secure systems (Chapters 1, 12) ■ Operating a system in a secure manner (Chapter 4) ■ Effective use of system privileges and protection mechanisms (Chapters 2, 4, 9, 12) ■ Warnings about possible misuse of authority (Chapters 12) ■ Threats to system security (Chapter 12) ■ Discretionary access control (Chapter 1, 12) ■ Group membership and object ownership (Chapter 12) ■ User account management (Chapter 12) ■ Identification and authentication (Chapters 1, 12) ■ System login parameters (Chapter 12) ■ Auditing and other security-relevant operations (Chapter 12) ■ System diagnostics, boot, and shutdown (Chapter 2) ■ Setting system clock and configuration parameters (Chapter 1) ■ Damaged data (Chapters 3, 4) ■ TCB file backup (Chapter 9) ■ Mounting/unmounting volumes (Chapters 3, 4) ■ Printers and printer output (Chapter 10) ■ Security-irrelevant procedures (Chapters 1, 5, 9, 10) ■ TCB file protection (Chapter 12) ■ Crash recovery (Chapter 2)

Table 1-2.
Trusted Facility Manual Information Mapping (continued)

Manual	Content Relevant to the *Trusted Facility Manual*
HP-UX Reference	Contains details on all security-relevant commands used for ■ Installing, configuring, and setting up an HP-UX trusted system ■ Auditing ■ Setting ACLs and DAC privileges ■ Encrypting files ■ Setting up and managing user accounts ■ Backing up data ■ Starting and stopping the system ■ Performing routine system maintenance in a secure manner ■ Describes all HP-UX system calls and function definitions including parameters, default settings, effects, and exceptions ■ Many examples of commands, system calls, and functions included
Managing HP-UX Software with SD-UX	■ Configuring and installing secure systems (Chapters 1, 2, 3) ■ System diagnostics (Chapters 3, 5) ■ List of TCB software and approved tools (Chapters 1, 5), ■ TCB generation and loading (Chapters 2, 3) ■ Damaged TCB data structures (Chapters 2, 3, 5) ■ Consistency checking (Chapters 3, 5) ■ Trusted distribution of the TCB (Chapter 2) ■ Correspondence of master and installed copy (Chapters 3, 5)
Read Me Before Installing or Upgrading to HP-UX 10.10	■ Late-breaking information on installing or upgrading to HP-UX Release 10.10 ■ Describes specific configuration details

E3/FC2 ITSEC Security Certification

HP-UX 10.10 has been certified as meeting the E3/FC2 level of security under the Information Technology Security Evaluation Criteria (ITSEC) of the European Community. This certification validates the commercial security functionality of HP-UX.

The following configuration must be installed and maintained for your system to match the system which was evaluated to the ITSEC criteria and to comply with the ITSEC certification:

- HP-UX Release 10.10 installed with the following patches for the Series 700:
  - PHKL_6484
  - PHKL_6662
  - PHKL_6677
  - PHKL_6682
  - PHKL_6716
  - PHKL_6765
  - PHKL_7017
  - PHKL_7055
  - PHKL_7164
  - PHKL_7334
  - PHKL_7458
  - PHKL_7615
  - PHNE_6317
  - PHNE_7152
  - PHNE_7749
  - PHCO_5400
  - PHCO_6587
  - PHCO_6633

- PHCO_6641
- PHCO_6705
- PHCO_6712
- PHCO_6770
- PHCO_6772
- PHCO_6777
- PHCO_6820
- PHCO_6821
- PHC0_6839
- PHCO_6875
- PHCO_7031
- PHCO_7032
- PHCO_7035
- PHCO_7046
- PHCO_7115
- PHCO_7171
- PHCO_7271
- PHCO_7466
- PHCO_6573
- PHCO_6920
- PHCO_7120
- PHC0_7246
- PHCO_7257
- PHCO_7258
- PHCO_7259
- PHCO_7394

- PHCO_7370
- PHCO_7663
- PHKL_7359
- PHNE_6068
- PHNE_6444
- PHNE_6688
- PHNE_6815
- PHNE_6919
- PHNE_6961
- PHNE_6983
- PHNE_6990
- PHNE_7020
- PHNE_7076
- PHNE_7087
- PHNE_7108
- PHNE_7433
- PHSS_6403
- PHSS_6469
- PHSS_6510
- PHSS_6577
- PHSS_6580
- PHSS_6582
- PHSS_6617
- PHSS_6622
- PHSS_7013

And for the Series 800:

- PHCO_6820
- PHNE_7355
- PHCO_6777
- PHCO_6573
- PHCO_6920
- PHCO_7120
- PHCO_7246
- PHCO_7257
- PHCO_7258
- PHCO_7259
- PHCO_7370
- PHCO_7394
- PHCO_7663
- PHKL_6485
- PHKL_6487
- PHKL_6663
- PHKL_6676
- PHKL_6681
- PHKL_6717
- PHKL_6791
- PHKL_7018
- PHKL_7056
- PHKL_7163
- PHKL_7335
- PHKL_7459
- PHKL_7616

- PHNE_6317
- PHNE_4450
- PHCO_5400
- PHCO_6641
- PHCO_6770
- PHCO_6839
- PHCO_6875
- PHCO_7031
- PHCO_7032
- PHCO_7046
- PHCO_7115
- PHCO_7171
- PHCO_7271
- PHCO_7466
- PHKL_7359
- PHNE_6068
- PHNE_6444
- PHNE_6815
- PHNE_6969
- PHNE_6961
- PHNE_6983
- PHNE_6990
- PHNE_7020
- PHNE_7077
- PHNE_7088
- PHNE_7108

  - PHNE_7433
  - PHSS_6403
  - PHSS_6469
  - PHSS_6510
  - PHSS_6577
  - PHSS_6580
  - PHSS_6582
  - PHSS_6617
  - PHSS_6622
  - PHSS_7013
- Networking not configured and the system not connected to a network
- Configured in Trusted Mode
- Auditing enabled
- HP-VUE and X-Windows disabled
- Restricted SAM not used

HP-UX 10.10 was certified in a resticted configuration. Networking was not configured and the system was not connected to a network. HP-VUE and X-Windows were disabled, and Restricted SAM was not used. You must configure your system in the same manner in order to meet the requirements for ITSEC E3/FC2 certification.

HP-VUE and X-Windows must be disabled. This can be done by editing the `/etc/inittab` to set the line `init:4:initdefault:` to init:3:initdefault:"

Do not use Restricted SAM. It is not part of the evaluated configuration.

By following these configuration requirements, you can ensure that your system meets the ITSEC E3/FC2 certification criteria.

2

Installation and Configuration of an HP-UX Trusted System

This chapter describes information that relates to the installation and configuration of an HP-UX system in preparation to converting the system to a C2-level trusted system. This chapter does not include all of the details needed to install your system. That information is provided in other documents to which this chapter refers for more information. This chapter does explain how to convert your already installed or upgraded system to a C2- level trusted system.

Note Your system must be running HP-UX Release 10.10 before you can configure it as a C2-level trusted system.

This chapter includes the following topics:

- Cross references to information about installing or upgrading HP-UX
- Conversion prerequisites
- Setting up your C2-level trusted system
- Auditing trusted systems
- Setting up password controls

Information about Installing or Upgrading HP-UX

HP-UX systems include system configuration logs which describes the current configuration of the system. They are in `/var/adm/su/`. If you change the system by installing or upgrading it, you should maintain the information in the log and keep it up to date. Log all changes and keep that information for future reference.

When preparing to set up a C2-level trusted system, you could be in any of the following situations:

- You have just received a new HP computer and you need to *install* HP-UX Release 10.10 on it.
- You have an HP computer running an HP-UX release prior to Release 10.10. You need to *upgrade* HP-UX to Release 10.10.
- You have an HP computer running HP-UX Release 10.10. Skip to "Conversion Prerequisites."

In the first two cases, you must bring the system up to HP-UX Release 10.10. The installation and upgrade process is beyond the scope of this manual. Refer to additional documentation for information as described below:

- You should read the *Readme Before Installing or Updating to HP-UX 10.10* before referring to other installation or upgrade manuals. It comes with HP-UX Release 10.10 and contains information about last-minute changes to HP-UX Release 10.10 and to the procedures for installing or upgrading your system.
- You can use the Software Distributor—SD-UX commands to install or update software from a software source (that is, a depot or physical media) to your local host. Refer to Chapter 2 of *Managing HP-UX Software with SD-UX* for details on installing or copying HP-UX software.
- If you are currently running 10.x, refer to *Installing HP-UX 10.10 and Updating from HP-UX 10.0x to 10.10* for additional installation or upgrade information.
- If you are currently running 9.x, you must upgrade the system to 10.01 before you can update to 10.10. This involves some pre-upgrade preparation in addition to the upgrade itself. For this you need the package "HP-UX Upgrade Tools for 9.* to 10.*," which you should have received with HP-UX

10.10. The package includes the manual *Upgrading from HP-UX 9.x to 10.x*, which explains the upgrade process.

Conversion Prerequisites

Before you can convert your system into a C2-level trusted system, the following prerequisites must be met:

- You have set SECURE to ON in the ISL when first booting your workstation. The steps are described in the following section.
- Your system must be running HP-UX Release 10.10. Refer to the section "Information about Installing or Upgrading HP-UX" earlier in this chapter for cross references to more information.
- Back up your entire HP-UX file system. Refer to Chapter 9 in *HP-UX System Administration Tasks*. You can use any of the backup and recovery programs provided by HP-UX for your initial backup and recovery. Once security features are implemented, however, you can use only *fbackup*(1M) and *frecover*(1M).
- You must install all required security patches. Refer to "Obtaining Security Patches" in the next section for more information.

Note You cannot convert your system to a trusted system without installing the security patches first. Even if you use SAM to convert your system, it will not be a C2-level trusted system without the patches.

- You must purchase and install anti-tamper devices on all workstations that will be included in the trusted system configuration. This will ensure that no one can open or tamper with your workstation. For servers, you must provide physical security for the system console.

Setting Secure Mode on Workstations

Before allowing users on a workstation, you must set SECURE to ON at the ISL prompt. This is the prompt you can receive when the system is booting. This prevents users from having access to the ISL prompt.

This action is needed to insure the security and integrity of the hardware.

In order to enable secure mode:

1. Interrupt the boot sequence (by pressing Escape) and at the BOOT ADMIN> prompt.
2. Type

```
SECURE ON
```

For additional information on ISL, see the *HP-UX System Administration Tasks* manual, Chapter 2.

Preventing Access to ISL and the System Console on Servers

The physical security of the system console is critical in order to prevent unauthorized access to the ISL prompt. You must prevent someone other than the system administrator from changing the security settings of your system. This is accomplished by restricting access to the system console.

For additional information on ISL, see the *HP-UX System Administration Tasks* manual, Chapter 2.

