



Practical UNIX & Internet Security

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

Index: A

absolute pathnames : [5.1.3. Current Directory and Paths](#)

access

 /etc/exports file : [20.2.1.1. /etc/exports](#)

 levels, NIS+ : [19.5.4. Using NIS+](#)

 by non-citizens : [26.4.1. Munitions Export](#)

 tradition of open : [1.4.1. Expectations](#)

 via Web : [18.2.2.2. Additional configuration issues](#)

access control : [2.1. Planning Your Security Needs](#)

 ACLs

[5.2.5. Access Control Lists](#)

[5.2.5.2. HP-UX access control lists](#)

[17.3.13. Network News Transport Protocol \(NNTP\) \(TCP Port 119\)](#)

 anonymous FTP : [17.3.2.1. Using anonymous FTP](#)

 Internet servers : [17.2. Controlling Access to Servers](#)

 monitoring employee access : [13.2.4. Auditing Access](#)

 physical : [12.2.3. Physical Access](#)

 restricted filesystems

[8.1.5. Restricted Filesystem](#)

[8.1.5.2. Checking new software](#)

 restricting data availability : [2.1. Planning Your Security Needs](#)

 USERFILE (UUCP)

[15.4.1. USERFILE: Providing Remote File Access](#)

[15.4.2.1. Some bad examples](#)

 Web server files

[18.3. Controlling Access to Files on Your Server](#)

[18.3.3. Setting Up Web Users and Passwords](#)

 X Window System

[17.3.21.2. X security](#)

[17.3.21.3. The xhost facility](#)

access control lists : (see [ACLs](#))

access.conf file : [18.3.1. The access.conf and .htaccess Files](#)

access() : [23.2. Tips on Avoiding Security-related Bugs](#)

access_log file

[10.3.5. access_log Log File](#)

[18.4.2. Eavesdropping Through Log Files](#)
with refer_log file : [18.4.2. Eavesdropping Through Log Files](#)

accidents
[12.2.2. Preventing Accidents](#)
(see also [natural disasters](#))

accounting process
[10.2. The acct/pacct Process Accounting File](#)
[10.2.3. messages Log File](#)
(see also [auditing](#))

accounts : [3.1. Usernames](#)
aliases for : [8.8.9. Account Names Revisited: Using Aliases for Increased Security](#)
changing login shell
[8.4.2. Changing the Account's Login Shell](#)
[8.7.1. Integrating One-time Passwords with UNIX](#)
created by intruders : [24.4.1. New Accounts](#)
default : [8.1.2. Default Accounts](#)
defense checklist : [A.1.1.7. Chapter 8: Defending Your Accounts](#)
dormant
[8.4. Managing Dormant Accounts](#)
[8.4.3. Finding Dormant Accounts](#)
expiring old : [8.4.3. Finding Dormant Accounts](#)
group : [8.1.6. Group Accounts](#)
importing to NIS server
[19.4.1. Including or excluding specific accounts:](#)
[19.4.4.2. Using netgroups to limit the importing of accounts](#)

Joes
[3.6.2. Smoking Joes](#)
[8.8.3.1. Joetest: a simple password cracker](#)

locking automatically : [3.3. Entering Your Password](#)
logging changes to : [10.7.2.1. Exception and activity reports](#)
multiple, same UID : [4.1.2. Multiple Accounts with the Same UID](#)
names for : (see [usernames](#))
restricted, with rsh : [8.1.4.5. How to set up a restricted account with rsh](#)
restricting FTP from : [17.3.2.5. Restricting FTP with the standard UNIX FTP server](#)
running single command : [8.1.3. Accounts That Run a Single Command](#)
without passwords : [8.1.1. Accounts Without Passwords](#)

acct file : [10.2. The acct/pacct Process Accounting File](#)

acctcom program

[10.2. The acct/pacct Process Accounting File](#)

[10.2.2. Accounting with BSD](#)

ACEs : (see [ACLs](#))