Obtaining Security Patches

To subscribe to automatically receive future new HP Security Bulletins from the HP SupportLine mail service via electronic mail, send an email message to

`support@us.external .hp.com` *No subject is required*

You can include one or more of the following additional instructions in the text portion of the message.

- To add your name to the subscription list for new security bulletins, send the following in the *text portion* of an email message:

```
subscribe security_info
```

- To retrieve the index of all HP Security Bulletins issued to date, send the following in the *text portion* of an email message:

  ```
  send security_info_list
  ```

- To get a patch matrix of current HP-UX and security patches referenced by either Security Bulletin or Platform/OS, put the following in the text of the email message:

  ```
  send hp-ux_patch_matrix
  ```

- You can view additional information on the World Wide Web at the URL:

  ```
  http://us.external.hp.com
  ```

  Choose "Support news" then "Security Bulletins."

- To report new security vulnerabilities, send email to

  ```
  security -alert@hp.com
  ```

  You need to encrypt exploit information using the security-alert PGP key, available from your local key server, or by sending a message with a -subject- of "get key" (without the quotes) to security-alert@hp.com.

Obtaining Non-Security Patches

Non-security patches to HP-UX 10.10 are also available on SupportLine through the World Wide Web on URL - http://us.external.hp.com

Click on "Patch Browsing and Downloading" to select and obtain the relevant patches.

Verifying and Replicating Your System Configuration

HP-UX maintains several very important records of your system installation and modification. These log files document how you installed and configured your system and are critical in the event you have to reconstruct your original configuration.

These files are located in `/var/adm/sw/`

Immediately after completing your installation, you should save these files. You should copy them to tape or make a hard copy. Keep these records in a safe place in the event you need them in the future.

Setting Up Your C2-Level Trusted System

HP-UX offers the security mechanisms available in the standard UNIX environment. By converting your system to a trusted system, HP-UX provides the following additional security features:

- A more stringent password and authentication system
- Auditing
- Terminal access control
- Time-based access control

The ability to convert your system to a trusted system is a feature of HP-UX. You should seriously consider the ramifications of converting your system to a trusted system before doing so. One ramification is reduced system performance due to the requirements of auditing.

Note Be sure that your system meets the specifications in "Conversion Prerequisites" before attempting to set up your trusted system.

Follow these steps to set up a C2-level trusted system:

1. Establish an overall security policy appropriate to your worksite. See the section "Planning System Security" in Chapter 1.

2. Install anti-tamper devices on all workstations that will be included in the trusted system configuration.
3. Inspect all existing files on your system for security risks and remedy them. This is mandatory the first time you convert to a trusted system. Thereafter, examine your files regularly, or when you suspect a security breach.
4. Change your workstation to character mode by typing:

   ```
   unset display
   ```

5. Convert to a trusted (secure) system:
   a. Type SAM (in character mode):

      ```
      sam
      ```

      The SAM main menu is displayed.
   b. Highlight `Auditing and Security`.
   c. Highlight `Audited Events`. The following message is displayed as soon as you click on any of the auditing options for the first time:

      ```
      You need to convert to a Trusted System before proceeding.
      Converting to a Trusted System does the following:

      1. Creates a protected database on the system for storing
         security information.

      2. Moves user passwords in "/etc/password" to this database.

      3. Replaces all password fields in "/etc/passwd" with "*".

      For more details, refer to the "System Security" chapter
      of the "System Administration Tasks" manual.

      Do you want to convert to a Trusted System now?
      ```

   d. Click Yes.

Note The system displays a warning message about ACLs not being supported on a VxFS system. This is because JFS systems (VxFS) do not support ACLs, an integral part of discretionary access control. JFS is not part of the TCB and you cannot configure JFS systems as trusted systems.

The system displays the following message:

```
Converting to a trusted system....
Successfully converted to a trusted system.

Press OK to continue.
```

The conversion program does the following:

a. Creates a new, protected password database in `/tcb/files/auth/`. The users' login information is organized under `/tcb/files/auth/*` by the first initial of the login name.

b. Moves encrypted passwords from the `/etc/passwd` file to the protected password database and replaces the password files in `/etc/passwd` with an asterisk (*). Be sure to back up the `/etc/passwd` file on tape before the conversion.

c. Forces all users to use passwords.

d. Creates an audit ID number for each user.

e. Sets the audit flag on for all existing users.

f. Converts the `at`, `batch`, and `crontab` files to use the submitter's audit ID.

6. Verify that the audit files are on your system:

   a. Use `swlist - fileset` to list the installed filesets. Look for the fileset called `SecurityMon` which contains the auditing program files.

   b. Verify that the following files not in `SecurityMon` also exist:

      i. `/etc/rc.config.d/auditing` which contains parameters to control auditing; this file may be modified by SAM or manually.
      ii. `/sbin/rc2.d/S760auditing` which is the script that starts auditing and should not be modified.

The Audited Events screen is displayed. It includes a table of events that can be audited, specifications on how the events are to be audited (on success, failure), and lists system calls associated with each event. On the screen you should see the message:

```
Auditing Turned Off
```

If Auditing is Turned On, your system is already converted to a trusted system. Do not proceed with the rest of these steps.

7. Click on any of the events to be audited. (Press Tab to move back and forth from the menus at the top of the screen to the auditing options.)
8. After conversion, you must enable the audit subsystem to run your HP-UX system as a trusted system. To enable auditing, run SAM and use the `Auditing and Security` screen. See "Turning On Auditing" later in this chapter.

Note Once your system is converted to a trusted system, you can only run SAM in character mode. Do not use the graphical user interface because it compromises the security of your trusted system.

---

9. Next, you must also establish password control by setting the many password options available. See "Setting Up Password Controls" later in this chapter.

Your system is now converted to a trusted system.

Completing the Setup

You must instruct system users to read the *Security Features User's Guide Supplement* for additional information they need to know about using a trusted system.

Verifying Setup

There are several log files you can check to verify the configuration of your system. Check the SAM log, installation log, and SD-UX log for this information. It is important that you also maintain information on the system configuration in the System Support Log which is supplied with your system.

You should keep a record of all pertinent information including: root disk selection, file system layout, swap size, and filename length. This information can be recorded in the System Support Log.

swverify(1M) can be used to check the files which have been installed on your system. See the *swverify*(1M) man page for more information.

Auditing Trusted Systems

An HP-UX trusted system provides *auditing,* which is the selective recording of events for analysis and detection of security breaches. You need to set up auditing so it records appropriate events after your system is converted to a trusted system. The audit subsystem collects information about security-related events specified and writes this information to a series of files called an *audit trail.*

Effective auditing concerns events such as system call requests from user processes, logins, logoffs, and failed login attempts. These events are critical to determining who has accessed the system, at what times, from which terminal, and what actions were performed.

You must review the audit trail on a regular basis to monitor system use and detect potential penetrations of the system and misuse of system resources. In accordance with a site's security policy, you should examine patterns of access to objects (such as files) and observe the actions of subjects (for example, specific users and their processes) in an effort to detect any attempts to violate protection and privilege mechanisms.

Administering Auditing

As system administrator, you are responsible for administering auditing and performing the following tasks:

- Setting up the auditing subsystem parameters
- Selecting event types and other selection criteria for generating auditing information
- Performing reduction and analysis of the audit trail
- Maintaining online and offline audit trail data
- Planning file system space consumption for audit data
- Coordinating disk space requirements and user-specific audit parameters

The audit subsystem lets you collect only the audit data you want. You can preselect the type of auditing information you want to collect, based on event type, user ID, and/or group ID.

Setting Up Auditing

You must have superuser privilege to set up auditing. You can administer auditing by using the character version of SAM. Using SAM is recommended because it focuses choices and helps avoid mistakes. You can also perform all auditing tasks manually using the following audit commands:

audsys(1M)	Starts or halts auditing; sets and displays audit file information.
audusr(1M)	Lets you specify users to be audited.
audevent(1M)	Changes or displays event or system call status.
audomon(1M)	Sets the audit file monitoring and size parameters.
audisp(1M)	Displays the audit record.

You can use *audsys*(1M) to start or halt the auditing subsystem and to specify the current and next audit files. *audsys*(1M) uses the *audctl*(2) system call to start auditing and specify the audit files to the kernel. The *audsys*(1M) also creates the audit files, if necessary, defines the parameters for the audit files,

and maintains the names of the auditing files in the `/.secure/etc/audnames` file.

When you start auditing, the `audomon` daemon starts to monitor the audit files. Thereafter, `audomon` is typically spawned by `/sbin/init.d/ auditing` as part of the *init*(1M) startup process when the system is booted.

Refer to the *HP-UX Reference* or system man pages for more information on the auditing commands.

Turning On Auditing

Note Auditing must be turned on for normal system operation on a trusted system. If you need to turn auditing off to perform system administrative functions, bring the system into single user mode, turn auditing off, then perform the desired operations.

Follow these steps to turn on auditing on a C2-level trusted system:

1. Consider what events you want to audit.
2. Run SAM (in character mode):

   ```
   sam
   ```

3. Highlight `Auditing and Security`.
4. Highlight `Audited Events`. The Audited Events screen is displayed. If you see the message:

   ```
   Auditing Turned Off
   ```

   make sure you turn auditing on by following these steps. If it says `Auditing Turned On`, you are done with this procedure.
5. Press Tab to move from the auditing options to the menus at the top of the screen. Use the right arrow to move to the Actions menu.
6. Select `Turn auditing ON`.

Auditing is now turned on. You must now select the events, users, and system calls you want to audit.

Selecting Events to Audit

Continue by selecting what you want to audit:

1. Select the event types you want to audit. You can audit selected events on success, failure, on both success and failure. Tab to the menus, select the Actions menu and choose the appropriate action:

   a. Audit for Success Only
   b. Audit for Failure Only
   c. Audit for Both Success and Failure
   d. Audit for Neither Success nor Failure

2. From the List menu, select `Audited System Calls`. Select the system calls you want to audit. You can audit selected system calls on success, failure, on both success and failure. Tab to the menus, select the Actions menu and choose the appropriate action.

3. From the List menu, select `Audited Users`. The Audited Users screen is displayed with the names of users on the system who can be audited along with system accounts such as `lp`, `bin`, and `root`. The screen also states the number of users currently being selected.

   a. To audit all users: tab to the menus and select `Action` and choose `Audit User(s)`. (To turn auditing off for all users, select `Action` and choose `Don't Audit User(s).`)
   b. To audit specific users:
      i. Tab to the list of usernames.
      ii. Use the arrow keys to select the user you want to audit.
      iii. Tab back to the menus and select `Action` and choose `Zoom`. The user attributes are then displayed.
      iv. Use the arrow keys to highlight `Login Audited  No` and press Return. `No` changes to `Yes`.

4. Select `Exit` when you are done.

Default Auditing Parameters

The system supplies default auditing parameters when auditing is turned on. Some of the defaults are activated automatically, others have to be enabled.