ACK bit : [16.2.4.2. TCP](#)

acledit command : [5.2.5.1. AIX Access Control Lists](#)

aclget, aclput commands : [5.2.5.1. AIX Access Control Lists](#)

ACLs (access control lists)

[5.2.5. Access Control Lists](#)

[5.2.5.2. HP-UX access control lists](#)

errors in : [5.2.5.1. AIX Access Control Lists](#)

NNTP with : [17.3.13. Network News Transport Protocol \(NNTP\) \(TCP Port 119\)](#)

ACM (Association for Computing Machinery) : [E.1.1. Association for Computing Machinery \(ACM\)](#)

active FTP : [17.3.2.2. Passive vs. active FTP](#)

aculog file : [10.3.1. aculog File](#)

adaptive modems : (see [modems](#))

adb debugger

[19.3.1.3. Setting the window](#)

[C.4. The kill Command](#)

add-on functionality : [1.4.3. Add-On Functionality Breeds Problems](#)

addresses

CIDR : [16.2.1.3. CIDR addresses](#)

commands embedded in : [15.7. Early Security Problems with UUCP Internet](#)

[16.2.1. Internet Addresses](#)

[16.2.1.3. CIDR addresses](#)

IP : (see [IP addresses](#))

Adleman, Leonard

[6.4.2. Summary of Public Key Systems](#)

[6.4.6. RSA and Public Key Cryptography](#)

.Admin directory : [10.3.4. uucp Log Files](#)

administration : (see [system administration](#))

adult material : [26.4.5. Pornography and Indecent Material](#)

Advanced Network & Services (ANS) : [F.3.4.2. ANS customers](#)

AFCERT : [F.3.4.41. U.S. Air Force](#)

ftpd server : [17.3.2.4. Setting up an FTP server](#)

agent (user) : [4.1. Users and Groups](#)

agent_log file : [18.4.2. Eavesdropping Through Log Files](#)

aging : (see [expiring](#))

air ducts : [12.2.3.2. Entrance through air ducts](#)

air filters : [12.2.1.3. Dust](#)

Air Force Computer Emergency Response Team (AFCERT) : [F.3.4.41. U.S. Air Force](#)

AIX

[3.3. Entering Your Password](#)

[8.7.1. Integrating One-time Passwords with UNIX](#)

access control lists : [5.2.5.1. AIX Access Control Lists](#)

tftp access : [17.3.7. Trivial File Transfer Protocol \(TFTP\) \(UDP Port 69\)](#)

trusted path : [8.5.3.1. Trusted path](#)

alarms : (see [detectors](#))

aliases

[8.8.9. Account Names Revisited: Using Aliases for Increased Security](#)

[11.1.2. Back Doors and Trap Doors](#)

[11.5.3.3. /usr/lib/aliases, /etc/aliases, /etc/sendmail/aliases, aliases.dir, or aliases.pag](#)

decode : [17.3.4.2. Using sendmail to receive email](#)

mail : [17.3.4. Simple Mail Transfer Protocol \(SMTP\) \(TCP Port 25\)](#)

aliases file : [11.5.3.3. /usr/lib/aliases, /etc/aliases, /etc/sendmail/aliases, aliases.dir, or aliases.pag](#)

AllowOverride option : [18.3.2. Commands Within the <Directory> Block](#)

American Society for Industrial Security (ASIS) : [F.1.2. American Society for Industrial Security \(ASIS\)](#)

ancestor directories : [9.2.2.2. Ancestor directories](#)

ANI schemes : [14.6. Additional Security for Modems](#)

animals : [12.2.1.7. Bugs \(biological\)](#)

anlpasswd package : [8.8.2. Constraining Passwords](#)

anon option for /etc/exports : [20.2.1.1. /etc/exports](#)

anonymous FTP

[4.1. Users and Groups](#)

[17.3.2.1. Using anonymous FTP](#)

[17.3.2.6. Setting up anonymous FTP with the standard UNIX FTP server and HTTP : 18.2.4.1. Beware mixing HTTP with anonymous FTP](#)