- By default, the audit status for all users is set to `y`. New users added to the system are automatically audited. According to C-2 level requirements, all users must be individually accountable for their actions from login until exit.
- The event types `admin`, `login`, and `moddac` are selected as defaults by the system. Both `Audit Success` and `Audit Failure` are set to `y`. This is the minimum event type selection recommended for running a trusted system. Event types are listed in Table 2-1.
- An audit record is written when the event is selected for auditing and the user initiating the event is selected for auditing. The `login` event is an exception. Once selected, login events are recorded whether or not the person logging in is being audited.
- When an event type is selected, its associated system calls are automatically enabled. Table 2-1 lists the system calls.
- The following audit monitor and log parameters are provided with default values shown. You can change them using SAM (in character mode) or audit commands.
  - Primary log file path name = `/.secure/etc/audfile1`
  - Primary log file file switch size (AFS) = 1,000KB
  - Auxiliary log file path name = `/.secure/etc/audfile2`
  - Auxiliary log file switch size (AFS) = 1,000KB
  - Monitor wake up interval = 1 minute
  - Allowable free space minimum (FSS) = 20% of file system
  - Warning messages sent when log reaches 90%
- Choose a file system with adequate space for your audit log files. (You can assess the size of your file systems using the *bdf* command.) Using the system supplied defaults:
  1. The `./secure/etc` file system must have more than 1000KB available for the primary audit log file.
  2. The file system must have more than 20% of its file space available.
  3. You must provide a new path name for the auxiliary audit log file.

Note We recommend that the primary and auxiliary audit log files reside on separate file systems. You must specify the path name of a new (or empty) file for the audit log file; otherwise, the contents of the file will be deleted.

Table 2-1. Audit Event Types and System Calls

Event Type	Actions Logged	Associated System Calls
`admin`	All administrative and privileged events	*stime*(2), *swapon*(2), *settimeofday*(2), *sethostid*(2), *privgrp*(2), *setevent*(2), *setaudproc*(2), *audswitch*(2), *setaudid*(2), *setdomainname*(2), *reboot*(2), *sam*(1M), *audisp*(1M), *audevent*(1M), *audsys*(1M), *audusr*(1M), *chfn*(1), *chsh*(1), *passwd*(1), *pwdk*(1M), *init*(1M)
`close`	All closing of objects (file close, other object close)	*close*(2)
`create`	All creations of objects (files, directories, other file objects)	*creat*(2), *mknod*(2), *mkdir*(2), *semget*(2), *msgget*(2), *shmget*(2), *shmat*(2), *pipe*(2)
`delete`	All deletions of objects (files, directories, other file objects)	*rmdir*(2), *semctl*(2), *msgctl*(2)
`ipcclose`	All `ipc close` events	*shutdown*(2)
`ipccreat`	All `ipc create` events	*socket*(2), *bind*(2)
`ipcdgram`	Ipc datagram transactions	*udp*(7) user datagram
`ipcopen`	All `ipc open` events	*connect*(2), *accept*(2)
`login`	All logins and logouts	*login*(1), *init*(1M)
`modaccess`	All access modifications other than Discretionary Access Controls	*link*(2), *unlink*(2), *chdir*(2), *setuid*(2), *setgid*(2), *chroot*(2), *setgroups*(2), *setresuid*(2), *setresgid*(2), *rename*(2), *shmctl*(2), *shmdt*(2), *newgrp*(1)

Table 2-1. Audit Event Types and System Calls (continued)

Event Type	Actions Logged	Associated System Calls
`moddac`	All modifications of Discretionary Access Controls	*su(1)*, *chmod*(2), *chown*(2), *umask*(2), *fchown*(2), *fchmod*(2), *setacl*(2), *fsetacl*(2)
`open`	All opening of objects (file open, other objects open)	*open*(2), *execv*(2), *ptrace*(2), *execve*(2), *truncate*(2), *ftruncate*(2), *lpshed*(1M)
`process`	All operations on processes	*exit*(2), *fork*(2), *vfork*(2), *kill*(2)
`removable`	All removable media events (mounting and unmounting)	*mount*(2), *umount*(2), *vfsmount*(2)
`uevent1`, `uevent2`, `uevent3`	User-defined events	See "Streamlining Audit Data" in *HP-UX System Administration Tasks*

Note Table 2-1 includes *uevent3* which is not listed in Table 11-1 in *HP-UX System Administration Tasks*, however, *uevent3* is available.

Selecting Data to Audit

You can concentrate on auditing a specific user, a group of users, or you can preselect only certain event, such as logon and logoff events, for auditing. By being selective, you can save disk space, because the number of audit records written to the collection files is reduced. Especially when performance is a concern, being selective can help reduce the impact of auditing on performance.

Note that you must choose carefully the event types that the system will audit. If, for example, you choose not to include login events in the audit trail, a penetration of the system through a dial-up line might go undetected.

The drawback to preselecting specific events to audit is that it may present an incomplete history of activities on your system. A more conservative approach is to perform full auditing. This ensures that all security- related events that

occur are recorded in the audit trail. Full auditing consumes a large amount of disk space, however.

You can also postselect audited events, examining only those records that are of interest. This lets you examine the audit trail based on event types, user IDs, group IDs, object names, or whatever criteria you find useful.

Some privileged programs are given the capability to self-audit. Self- auditing programs suspend system call auditing of themselves and write their own audit records. This is done to reduce the amount of data in the audit trail and to provide high-level summary information.

Refer to "Streamlining Audit Log Data" in Chapter 12 of *HP-UX System Administration Tasks* for details on ways to reduce the amount of audit log data collected including a description of self-auditing programs.

Auditing Log Files

All auditing data is written to an *audit log file.* When you set up auditing, you define a primary log file and an optional auxiliary log file to collect auditing data.

To set audit monitor and log parameters:

1. Run SAM:

   ```
   sam
   ```

   The SAM main menu is displayed.

2. Highlight `Auditing and Security`.

3. Tab to the menus and select `Action`.

4. Select `Set Audit Monitor and Log Parameters`. The Set Audit Monitor and Log Parameters screen is displayed.

5. Specify the auditing information including:

   a. Primary Audit Log File name and maximum size
   b. Auxiliary Audit Log File name and maximum size
   c. Minimum time interval for checking the log file (in minutes)
   d. Percentage of allowable free space minimum
   e. Percentage of log file to be filled before sending messages

6. Select `OK`.

Processes that perform a security-relevant event generate an *audit record*. Audit records are generated as a result of a user initiating a system call or due to a self-auditing program through a call to *audwrite*(2). Audit records are classified into different audit event types as shown previously in Table 2-1.

As audit records are generated, they are written to the primary audit file. Audit files are located in `/.secure/etc/audfile*`. When auditing is enabled, at least one audit log file must be present. Setting up an auxiliary (backup) log file on another file system is recommended.

The growth of the audit files is closely monitored by the audit overflow monitor daemon, `audomon`, to ensure that no audit data are lost. It prints warning messages when either the audit file or the file system is getting full, and automatically switches to the auxiliary audit file if one is available. If no backup is located, `audomon` requests appropriate action so you can react to the conditions that could cause the system to shut down.

It is critical for security that the system administrator place the system in single user mode before modifying or extending the audit file or auxiliary audit file. This action will ensure that no users can perform actions what would not be audited while maintenance of the audit files is taking place.

Audit Record Formats

Audit records are made up of a fixed-length header and a variable-length body. The header contains the time, process ID, error, event type, and record body length.

The body contains additional information about the audited activity. For records generated by system calls, the body contains the parameters of the system calls. For records generated by self-auditing programs, the body contains a high-level description of the event. See *audwrite*(2). Refer to Appendix A for a detailed description of the record format of audit records.

Reducing and Analyzing the Audit File

Auditing accumulates a lot of data. SAM allows you to select which data to view. You can select the following items:

- Whether the log output is directed to the screen or to a file
- The name of the file to which log output is to be directed
- Whether to view successful or failed events
- Which log file to view
- Which `tty` to view
- Which events or system calls to view

Viewing the Audit File

To view the audit file:

1. Run SAM:

   ```
   sam
   ```

   The SAM main menu is displayed.
2. Highlight `Auditing and Security`.
3. Tab to the menus and select `Action`.
4. Select `View Audit Log File`. The View Audit Log screen is displayed.
5. Select whether to display the log on the screen or put the information into a file. Select `Screen` or `File`.
6. Select which records to view:
   a. Successful and Failed Events
   b. Successful Events
   c. Failed Events
7. Select one or more of the following information filters. You can audit all or select particular items of each type:
   a. Users
   b. Events
   c. System calls

d. TTYs
e. Time Interval

8. Highlight `Select` to select particular items to audit.
9. Select `OK`.

   Once you have specified the items to view, it may take a few minutes to prepare the report for viewing, especially if you are working with a very large audit file. Then the audit file is displayed.

Analyzing the Auditing Data

When viewing auditing data, be aware of the following:

- Auditing data may be inaccurate when programs that call auditable system calls supply incorrect parameters.
- System calls that take file name arguments may not have device and inode information properly recorded.
- Auditing the superuser while using SAM to change event or system call parameters will result in a long auditing record.

Maintaining the Auditing Subsystem

You can use SAM to perform maintenance functions on the auditing subsystem such as:

- Enabling and disabling auditing
- Saving and restoring audit session files
- Displaying session information for backup or reduction
- Retrieve subsystem statistics

Note Auditing must be turned on for normal system operation on a trusted system. If you need to turn auditing off to perform system administrative functions, bring the system into single user mode, turn auditing off, then perform the desired operations.

See "Guidelines for Administering Auditing" in Chapter 3 for information. Refer to *HP-UX Administration Tasks* for additional guidelines for administering your auditing system.

Planning Sufficient Disk Space for Auditing Data

Note Auditing must be turned on for normal system operation on a trusted system. If you need to turn auditing off to perform system administrative functions, bring the system into single user mode, turn auditing off, then perform the desired operations.

Note Auditing must be turned on for normal system operation on a trusted system. If you need to turn auditing off to perform system administrative functions, bring the system into single user mode, turn auditing off, then perform the desired operations.

The amount of disk space required for auditing depends on many factors such as system size, the amount of system activity, the number of events that you are auditing. It is of the utmost importance that you monitor the audit files and archive them daily.

The auditing subsystem warns you when disk space is low. You have the option of disabling auditing or shutting the system down when the free space of file systems is too low. For this reason, you can specify multiple directories for the audit files. If an error occurs when writing audit data to a directory or is disk space is exhausted, the subsystem and the daemon attempt to use the next directory on the list.

Maintaining Audit Across Boot

To ensure that auditing remains in effect when your system is rebooted, you must:

- set boot authentication to root
- ensure that your system reboots in single-user mode

- make sure that auditing is on after a reboot and before you bring the system back into multi-user mode

Recovering From a System Crash

Your audit records will be preserved in the event of a system crash. If your system were to crash, it will, if possible, reboot automatically. When your system reboots it will come up in multi-user mode with auditing enabled. Auditing will continue as before the crash.

If your system cannot automatically reboot, you will have to determine and correct the problem. This may require obtaining help from Hewlett-Packard. After your system has recovered from the crash, ensure that it is returned to trusted mode with auditing enabled.

The maximum number of audit records lost during a system crash is one per process except when the file system is full and the system administrator continues to carry out operations.

Setting Up Password Controls

The password is the most important individual user identification symbol. With it, the system authenticates a user to allow access to the system. Since they are vulnerable to compromise when used, stored, or known, passwords must be kept secret at all times. You and every user on the system must share the responsibility for password security.

This section provides an overview of the tasks required for setting up password controls. For detailed information about users and passwords on UNIX systems, refer to *Practical UNIX Security*.

To maintain a secure system, you must perform the following security tasks:

- Generate authorization numbers for the system and new users.

  To maintain password privacy, SAM generates an authorization number for each new account. This number must be used for first login. Once the number is verified, the new user is prompted for a password. This process shields user passwords even from the system administrator.

- Maintain proper permissions on the `/etc/passwd` password file and the `/tcb/files/auth/`*user_initial*`/`*username* protected password file
- Establish password aging
- Delete and nullify expired passwords, user IDs, and passwords of users no longer eligible to access the system

Before Adding Users . . .

To ensure the maximum security of your users' directories and files, you *must* perform the following before adding users to a trusted system.

Be sure to add the following line to the system files listed below:

```
umask 077
```

System files:

/.profile
/etc/profile
/etc/.profile
/etc/csh.login
/etc/d.profile
/etc/skel/.profile
/etc/skel/.login
/etc/skel/.cshrc
/usr/newconfig/.profile
/usr/newconfig/etc/profile
/usr/newconfig/etc/csh.login

If you already added users to the system such as with an update from a previous version, you will have to change the umask in all existing accounts. Be sure also to change the umask for root.

Note This action provides a default permission of u=rwx g=- - - o=- - - on all user files and directories. While this sets the defaults for the most restrictive permissions, some users may have to use chmod on individual files or directories to open the permissions for certain applications.

Setting Up Password and Account Securities Policies

You can set up password and account security policies using SAM:

1. Run SAM:

   ```
   sam
   ```

   The SAM main menu is displayed.

2. Highlight `System Securities Policies`. A new screen is displayed that lets you choose from the following options:

   - Password format policies
   - Password aging policies
   - General user account policies
   - Terminal securities policies

Refer to the following sections for how to set up the specific aspects of password and account security.

Setting Up Password Format Policies

You can set system policies for user accounts. The policies you set apply to all users unless you set user-specific policies. Refer also to "Selecting and Generating Passwords" later in this chapter.

To set up password format policies using SAM:

1. Highlight `System Securities Policies`.
2. Highlight `Password Format Policies`. The Password Format Policies screen is displayed.
3. Select appropriate options by using the arrow keys to highlight them and pressing Return to toggle the options on or off.
4. Select one or more of the Password Selection Options to cause the system to generate passwords for your users:

   a. `System Generates Pronounceable`
   b. `System Generates Character`
   c. `System Generates Letters only`
   d. `User Specifics`

Note If you select more than one of the above options, users will get to choose which they prefer at login time.

5. If you toggle `User Specifics` on, you can select additional options:
   a. `Use Restriction Rates`
   b. `Allow Null Passwords`

Note For trusted systems, you should not allow null passwords. This severely compromises system security.

6. Select `OK`.

Setting Up Password Aging Policies

HP-UX lets you select password aging options. The amount of time a user has a particular password on his or her account directly related to the amount of time a penetrator has to guess it. The system maintains a time between password changes, an expiration time, and a lifetime for passwords on the system when password aging is enabled. Refer to "Password Aging" later in this chapter for more information.

If there is a system compromise, you can also choose to expire all user passwords immediately and force users to select new passwords.

To set up password aging policies using SAM:

1. Highlight `System Securities Policies`.
2. Highlight `Password Aging Policies`. The Password Aging Policies screen is displayed.
3. Set Password Aging to `Enabled`. The Enable Password Aging screen is displayed.
4. Select appropriate options by using the arrow keys to highlight them and typing appropriate options.
5. Set the `Time Between Password Changes` (in days). This sets the minimum time a user must have a password to prevent users from changing their passwords and then changing it back again to the old one.

6. Specify the `Password Expiration Time` (in days). The expiration time of a password specifies a time after which a user must change the password.
7. Indicate the `Password Warning Time` (in days). This is when to start sending warning messages to the user that they will need to change their password soon.
8. Specify the `Password Lifetime` (in days). The lifetime specifies the time at which the account associated with that password is locked. Once locked, the password must be changed before the person can log in.
9. Select `OK` to accept these values.

Setting Up General User Account Policies

You can set some general policies to help ensure system security on user accounts.

To set up general user account policies using SAM:

1. Highlight `System Securities Policies`.
2. Highlight `General User Account Policies` . The General User Account Policies screen is displayed.
3. Select appropriate options by using the arrow keys to highlight them and pressing (Return) to toggle the options on or off or by typing appropriate values.
4. Set whether or not to require a user to log in when booting the system in single-user mode.

Note It is recommended that you require a password when booting to single-user mode to prevent unauthorized users from rebooting the system and performing activities that should be restricted to the system administrator.

Be sure to remember the password!

---

5. Select `OK`.

Boot Authentication

When setting up a general user account, you must ensure that the user is not authorized to boot in single-user mode. This must be reserved for the system administrator. See "Setting Up General User Account Policies" for instructions. See the *System Administration Task* manual and the following man pages for more information: *default*(4), *getprpwent*(3), and *prpwd*(4).

Note It is critical that boot authentication be set to root and that the system reboots in single-user mode. When the system reboots, you must ensure that auditing is turned on before bringing the system into multi-user mode.

Setting Up Terminal Securities Policies

This screen allows you to specify login restrictions. By setting these restrictions, you can enforce greater system security.

To set terminal securities policies using SAM:

1. Highlight `System Securities Policies`.
2. Highlight `Terminal Securities Policies`. The Terminal Securities Policies screen is displayed.
3. Select appropriate options by using the arrow keys to highlight them and typing appropriate options.
4. Set the number of allowable unsuccessful login tries (in seconds).
5. Specify the delay between login tries (in seconds).
6. Specify the login timeout value (in seconds).
7. Select `OK`.

Maintaining the Password Files

A trusted system has two password database files:

- `/etc/passwd` password file
- `/tcb/files/auth/`*user_initial*`/`*username* protected password file

Each of these files enforces the security policy previously defined in this chapter. Every user has entries in both files and `login` looks at both entries to authenticate login requests. All passwords are encrypted immediately after entry and stored in `/tcb/files/auth/`*user_initial*`/`*username* on a trusted system. The password field in `/etc/passwd` is ignored.

A user with an empty password is forced to set a password upon login on a trusted system. However, this leaves a potential security breach, because any user who knew about the account could set the password for that account before a password is set for the first time.

Note Do not edit the password files directly, Use SAM, `useradd`, or `usermod` to modify password entries.

HP-UX generates these mapping files to provide faster access to the password files:

```
/tcb/files/auth/system/pw_id_map
/tcb/files/auth/system/gr_id_map
/tcb/files/auth/system/aid_id_map
```

It is possible for these mapping files to get out of sync with the password database files, resulting in users unable to log in. In this case, remove the mapping files. The system automatically regenerates new mapping files.

/etc/passwd

The `/etc/passwd` file is used to authenticate users at login time on standard HP-UX systems. This file contains descriptions of every account on the system. Refer to *HP-UX System Administration Tasks* and the *passwd*(1) and *passwd*(4) man pages in the *HP-UX Reference*.

/tcb/files/auth/*/*

When a system is converted to a trusted system, the encrypted password, normally held in the second field of `/etc/passwd`, is moved to the protected password database file, and an asterisk holds its place in the `/ etc/passwd` file.

Protected password database files are stored in `/tcb/files/auth` hierarchy. User authentication profiles are stored in these directories based on the first

letter of the user account name. For example, authentication profile for user `dgarcia` is stored in the file `/tcb/files/auth/d/dgarcia`.

The protected password file is an important part of a C2-level trusted system. Key security elements are stored in the protected password database and are accessible only to superusers. You need to set password entries using character mode SAM. Password data not set for a user uses the system defaults stored in the file `/tcb/files/auth/system/default`.

When you add new user accounts to the system using character mode SAM, user protected password database entries are created as a side effect. SAM ensures that each account has a unique login name. SAM issues a warning message if you try to create an account with an existing UID. SAM ensures that a unique audit ID is assigned for each UID. Refer to *HP-UX System Administration Tasks* for additional information about adding users to your system and controlling system access.

If adding more than one account for a user, you must be sure that each account has a unique UID, for security reasons. Each login must have a unique UID on a trusted system.

Entries in the Protected Password Database

Each entry in the protected password database corresponds to a single user. Each entry contains the following fields:

- User name and UID (User ID)
- Encrypted password
- Account owner
- Boot flag (whether or not the user can boot the system to single user mode)
- Audit ID and auditing flag (whether or not this user is audited)
- Minimum time between password change (or default)
- Maximum password length
- Password expiration interval (after which the password must be changed)
- Password lifetime (after which the account is locked)
- Time of last successful password change
- Time of last unsuccessful password change
- User ID of last person who changed the password, if not the account owner
- Password expiration date
- Maximum time allowed between logins before the account is locked

- Number of days before expiration when warning will appear
- Whether or not the user can use the account without a password
- Whether passwords are user-generated or system-generated
- Whether triviality checks are performed on user-generated passwords
- Type of system-generated passwords
- Times when the user is permitted to log in
- Time stamp of last successful login
- Terminal ID (TTY) of last successful login
- Time stamp of last unsuccessful login
- Number of unsuccessful logins since the last successful login
- Maximum number of unsuccessful login attempts allowed
- Administrative account lock

Refer to *prpwd*(4) for more information on these entries.

Selecting and Generating Passwords

On trusted systems, the following methods control how passwords are generated:

- User-generated passwords

  A password screening option checks user-generated passwords again the dictionary and checks for the use of login names, login name permutations, and repeated characters.

- System-generated passwords (alphabetic)

  You can have the system generate passwords using alphabetic characters only.

- System-generated passwords (alphanumeric)

  You can have the system generate passwords using alphabetic, numeric, and punctuation characters.

- System-generated passwords (English phrases)

  You can have the system generate passwords using alphabetic characters only.

You can set these options for your HP-UX system or for specific users.

Password Aging

You can enable or disable password aging for each user. When password aging is enabled, the system maintains the following for the password:

- **Minimum Time**—specifies the minimum time required between password changes.
- **Expiration time**—specifies a time after which a user must change the password at login.
- **Warning time**—specifies the time before expiration when a warning will be issued to the user.
- **Lifetime**—specifies the time at which the account associated with the password is locked if the password is not changed. Once locked, only the system administrator can unlock it. Once unlocked, the password must still be changed before the user can log into the account.