ANS (Advanced Network & Services, Inc.) : [F.3.4.2. ANS customers](#)

ANSI C standards : [1.4.2. Software Quality](#)

answer mode : [14.3.1. Originate and Answer](#)

answer testing : [14.5.3.2. Answer testing](#)

answerback terminal mode : [11.1.4. Trojan Horses](#)
APOP option (POP) : [17.3.10. Post Office Protocol \(POP\) \(TCP Ports 109 and 110\)](#)
Apple CORES (Computer Response Squad) : [F.3.4.3. Apple Computer worldwide R&D community](#)
Apple Macintosh, Web server on : [18.2. Running a Secure Server](#)
applets : [11.1.5. Viruses](#)
application-level encryption : [16.3.1. Link-level Security](#)
applications, CGI : (see [CGI, scripts](#))
ar program : [7.4.2. Simple Archives](#)
architecture, room : [12.2.3. Physical Access](#)
archiving information
 [7.1.1.1. A taxonomy of computer failures](#)
 (see also [logging](#))
arguments, checking : [23.2. Tips on Avoiding Security-related Bugs](#)
ARPA (Advanced Research Projects Agency)
 [1.3. History of UNIX](#)
 (see also [UNIX, history of](#))
 ARPANET network : [16.1.1. The Internet](#)
ASIS (American Society for Industrial Security) : [F.1.2. American Society for Industrial Security \(ASIS\)](#)
assert macro : [23.2. Tips on Avoiding Security-related Bugs](#)
assessing risks
 [2.2. Risk Assessment](#)
 [2.2.2. Review Your Risks](#)
 [2.5.3. Final Words: Risk Management Means Common Sense](#)
assets, identifying : [2.2.1.1. Identifying assets](#)
ASSIST : [F.3.4.42. U.S. Department of Defense](#)
Association for Computing Machinery (ACM) : [F.1.1. Association for Computing Machinery \(ACM\)](#)
asymmetric key cryptography : [6.4. Common Cryptographic Algorithms](#)
asynchronous systems : [19.2. Sun's Remote Procedure Call \(RPC\)](#)
Asynchronous Transfer Mode (ATM) : [16.2. IPv4: The Internet Protocol Version 4](#)
at program
 [11.5.3.4. The at program](#)
 [25.2.1.2. System overload attacks](#)
AT&T System V : (see [System V UNIX](#))
Athena : (see [Kerberos system](#))

atime

[5.1.2. Inodes](#)

[5.1.5. File Times](#)

ATM (Asynchronous Transfer Mode) : [16.2. IPv4: The Internet Protocol Version 4](#)

attacks : (see [threats](#))

audio device : [23.8. Picking a Random Seed](#)

audit IDs

[4.3.3. Other IDs](#)

[10.1. The Basic Log Files](#)

auditing

[10. Auditing and Logging](#)

(see also [logging](#))

C2 audit : [10.1. The Basic Log Files](#)

checklist for : [A.1.1.9. Chapter 10: Auditing and Logging](#)

employee access : [13.2.4. Auditing Access](#)

login times : [10.1.1. lastlog File](#)

system activity : [2.1. Planning Your Security Needs](#)

user activity : [4.1.2. Multiple Accounts with the Same UID](#)

who is logged in

[10.1.2. utmp and wtmp Files](#)

[10.1.2.1. su command and /etc/utmp and /var/adm/wtmp files](#)

AUTH_DES authentication : [19.2.2.3. AUTH_DES](#)

AUTH_KERB authentication : [19.2.2.4. AUTH_KERB](#)

AUTH_NONE authentication : [19.2.2.1. AUTH_NONE](#)

AUTH_UNIX authentication : [19.2.2.2. AUTH_UNIX](#)

authd service : [23.3. Tips on Writing Network Programs](#)

authdes_win variable : [19.3.1.3. Setting the window](#)

authentication : [3.2.3. Authentication](#)

ID services : [16.3.3. Authentication](#)