The expiration time and lifetime values are reset when a password is changed. A lifetime of zero specifies no password aging; in this case, the other password aging times have no effect.

Time-Based Access Control

On trusted systems, you can specify times of day and days of week that are allowed for login for each user. This is another mechanism to ensure that the C2-level security is maintained.

When a user attempts to log in outside of the allowable access time, the event is logged (if auditing is enabled for login failures and successes) and the login time is terminated. Administrators with superuser privilege can log in outside the allowable access time, but the event is logged. The access time is stored in the protected password database. You can change the access times using SAM.

Device-Based Access Control

You (the superuser) can also control access to the system using serial devices. For each mux port and dedicated DTC port on a trusted system, you can specify a list of users allowed access. If the list is empty (null) for a device, all users are allowed access.

Device Assignment Database

The device access information is stored in the device assignment database, `/tcb/files/auth/devassign`, which contains an entry for each device on the trusted system. Each entry in the device assignment database contains the following fields:

- A list of pathnames for each physical device attached to the system
- For each device, a device type (login terminal, remote terminal)
- The external name of the device
- The list of users who can access the device

You can modify the device assignment database using SAM. Functions provided allow you to administer the relationship between physical devices and pathnames, to assign device types, and to designate which users can use the devices. See *devassign*(4) for more information.

Terminal Control Database

You can also control access to terminals to enforce even stricter controls. Terminal login information on a trusted system is stored in the terminal control database, `/tcb/files/ttys`, which provides the following data for each terminal:

- Device name
- User ID of the last user to successfully log into the terminal
- Last successful login time to the terminal
- Last unsuccessful login time to the terminal
- Number of consecutive unsuccessful logins before terminal is locked
- Terminal lock flag

One special login terminal is called the *system console*. When the kernel is configured during system installation, you need to specify the hardware device to which the system console is attached.

You can access the terminal control database using SAM and set or modify all entries. See *ttys*(4) for more information.

Manipulating the Trusted System Databases

Table 2-2 lists the library routines you can use to access information in the password files and other trusted system databases. Refer to the *HP- UX Reference* for details.

Table 2-2.
Library Routines for Manipulating Trusted System Databases

Routine	Description
`getpwent`	Get password entries from `/etc/passwd`
`getprpwent`	Get password entries from `/tcb/files/auth/*/*`
`getspwent`	Get password entries from `/tcb/files/auth/*/*`, provided for backward compatibility
`putpwent`	Write password file entries to `/etc/passwd`
`putprpwnam`	Write password entries to `/tcb/files/auth/*/*`
`putspwent`	Write password file entries to old secure password file format provided for non-HP software compatibility. Will not work with protected password database.
`getdvagent`	Manipulates device entries in `/tcb/files/auth/devassign`
`getprdfent`	Manipulates system defaults in `/tcb/files/auth/system/default`
`getprtcent`	Manipulates terminal control database `/tcb/files/ttys`

Account and Terminal Lock Flags

You can set or reset account or terminal lock flags using SAM. Refer to the *sam*(1M) man page or use SAM to set the flags.

Changing the Owner of a File

If you have superuser privilege, you can use the *chown*(8) to change the owner of a file. This can be a security problem because a user can cover his tracks or change owners of a file to acquire additional disk space on the system. Refer to the *chown* man page for additional information.

3

Practices that Enforce the Trustworthiness of the System

The way an HP-UX trusted system is run determines how secure it will be.

This chapter describes some of the practices that help to enforce and maintain C-level HP-UX system security.

Background on Security Practices

To run a secure system, you need to set up and run your system according to standard practices and be aware of potential threats. To do this you need a strong background in UNIX security basics. For background and details about the basics of UNIX security, refer to *Practical UNIX Security, Second Edition* by S. Garfinkel and G. Spafford. Some of the topics it presents are:

- Types of UNIX security
- Users, passwords, logging onto a UNIX system
- UNIX file system and setting file permissions
- Defending system accounts against unauthorized access
- Securing data against loss due to theft, system failure, user error, or other disaster
- Descriptions of UNIX log files and ways to use them
- Protecting against programmed threats
- Background on networks and security
- Handling security incidents such as break-ins or attacks

This book is available from your local computer bookstore or by ordering ISBN 0-937175-72-2 from O'Reilly & Associates, Inc. at 1-800-889-8969 or via email at ORDER@ORA.COM.

Additional detailed information that describes good security practices is provided in "Guidelines for Running a Trusted System" in Chapter 12 of *HP-UX System Administration Tasks*. It provides the following information:

- Guidelines for Handling setuid and setgid Programs
- Guidelines for System Initialization
- Guidelines for Trusted Backup and Recovery
- Guidelines for Mounting and Unmounting a File system
- Guidelines for Handling Security Breaches

Safe Administrative Practices

System administrators of trusted HP-UX systems are responsible for performing standard HP-UX administrative tasks. The standard HP-UX tasks are described in detail in *HP-UX System Administration Tasks* (B2355-90079). Chapter 12 of that manual, "Managing System Security" describes many of the tasks that need to be performed on a trusted system.

System administrators on trusted systems are responsible for performing the following security functions:

- Setting up the trusted system
- Setting up security databases
- Maintaining additional security parameters of users' authentication profiles
- Monitoring the security and integrity of the system
- Auditing security-related events and maintain the system's audit functions
- Perform miscellaneous administrative tasks associated with HP-UX

C-level protected subsystems

In addition, on a trusted system, the system administrator is responsible for maintaining the Trusted Computing Base. For details about maintaining Unix systems and protecting against system threats, refer to *Practical UNIX Security* by S. Garfinkel and G. Spafford.

Common Security Practices

Part of running a secure system involves educating your system users and enforcing standard security practices such as the following:

- Restrict login access to software to those with legitimate need.
- Have users log off or use the `lock` command when not using their terminals.
- Decentralize computer duties by rotating computer operators.
- Store backup media at bonded, offsite depositories.
- Erase obsolete data and securely disposing of console logs and printout.

User Passwords

One of the main ways you can keep your trusted system secure is to teach users good password security. When you set up accounts for new users, you should discuss guidelines such as the following with them:

- Users must remember their passwords and keep them secret at all times
- Users must be sure no one is watching when entering the password
- Users should change their initial password immediately and change their passwords periodically
- Users should report any changes in status and any suspected security violations
- Users with accounts on more than one system should choose a different password for each machine

You should also set your system up so that users must use secure passwords.

For example, passwords should have the following characteristics:

- Six or more characters including asterisks and slashes
- Contain both alphabetic and numeric characters
- Contain both upper- and lowercase characters
- Be easy to remember
- Do not use a password that is easily associated with you, such as a pet name or a hobby
- Do not use a password found in a dictionary, even if it is spelled backwards. Software programs exist that can find and match it.

Account Security

- Use the password aging feature to deactivate an account that is not being used, to set an expiration time for a password, and specify the lifetime of a password.
- Rather than removing or reassigning old accounts, you should use the administrative lock feature of SAM. Accounts should not be removed because it would then be possible for a given user ID to be reused later by another account. You must only have one user ID per user.
- Do not permit any empty password fields.
- Maintain proper permissions on the `/etc/passwd` password file or the `/tcb/files/auth/`*user_initial*`/`*username* protected password file.
- Maintain proper permissions on the `/etc/passwd` password file and the `/tcb/files/auth/`*user_initial*`/`*username* protected password file.
- A user with an empty password is forced to set a password upon login on a trusted system. However, this leaves a potential security breach, because any user can set the password for that account before a password is set for the first time.

  You should discuss the new account with the user confidentially. Then, take the time to follow up and be assured that the correct person validates the account by logging on and changing the password right away.

- Refer to the section "Eliminating Pseudo-Accounts and Protecting Key Subsystems" in Chapter 12 of *HP-UX System Administration Tasks* for information relevant to keeping accounts listed in /etc/passwd secure.

Managing File and Directory Access

Along with traditional HP-UX file access protection, files and directories can be protected from unauthorized access by using Access Control Lists (ACLs). An ACL is a set of entries that allows users to specify different access rights to many individuals and groups instead of one of each. ACL entries define which users, groups and/or hosts have permission to access software objects (such as files and directories).

By understanding the full use of ACLs, you can help system users to protect information to a great degree. Refer to "Managing Access to Files and Directories" in Chapter 12 of *HP-UX System Administration Tasks* for information on ACLs including a subsection on "Security Considerations for Device Files."

Guidelines for Administering Auditing

The following guidelines describe good practices when administering auditing on a trusted system in order to avoid audit data loss:

- Check the audit logs at least once per day. Keep the online auditing file for at least 24 hours. Keep all auditing records stored offline for at least 30 days.
- Review the audit log for unusual activities such as late night logins, login failures, failed access to files, or failed attempts to perform security-relevant tasks such as changing file permissions or ACLs.
- Archive the audit file everyday to prevent it from overflowing (and potential loss of auditing data).
- Revise the events that are audited periodically.
- Change the audited users periodically.
- Do not follow any pattern or schedule for event or user selection.

- Specify site guidelines. Involve users and management in determining these guidelines.
- Ensure the physical security of systems and disks containing the audit logs, backups of these logs, and printouts of these logs.
- Provide a backup power source (UPS) for the disks containing the audit log so the data are not lost in the event of power failure.
- Provide disk mirroring and other high availability support for the audit log disks.

Recovering From Full Audit Files

When the audit files (primary and secondary) are full:

1. bring the system into single-user mode
2. backup all audit logs
3. free audit file space by:
   a. increasing the size of the audit logs and audit log filesystem
   b. renaming the audit logs and copy them to another filesystem
   c. copying the audit logs to tape and archive
4. ensure that auditing is on
5. bring the system back to multi-user mode

Privileged Groups

A "privilege" is the ability to ignore access restrictions and change restrictions imposed by security policy and implemented in an access control mechanism. On HP-UX, only system administrators and members of certain groups are the only privileged users.

The system administrator can associate a group with a system capability so that members of certain groups can be granted special privileges. The groups are called *privileged groups*.

All users by default are members of the *CHOWN* privilege group. People with this privilege can change the ownership of files they don't own. The system administrator may limit access to the *chown*(1) command by setting up privileged groups using *setprivgrp*(1M). In that case, only those in the privileged group or groups can change file ownership using *chown*(1). Refer to the *chown*(1) man page for more information.

Users can also execute the *getprivgrp*(1) command to determine the special attributes for groups to which they belong. If the groupname is omitted, the command lists the access privileges.

Note *PRIV_SETRUGID* is a special privilege group which has been provided for backwards compatibility. It may present a security problem and should not be used.