Kerberos

[19.6.1. Kerberos Authentication](#)

[19.6.1.4. Kerberos 4 vs. Kerberos 5](#)

of logins : [17.3.5. TACACS \(UDP Port 49\)](#)

message digests

[6.5.2. Using Message Digests](#)

[9.2.3. Checksums and Signatures](#)

[23.5.1. Use Message Digests for Storing Passwords](#)

NIS+ : [19.5.4. Using NIS+](#)

RPCs

[19.2.2. RPC Authentication](#)

[19.2.2.4. AUTH KERB](#)

Secure RPC : [19.3.1. Secure RPC Authentication](#)

security standard for : [2.4.2. Standards](#)

for Web use : [18.3.3. Setting Up Web Users and Passwords](#)

xhost facility : [17.3.21.3. The xhost facility](#)

authenticators : [3.1. Usernames](#)

AuthGroupFile option : [18.3.2. Commands Within the <Directory> Block](#)

authors of programmed threats : [11.3. Authors](#)

AuthRealm option : [18.3.2. Commands Within the <Directory> Block](#)

AuthType option : [18.3.2. Commands Within the <Directory> Block](#)

AuthUserFile option : [18.3.2. Commands Within the <Directory> Block](#)

Auto_Mounter table (NIS+) : [19.5.3. NIS+ Tables](#)

autologout shell variable : [12.3.5.1. Built-in shell autologout](#)

Automated Systems Incident Response Capability (NASA) : [F.3.4.24. NASA: NASA-wide](#)

automatic

[11.5.3. Abusing Automatic Mechanisms](#)

(see also [at program](#); [cron file](#))

account lockout : [3.3. Entering Your Password](#)

backups system : [7.3.2. Building an Automatic Backup System](#)

cleanup scripts (UUCP) : [15.6.2. Automatic Execution of Cleanup Scripts](#)

directory listings (Web) : [18.2.2.2. Additional configuration issues](#)

disabling of dormant accounts : [8.4.3. Finding Dormant Accounts](#)

logging out : [12.3.5.1. Built-in shell autologout](#)

mechanisms, abusing

[11.5.3. Abusing Automatic Mechanisms](#)

[11.5.3.6. Other files](#)

password generation : [8.8.4. Password Generators](#)

power cutoff : (see [detectors](#))

sprinkler systems : [12.2.1.1. Fire](#)

wtmp file pruning : [10.1.3.1. Pruning the wtmp file](#)

auxiliary (printer) ports : [12.3.1.4. Auxiliary ports on terminals](#)

awareness, security : (see [security, user awareness of](#))

awk scripts

[11.1.4. Trojan Horses](#)

[11.5.1.2. IFS attacks](#)

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

[Copyright](#) © 1999 [O'Reilly & Associates, Inc.](#) All Rights Reserved.

[[Library Home](#) | [DNS & BIND](#) | [TCP/IP](#) | [sendmail](#) | [sendmail Reference](#) | [Firewalls](#) | [Practical Security](#)]



Practical UNIX & Internet Security

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

Index: B

back doors

[2.5. The Problem with Security Through Obscurity](#)

[6.2.3. Cryptographic Strength](#)

[11.1. Programmed Threats: Definitions](#)

[11.1.2. Back Doors and Trap Doors](#)

[11.5. Protecting Yourself](#)

[27.1.2. Trusting Trust](#)

in MUDs and IRCs : [17.3.23. Other TCP Ports: MUDs and Internet Relay Chat \(IRC\)](#)

background checks, employee : [13.1. Background Checks](#)

backquotes in CGI input

[18.2.3.2. Testing is not enough!](#)

[18.2.3.3. Sending mail](#)

BACKSPACE key : [3.4. Changing Your Password](#)

backup program : [7.4.3. Specialized Backup Programs](#)

backups

[7. Backups](#)

[7.4.7. inode Modification Times](#)

[9.1.2. Read-only Filesystems](#)