Root Use Guidelines

Commands and system calls used only by the system administrator are reserved for the superuser. To protect the system, observe the following:

- Restrict knowledge of the root password to the barest minimum number of people—one if possible. The root password should be held in strictest secrecy and changed periodically.
- All root accounts should have PATH set (in .profile or .login) to some default that does not contain the current directory ("dot"). The following PATH is recommended: /bin:/usr/bin:/etc

- Most system administration tasks should be performed by invoking SAM, because its menus restrict choices and thus reduces potential damage.
- If the root user forgets the root password, reboot the system in single-user state, and reassign the password.
- Superusers should construct *at* and *cron* jobs carefully. When *at* and *cron* are executed, the system searches the path set by root.
- Set your file creation mask with a *umask* of 077 before creating a file. This restricts read and write permissions to the file owner by default.
- Do not leave executables where they were developed. Restrict access to executables under development.

4

Practices that Compromise the Trustworthiness of the System

This chapter describes some of the practices that compromise the trustworthiness of your HP-UX trusted system. Basically, not following the good security practices and guidelines described in Chapter 3 of this manual and in Chapter 12 of *HP-UX System Administration Tasks* amounts to putting your system at risk.

Lack of Password Security

A user must log onto the system by specifying a user name and a password. If system administrators and users are not careful about creating accounts with secure passwords, if they do not keep passwords private, unauthorized users can easily gain access to the system and explore security holes. Maintaining password security is one essential method of keeping your system and data safe.

Incomplete User Education

As the system administrator, it is your responsibility to educate your system users about keeping their accounts and passwords secure. You are the main source of information on system security to users and their managers. By not providing information and not keeping an eye on system use, you risk unauthorized user access. This is one of the most difficult types of system intrusion to detect because proper authentication procedures are followed.

In addition, making a secure environment seem confining to users is asking for trouble. Making security guidelines sound like dictums that must be followed may seem restrictive and unappealing. Users might want to strike out against the rules and could senselessly damage the system. Therefore, it is to your advantage to be diplomatic when employing the rules. Involve users in

developing security policy and make them aware of the advantages for them and possible bad consequences they could face.

Unsafe Password Practices

- Not implementing restrictions on the passwords chosen
- Creating accounts without passwords
- Not requiring password aging
- Allowing usernames of less than three characters
- Writing passwords down
- Allowing users to share accounts
- Letting users have multiple accounts and passwords with the same username and password

Password aging lets you set a limit to the time you can use a specific password before it has to be changed.

Even if a password is compromised, that password will be changed. Without password aging and expiration policies, user passwords and accounts may not remain current and you're increasing system risk.

Creating accounts with no passwords or using simplistic passwords such as "123" for general access can leave a way for someone to gain system access. By allowing usernames of less than three characters can cause confusion due to potential duplication. Not implementing restrictions on the passwords chosen can make it easier for users to assign passwords that can be easily guessed. For example, by allowing users to assign alphabetic passwords, they might use a word that is in the dictionary or a name of a family member.

Another bad practice occurs when users find the need to write their passwords down or send information about passwords in email. In addition, allowing users to share accounts compromises system accountability.

Lack of Routine System Checks

Part of implementing system security is being good at interpreting events and recognizing questionable activities. A system administrator that doesn't perform routine system checks is putting the system at risk.

Auditing Not Used Effectively

You have the ability to enable auditing to record events of various types on the system. However, recording the events but not analyzing the audit trail thoroughly and checking the logs infrequently does little to keep your system secure. You need to learn what to look for and track various events, different users, and at different times to be able to detect security problems. By not varying the pattern of event logging, your actions can become predicatable making it easier to schedule break-in attempts.

Auditing logs must be archived everyday. By not being attentive to the logs, their sizes, maintaining backups for some period of time, you risk losing the comprehensive tracking of system events and potential threats.

Unlimited File and Directory Access

Although difficult, you need to set up file and directory access so that it perfectly meets the needs of your organization or department. By default, access to files on a system can be very relaxed. By not controlling file access, you may leave files and directories unrestricted and open to many users. Use of groups, file permission bits, and Access Control Lists (ACLs) are all methods that let you control file and directory access.

Unsafe Storage of System Backups

It doesn't matter how secure your system is if the backup tapes are stored where they can be accessed. A full system can be replicated from the backup tapes. Typically, full system backups are stored off site in a secure facility on a regular basis.

Lack of Physical Security

One of the most important, yet overlooked, aspects of computer system security is keeping the physical computer and related documentation in a safe area. This section summarizes the major risks. For background and details about physical security risks and remedies, refer to *Practical UNIX Security* by S. Garfinkel and G. Spafford, Second Edition.

Improper Access to System Hardware

Unauthorized personnel can potentially damage a system that they can physically access even if they do not have an account on the system. For example, a system could be turned off without following proper shutdown procedures, damaged by physical attack, and data could be compromised. Not protecting the physical computer system by placing it in a secure computer room with limited access leaves your system open to potential attack.

Lack of anti-tamper devices on workstations, servers, and consoles in a trusted system configuration allows for potential system access both internally and also to external buses. Be sure to provide physical security for these components.

Improper Access to System Documentation

If unauthorized personnel can review system documentation, especially that which is written for system administrators, they can determine ways to compromise the system. For example, a system could be brought down and reinstalled if an unauthorized person could use the installation documentation for HP-UX systems.

Environmental Risks

Not following specified site preparation guidelines when setting up your system enironment can leave it open to physical problems. For example, most computer systems work best in within certain temperature ranges where they are not exposed to water, smoke, fire, dust, insects, open windows, food, or drink.

A

Audit Record Format

This appendix describes the format and structure of Hewlett-Packard's audit trail as shipped with HP-UX 10.10. Note that access to the auditing system is restricted to the system administrator.

The commands to start auditing are located in the file `/sbin/init.d/auditing`. The default values for the event types that are going to be audited, the sizes of the files, and file names are stored in `/etc/rc.config.d/auditing`. Refer to these files for additional information about how your auditing system is set up.

Audit Records

Audit records are generated in the following cases:

- When users make security-relevant system calls
- As a result of self-auditing processes

The audit record format varies for each case (for details, see "System Call Audit Record Format" and "Self-Auditing Audit Record Format" later in this appendix).

The records in the audit file are compressed to save space. When a process is audited for the first time, a PID identification record (PIR) is written into the audit file containing information that remains constant throughout the life of the process including:

- Parent's process ID
- Audit ID
- Real user ID

- Real group ID
- Effective user ID
- Effective group ID

System Call Audit Record Format

System call records have a format that is understood by the kernel and are generated as a result of invoking system services. System call records are generated within the kernel.

Each audit record consists of an *audit record header* and a *record body*. The record body is the variable-length part of an audit record containing more information about the audited activity.

The record header for audit records (except self-auditing records) contains the following:

Time	the date and time the audited event completed.
Process ID	the process ID (PID) of the process being audited.
Error	whether the event ended in success or failure.
Event type	the type of audited activity.
Record body length	the length of the record body in bytes.

The variable length portion of the audited system calls has the following format:

```
RETURN VALUE              = <system call return value>

PARAM #<[1..n]> (<type>) = <value
of the parameter>
```

where:

n	is the number of system call parameters for the system call being audited. Each parameter for a particular system call will have *n* `"PARM #x"` entries.
type	is the type of the system call parameter variable (for example, int, long).

The man pages for each of the system calls provide information about the type, count, and definitions of each of the parameters for the system calls.

The record body contains the parameters of the system calls that generated the audit record.

Self-Auditing Audit Record Format

Self-auditing processes are those which call *audwrite*(2).

Self-auditing records contain the following:

Date	the date the event occurred.
Time	the time the audited event completed.
Process ID	the PID of the process that caused the audited event.
Success or Failure	whether the event completed as a success or failure.
Event Name	the name of the audited event.
Parent Process ID	the PID of the parent process of the process that caused the audited event.
Audit ID	the audit ID of the process that caused the event.
Effective UID	the UID of the process that caused the audited event.
Effective GID	the GID of the process that caused the audited event
Tty	the tty where the process was initiated.
Text	the information that appears in the audit record.

Records generated by self-auditing processes include a high-level description of the event. The following commands are self-auditing:

- *chfn*(1)
- *chsh*(1)
- *chsh*(1)
- *login*(1)
- *newgrp*(1)
- *passwd*(1)

- *audevent*(1m)
- *audisp*(1m)
- *audsys*(1m)
- *audusr*(1m)
- *fbackup*(1m)

Text in the record structure includes information on the outcome of the command. For more information, see the *audwrite*(2) man page and the following section.

Self-Auditing Commands

The following sections describe the formats of the self-auditing commands. Review the Text field to see the possible information that will be put into the audit trail as a result of executing the command.

chfn(1)

Header	
Event	EN_CHFN
User ID	
Real Group ID	
Effective Group ID	
Text	"User=",username,message
	"No account for user."
	"Permission denied."
	"Current user." "No passwd file entry."
	saved_name, "Temporary file busy."
	saved_name, "Error in chown."
	saved_name, "Error in rename."
	saved_name, "Successful chfn."

chsh(1)

Header	
Event	EN_CHSH
User ID	
Real Group ID	
Effective Group ID	
Text	"User=",username,"shell=", message
	"Permission denied"
	"Temporary file busy"
	"Can't create temporary file"
	"Can't recover"
	"Successfully changed"
	"Chsh failed"

login(1)

Header	
Event	EN_LOGINS
User ID	
Real Group ID	
Effective Group ID	
Text	"User=",username, "uid=", userid, "audid=", auditID, msg
	"attempted to login - too many users on the system"
	"attempted to login - not on system console"
	"attempted to login - must exec login from the lowest level"
	"attempted to login - bad group id"

	“attempted to login - bad audit flag”
	“attempted to login - bad audit id”
	“Successful login”
	“attempted to login - no shell”
	“Failed login (bailout)”
	“attempted to login - bad user id”
	“attempted to login - cannot execute /usr/bin/passwd”
	“attempted to login - failed login_validate”

newgrp(1)

Header	
Event	EN_NEWGRP
User ID	
Real Group ID	
Effective Group ID	
Text	“newgrp=”,group_name,message
	“Sorry.”
	“You have no shell.”
	“Failed newgrp.”
	“Successful newgrp.”

passwd(1)

Header	
Event	EN_PASSWD
User ID	
Real Group ID	
Effective Group ID	

Text	"User=",username,message
	"Password successfully changed."
	"Attempt to change password failed."

audevent(1M)

Header	
Event	EN_AUDEVENT
User ID	
Real Group ID	
Effective Group ID	
Text	"audevent: getting event and syscall status"
	"audevent: disable success for event", event_name
	"audevent: enable success for event", event_name
	"audevent: disable failure for event", event_name
	"audevent: enable failure for event", event_name
	"audevent: disable success for syscall", syscall_name
	"audevent: enable success for syscall", syscall_name
	"audevent: disable failure for syscall", syscall_name
	"audevent: enable failure for syscall", syscall_name

audisp(1M)

Header	
Event	EN_AUDISP
User ID	
Real Group ID	
Effective Group ID	
Text	argument_list

Header	
Event	EN_AUDSYS
User ID	
Real Group ID	
Effective Group ID	
Text	
	"audsys <noargs>"
	"audsys -n"
	"audsys -f"
	"audsys -c", current_audit_file, "-s", current_audit_file_switch_size
	"audsys -x", next_audit_file, "-z", next_audit_file_switch_size
	"audsys -s", current_audit_file_switch_size
	"audsys -z", next_audit_file_switch_size
	"audsys: unable to open/lock /.secure"
	"audsys: unable to open/lock /.secure/etc/audnames"
	"audsys: unknown internal error"
	"audsys: could not find /.secure/etc/audnames"
	"audsys: detected bad /.secure/etc/audnames"
	"audsys: auditing system shut-down"
	"audsys: internal error: shut-down failed"
	"audsys: current audit file is changed to ", current_audit_file
	"audsys: unknown current audit file in use ", system_current_audit_file,

	"audsys: auditing system unchanged."
	"audsys: auditing system unchanged."
	"audsys: unknown current audit file in use ", system_current_audit_file,
	"audsys: unknown next audit file in use ", system_next_audit_file,
	"audsys: auditing system unchanged"
	"audsys: current and next file set to same file (no-next)"
	"audsys: next audit file is changed to", next_audit_file
	"audsys: reset next file to NULL"
	"audsys: corrected /.secure/etc/audnames"
	"audsys: internal error: could not update kernel"
	"audsys: auditing system started"
	"audsys: internal error: /.secure/etc/audnames update failed"
	"audsys: current file is ", current_audit_file, "audsys: next file is", next_audit_file

audusr(1M)

Header	
Event	EN_AUDUSR
User ID	
Real Group ID	
Effective Group ID	
Text	"All users will be audited"
	"All users will not be audited"
	argument_list_of_users, "will be audited"

	argument_list_of_users, “will not be audited”

fbackup(1M)

Header	
Event	EN_SAMFBACKUP or EN_SAMIBACKUP
User ID	
Real Group ID	
Effective Group ID	
Text	“Perform a Full Backup Online”
	“Perform an Incremental Backup Online”

B

Commands and System Calls

This appendix lists commands and system calls that are part of a C2-level HP-UX trusted system.

For more information, refer to the online man pages.

Table B-1. Commands and System Calls

Function	Function Type
accept	System call
access	System call
ar	Command
async_daemon	System call
at	Command
batch	Command
atexit	System call
audctl	System call
audevent	Command
audisp	Command
audswitch	System call
audsys	Command
authck	Command
batch	Command

Table B-1. Commands and System Calls (continued)

Function	Function Type
bdf	Command
bind	System call
boot	Command
brk	System call
bsdproc	System call
bsdproc	System call
cat	Command
cd	Command
cds	System call
chacl	Command
chatr	Command
chdir, fchdir	System call
chfn	Command
chgrp	Command
chmod	Command
chown, chgrp	Command
chown, fchown	System call
chroot	System call
chsh	Command
close	System call
cklri	Command
cluster	System call
cmp	Command

Table B-1. Commands and System Calls (continued)

Function	Function Type
comm	Command
connect	System call
convertfs	Command
cp	Command
cpio	Command
cpio	Command
creat	System call
cron	Command
crontab	Command
crypt	Command
cs	System call
csh	Command
csplit	Command
df	Command
df (generic)	Command
diff	Command
diff3	Command
diffmk	Command
disable	Command
dos cp	Command
dump	Command
dup	System call
dup2	System call

Table B-1. Commands and System Calls (continued)

Function	Function Type
egrep	Command
enable, disable	Command
env	Command
errno	System call
exec	Command
exit	Command
exit(2)	System call
exit, _exit	System call
fbackup	Command
fchdir	System call
fchdir	System call
fchmod	System call
fchown	System call
fclose_unlocked	System call
fcntl	System call
fgetacl	System call
fgrep	Command
find	Command
fork(2)	System call
fpathconf	System call
frecover	Command
fsck (generic)	Command
fsctl	System call

Table B-1. Commands and System Calls (continued)

Function	Function Type
fsdb	Command
fsetacl	System call
fss	System call
fstat	System call
fstatfs	System call
fstyp	Command
fsync	System call
ftruncate	System call
fuser	Command
get_sysinfo	System call
getaccess	Command
getacl	System call
getcontext	System call
geteuid	System call
getgid	System call
getgroups	System call
getmount_cnt	System call
getmount_entry	System call
getpeername	System call
getprivgrp	System call
getprivgrp(2)	System call
getrusage	System call
getsockname	System call

Table B-1. Commands and System Calls (continued)

Function	Function Type
getsockopt	System call
gettimeofday	System call
getty	Command
getuid	System call
grep	Command
groups	Command
grpck	Command
head	Command
id	Command
init	Command
init(2)	System call
insf	Command
ioctl	System call
ioinit	Command
ipcrm	Command
ipcs	Command
isl	Command
kill	Command
killall	Command
killpg	System call
ksh	Command
l	Command
link	System call

Table B-1. Commands and System Calls (continued)

Function	Function Type
listen	System call
ll	Command
ln	Command
lockf	System call
logger	Command
login	Command
logname	Command
lpadmin	Command
lpfence	Command
lpmove	Command
lpmove	Command
lpsched	Command
lpshut	Command
ls	Command
lsacl	Command
lseek	System call
lsf	Command
lsr	Command
lstat	System call
lsx	Command
madvise(2)	System call
mediainit	Command
merge	Command

Table B-1. Commands and System Calls (continued)

Function	Function Type
mesg	Command
mkdir	Command
mkfifo	Command
mkfs	Command
mkfs (generic)	Command
mknod	System call
mktemp	Command
mktmp	Command
mmap(2)	System call
more, page	Command
mount	System call
mprotect	System call
msem_init(2)	System call
msem_lock(2)	System call
msem_remove(2)	System call
msem_unlock(2)	System call
msgctl	System call
msgget	System call
msync	System call
msync(2)	System call
munmap(2)	System call
mv	Command
mvdir	Command

Table B-1. Commands and System Calls (continued)

Function	Function Type
mysite	System call
ncheck	Command
newfs (generic)	Command
newgrp	Command
nice	Command
nohup	Command
nroff	Command
nsp_init	System call
open	System call
passwd	Command
paste	Command
pathconf	System call
pax	Command
pg	Command
pipe	System call
plock(2)	System call
popen, pclose	System call
pr	Command
ps	Command
pstat(2)	System call
ptrace(2)	Command
pwck, grpck	Command

Table B-1. Commands and System Calls (continued)

Function	Function Type
pwd	Command
quotactl	System call
rdump	Command
read	System call
readlink	System call
readv	System call
reboot(2)	System call
recv	System call
recvfrom	System call
recvmsg	System call
reject	Command
rename	System call
renice	Command
restore	Command
rksh	Command
rm	Command
rmdir	Command
rrestore	Command
rsh	Command
sam	Command
sar	Command
sbrk(2)	System call
sdiff	Command

Table B-1. Commands and System Calls (continued)

Function	Function Type
select	System call
sem_remove	System call
semctl	System call
semget	System call
semop	System call
send	System call
sendmsg	System call
sendto	System call
setacl, fsetacl	System call
setaudid	System call
setaudproc	System call
setcontext	System call
setcore	System call
setdomainname	System call
setevent	System call
setgid	System call
setgroups	System call
setmnt	Command
setpriority	System call
setprivgrp	System call
setprtcent	Command
setresgid	System call
setresuid	System call

Table B-1. Commands and System Calls (continued)

Function	Function Type
setsockopt	System call
settimeofday	System call
setuid, setgid	System call
setuname	System call
sh	Command
shmat	System call
shmctl	System call
shmdt	System call
shmget	System call
shmop	System call
shposix	Command
shutdown	System call
shutdown(1M)	Command
signal	System call
sigsetreturn	System call
sigsetstatemask	System call
sigsuspend	System call
sigvec	System call
sitels	System call
size	Command
socket	System call
socketpair	System call

Table B-1. Commands and System Calls (continued)

Function	Function Type
sort	Command
split	Command
stat	System call
stime	System call
su	Command
swacl	Command
swagent	Command
swagentd	Command
swap_clients	System call
swapfs	System call
swapon	Command
swapon	System call
swconfig	Command
swinstall	Command
swlist	Command
swreg	Command
swremove	Command
swverify	Command
symlink	System call
tail	Command
tar	Command
tee	Command
test	Command

Table B-1. Commands and System Calls (continued)

Function	Function Type
touch	Command
truncate	System call
tsync	System call
tty	Command
tunefs	Command
ulimit	Command
umask	Command
umount	System call
umount	System call
uname	Command
unlink	System call
unsp_open	System call
utime	Command
utssys	System call
valloc	System call
vfsmount	System call
vipw	Command
vmstat	Command
wait	System call
wait3	System call
waitpid	System call
wall	Command
write	System call

Table B-1. Commands and System Calls (continued)

Function	Function Type
writev	System call
xargs	Command

C

SFUG Supplement

Security Features User's Guide Supplement

August 1996

5965-4311

Welcome to the world of HP-UX, a powerful, versatile system that meets the computing needs of diverse groups of users. You can use HP-UX simply to run applications, or you can develop your own applications in its rich software development environment.

Trusted System

==========

Your HP-UX system can be configured as a C2-level trusted system, as described in Section 2.2 of the Department of Defense Trusted Computer System Evaluation Criteria, DOD 5200.28-STD, December 1985.

To be evaluated as a trusted system, a system must supply information in a document that the government refers to as the Security Features User's Guide. The following documents provide the information required for the Security Features User's Guide.

For Series 700 systems: Using Your HP-UX Workstation

For Series 800 systems: Using HP-UX

This document is a supplement to the above manuals. It provides additional security information that you will need if your system is set up as a trusted system.

The system administrator is responsible for the security of your system and how it is configured. Your system administrator can inform you if your system is a trusted system. When appropriately configured as a trusted system,

HP-UX provides additional security features such as discretionary access control and system auditing.

Security Policy

A "security policy" is a statement of the rules and practices that regulate how an organization manages, protects, and distributes sensitive information. HP-UX C2-level security expands on existing HP-UX security mechanisms and provides procedures and guidelines to help enforce your company's security policy.

The Hewlett-Packard C2-level trusted system is made up of the HP-UX operating system configured in trusted mode and its commands, utilities, and subsystems along with supported hardware. The system's application interface must work correctly and satisfy the computing needs of its system users. The system's security features provide the mechanisms necessary to enforce your site's security policy and protect system users and their data from threats.

Logging In

To begin using your HP-UX system, you must log in. When you log in, HP-UX prompts you for your username and password. Note that when working on a trusted system, you should be aware of several restrictions that relate to the login process.

Typically, you have three tries to log in successfully. If you still fail to log in, you may not be able to log in again at that time. It is possible that your system administrator may have configured your workstation so it locks you out for some period of time after some number of failed login attempts.

Changing Your Password and Password Aging

For security reasons, you should frequently change your password. Often you are periodically forced to change your password. This security feature is know as password aging.

When you log in to the system, you may see a message informing you that your password is about to expire. In this case, you must change your password by using the passwd command as follows:

$passwd

The system prompts you for your old password. When you type it successfully, you are prompted for a new password which you must type then retype to validate it.

Terminal Restrictions

==========

Your system administrator may set an authorization list for a terminal limiting who can log on to specific terminals. You will only be able to log on to terminals to which you have access in this case. The system administrator can also set time-of-day restrictions on accounts, and you cannot log in if you try to log on at a time you are not authorized to do so. Your system administrator should inform you of any restrictions on your account.

Password Protection

==========

Your system administrator controls how passwords are generated. The following password generation options are available:

* User-generated passwords: You select your own password but passwords are run through a screening program that checks the password against the dictionary, a list of login names, login name permutations, repeated characters, and palindromes.

* System-generated passwords using letters only: The system assigns passwords using alphabetical characters only.

* System-generated passwords using a combination of letters, numbers, and punctuation characters: The system assigns passwords using alphanumerics and punctuation characters.

* System-generated passwords using pronounceable English phrases: The system assigns passwords that you can pronounce.

Your system administrator can inform you which option(s) are implemented on your system.

For user-generated passwords, when you choose a password, you need to follow certain guidelines for selection. For example, when you change your password, pick a new password and do not reuse an old one.

* You must remember your password and keep it secret at all times

* You must be sure no one is watching when you enter the password

* You should change your initial password immediately and change your password periodically

* You should report any changes in status and any suspected security violations to your system administrator

* If you have an account on more than one system, you should choose a different password for each one

Passwords should have the following characteristics:

* Six or more characters including asterisks and slashes

* Contain both alphabetic and numeric characters

* Contain both upper- and lowercase characters

* Be easy to remember

* Do not use a password that is easily associated with you, such as a pet name or a hobby

* Do not use a password found in a dictionary, even if it is spelled backwards. Software programs exist that can find and match it.

* While you can enter a password length as long as 80 characters, it is recommended that you limit your password length to something more reasonable.

Group Access on Your System

==========

In addition to your login account, you may be organized into a working group on your system. This allows all members of a group to share a set of files and directories yet protects the files from access by others who are not in your group. Typically, the system administrator organizes users into groups on the

system, if required, by using sam(1m) and system calls such as setuid(2) and setgid(2).

You can be a member of more than one group, and you can change your current group with the newgrp(1) command. Errors may occur if you attempt to change to a group that doesn't exist or to a group to which you do not have access. See the newgrp(1), setuid(2), and setgid(2) online man pages for more information.

Privileged Groups

A "privilege" is the ability to ignore access restrictions and change restrictions imposed by security policy and implemented in an access control mechanism. On HP-UX, only superusers and members of certain groups are the only privileged users.

The system administrator can associate a group with a system capability so that members of certain groups can be granted special privileges. These groups are called "privileged groups."

All users by default are members of the CHOWN privilege group. People with this privilege can change the ownership of files you own. Your system administrator may limit access to the chown(1) command by setting up privileged groups using setprivgrp(1M). In that case, only those in the privileged group or groups can change file ownership using chown(1). Refer to the chown(1) man page for more information.

Your system administrator can tell you what type of privileges you have been granted. You can also execute the getprivgrp(1) command to determine the special attributes for groups to which you belong:

getprivgrp [groupname]

where groupname is the name of the group for which you want to determine your special attributes. If omitted, the command lists the access privileges for all privileged groups to which you belong. Refer to the getprivgrp(1) man page for more information.

Discretionary Access Control

==========

Using discretionary access control (DAC), owners of objects containing data can allow or deny access to these objects at their own discretion, on a need-to-know basis. Objects are things such as files, devices, or interprocess communications mechanisms that another user's process or your process is attempting to access. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission to any other subject.

On a standard HP-UX system, you can protect objects, such as files, by establishing read, write, and access permissions to these objects. If you are the owner, you can set permissions on objects so that your access is different from other group members; group members can have different access to an object than the rest of the user community. The owner can change these protection attributes so they are more restrictive(controlled access) or more permissive (open access).

You can use the chown and chmod commands to control file and directory access. For more information, refer to the chown(1) and chmod(1) online man pages. To learn how to change your current group selection, refer also to the newgrp(1) man page. The newgrp command changes your group ID without changing your user ID and replaces your current shell with a new one.

On a C2-level trusted system, you can have additional discretionary controls on an object that let you include or exclude access even to specific users. You control who (that is, users or groups of users) has access to files and directories by assigning optional access control lists (ACL) permissions.

Realize that the system administrator can use the su(1) command to become another user without logging out. The system administrator or superuser can access all files and perform any task on the system. So file access is not restricted for system administrators. Refer to the su(1) online man page for more information.

Access Control Lists (ACLs)

==========

Access control lists are key to enforcing discretionary access control on trusted systems. ACLs offer a greater degree of selectivity than HP-UX permission bits.

An access control list is a set of user, group, and mode entries associated with a file that specify permissions for all possible user ID or group ID combinations.

Refer to the acl(5) online man page for detailed information about access control lists and definitions of related security terminology.

Listing ACLs

To see who can access certain files and directories and what permissions are allowed, you can use the lsacl command:

$ lsacl filename

The system responds with a listing in this general form:

(user.group,mode) ... filename

where (user.group,mode) is an ACL entry and filename is the name of the file or directory for which you want a listing.

For example:

$ lsacl filex

(sarah.adm,rw-) (alex.%,r—) (%.mtg,r—) (%.%,—-) xfile

where:

(sarah.adm,rw-) means user sarah in group adm has read and write permissions (rw-) on xfile.

(alex.%,r—) means user alex in any group (%) has read permission (r—) on xfile.

(%.mtg,r—) means any user (%) in the group mtg has read permission (r—) on xfile.

(%.%,—-) means no other user from any other group has read, write or execute permission on xfile.

Changing ACLs

By adding entries to access control lists, you can allow or deny access to particular users or groups of users. You can set or change ACLs using the chacl command.

The general form of the chacl command is as follows:

$ chacl 'user.group operator mode' filename

where:

user is the login name; a % here means all users.

group is the user's group; a % here means all groups.

operator is +, -, or = to add, deny, or specify permissions to existing ACL entries.

mode indicates the permissions allowed (that is, r for read, w for write, and x for execute/search.

filename is the name of the file or directory for which you want to specify access.

For example:

$ chacl 'cyc.%=rw' myfile

Creates a new ACL entry allowing the user cyc in any group (%) read and write (=rw) access to myfile.

$ chacl '%.%+r' status

Modifies an ACL entry to allow all users(%) in all groups (%) read access (+r) to the file status.

Refer to the chacl(1) online man page for more information and examples of setting ACLs.

Additional Warnings

---

* If a file contains ACLs and you use the chmod command to change file mode access permissions without using the -A option, you will delete any optional entries in the file's ACL.

* Trying to delete a base ACL entry will result in no access to a file.

* Only the fbackup (1M) and frecover(1M) file archive utilities handle ACLs correctly. Archive programs such as AR(1), cpio(1), ftio(1), tar(1), and dump(1M) are unable to handle ACLs on files with optional ACL entries.

Backing Up and Recovering Files

==========

On a trusted system, you should only use fbackup(1M) and frecover(1M) to back up and recover files selectively. These commands retain ACLs that have been applied to the files. Your system administrator can help with the authorized copying of files to tape or disk. It is likely you will have to get permission to use the tape drive or other media and you will need to get the name of the device.

Realize that you need to keep copied files in a safe location. Label tapes and disks. Make sure the files are copied with the correct access permissions if you load them onto another system.

Refer to the fbackup(1M) and frecover(1M) online man pages for more information.

Removable Media Security

==========

It is your responsibility to protect the physical security of removable media such as floppy disks and tapes. Do not leave them lying around. It is best to keep them locked up since it is easy for other people to read what you have on these media.

The command tar(1) needs to be used properly to ensure that the DAC permissions are preserved when coping files to and from tape. Be sure to use the -p when taring files from a tape to your system in order to preserve DAC permissions. See the tar(1) man page for more information.

Running Commands at Preset Times using at and crontab

==========

The at and crontab commands are useful if you want to run resource intensive commands when demands on the system are low or to routinely run commands at certain times. For example, you can schedule a long file to print at midnight or erase temporary files in your home directory everyday.

at runs commands in your home directory at the time you specify. crontab runs commands in your home directory at regularly specified intervals.

Prerequisites for using at and crontab

Before you can use crontab or at, your system administrator must set up certain files that allow you permission to run these commands.

Two files called at.allow and at.deny in /usr/lib/cron determine whether you can use the at command. You can use it if your name is in at.allow.

If at.allow does not exist, the system checks to see if your name is in at.deny. If it is, you are denied access to the at command.

If neither at.allow nor at.deny exists, only those with superuser privilege can use at. If only at.deny exists and it is empty, all users can use at.

Permission to use crontab is determined in the same way except that the files are called cron.allow and cron.deny.

Refer to the at(1) and crontab(1) man pages for more information.

Running Commands using at

Suppose you want to print a large file at night when system usage is low. The following at command sequence prints the file bigfile at 4:00 AM.

at 4am Type the at command

lp bigfile Enter the command you want to schedule for later.

Ctrl-D End the command by pressing Ctrl-D.

You can also specify a date. For example, to print a file on January 1- at 3:30 AM, use the following commands:

at 3:30am Apr 10

lp bigfile

Ctrl-D

To list jobs scheduled with at, enter:

at -l

You will see output such as:

job 617 at wed apr 10 030:30:00 1996

Running Commands at Regular Intervals using crontab

You can use the crontab command to run commands at regular intervals. For example, you can send a weekly reminder for a meeting to your mailbox or erase all tmp files everyday.

The crontab command creates a file called by your username in the directory /usr/spool/cron/crontabs. The commands in the file are executed at the specified intervals in your home directory.

A crontab file contains line with six fields each separated by spaces or tabs. The first five fields specify the time the command will be run

minute (0-59)

hour (0-23)

date of the month (1-31)

month of the year (1-12)

day of the week (0-6 with 0=Sunday)

The sixth field is a string that is executed at the appropriate time.

To create a crontab command file, enter:

crontab

Then type the commands you want to schedule and press Ctrl-D.

30 8 * * 4 echo "Staff meeting today at 10:00 AM"

0 0 rm *.tmp 2 > errfile

Ctrl-D

The crontab file is interperted as follows:

On Thursday at 8:30 AM, crontab sends you a reminder of your 10:00 AM staff meeting. The first field (30) indicates 30 minutes after the hour. The second

field indicates the hour (8). The asterisks mean all legal values. The 4 means Thursday.

At midnight everyday, crontab erases files with a *.tmp extension in your directory. Error messages are redirected to a file called errmsg in your home directory.

Refer to the crontab(1) man page for more information.

Submitting Batch Jobs

You can also use the batch command to submit a batch file. For example:

batch

nroff filename > outfile

Ctrl-D

This command executes an nroff command when the system is able to handle it. Refer to the batch (1) man page for more details.

Index