[24.2.2. What to Do When You Catch Somebody](#)

across networks : [7.4.5. Backups Across the Net](#)

for archiving information : [7.1.1.1. A taxonomy of computer failures](#)
automatic

[7.3.2. Building an Automatic Backup System](#)

[18.2.3.5. Beware stray CGI scripts](#)

checklist for : [A.1.1.6. Chapter 7: Backups](#)

criminal investigations and : [26.2.4. Hazards of Criminal Prosecution](#)
of critical files

[7.3. Backing Up System Files](#)

[7.3.2. Building an Automatic Backup System](#)

encrypting

[7.4.4. Encrypting Your Backups](#)

[12.3.2.4. Backup encryption](#)

hardcopy : [24.5.1. Never Trust Anything Except Hardcopy](#)

keeping secure

[2.4.2. Standards](#)

[2.4.3. Guidelines](#)

[7.1.6. Security for Backups](#)

[7.1.6.3. Data security for backups](#)

[26.2.6. Other Tips](#)

laws concerning : [7.1.7. Legal Issues](#)

of log files : [10.2.2. Accounting with BSD](#)

retention of

[7.1.5. How Long Should You Keep a Backup?](#)

[7.2. Sample Backup Strategies](#)

[7.2.5. Deciding upon a Backup Strategy](#)

rotating media : [7.1.3. Types of Backups](#)

software for

[7.4. Software for Backups](#)

[7.4.7. inode Modification Times](#)

commercial : [7.4.6. Commercial Offerings](#)

special programs for : [7.4.3. Specialized Backup Programs](#)

strategies for

[7.2. Sample Backup Strategies](#)

[7.2.5. Deciding upon a Backup Strategy](#)

[10.8. Managing Log Files](#)

theft of

[12.3.2. Protecting Backups](#)

[12.3.2.4. Backup encryption](#)

verifying : [12.3.2.1. Verify your backups](#)

zero-filled bytes in : [7.4. Software for Backups](#)

bacteria

[11.1. Programmed Threats: Definitions](#)

[11.1.7. Bacteria and Rabbits](#)

BADSU attempts : (see [sulog file](#))

Baldwin, Robert : [6.6.1.1. The crypt program](#)

bang (!) and mail command : [15.1.3. mail Command](#)

Bash shell (bsh) : [8.1.4.4. No restricted bash](#)

Basic Networking Utilities : (see [BNU UUCP](#))

bastion hosts : [21.1.3. Anatomy of a Firewall](#)

batch command : [25.2.1.2. System overload attacks](#)

batch jobs : (see [cron file](#))

baud : [14.1. Modems: Theory of Operation](#)

bell (in Swatch program) : [10.6.2. The Swatch Configuration File](#)

Bellcore : [F.3.4.5. Bellcore](#)

Berkeley UNIX : (see [BSD UNIX](#))

Berkeley's sendmail : (see [sendmail](#))

bidirectionality

[14.1. Modems: Theory of Operation](#)

[14.4.1. One-Way Phone Lines](#)

bigcrypt algorithm : [8.6.4. Crypt16\(\) and Other Algorithms](#)

/bin directory

[11.1.5. Viruses](#)

[11.5.1.1. PATH attacks](#)

backing up : [7.1.2. What Should You Back Up?](#)

/bin/csh : (see [csh](#))

/bin/ksh : (see [ksh](#))

/bin/login : (see [login program](#))

/bin/passwd : (see [passwd command](#))

/bin/sh : (see [sh](#))

in restricted filesystems : [8.1.5. Restricted Filesystem](#)

binary code : [11.1.5. Viruses](#)

bind system call

[16.2.6.1. DNS under UNIX](#)

[17.1.3. The /etc/inetd Program](#)

biological threats : [12.2.1.7. Bugs \(biological\)](#)

block devices : [5.6. Device Files](#)

block send commands : [11.1.4. Trojan Horses](#)

blocking systems : [19.2. Sun's Remote Procedure Call \(RPC\)](#)

BNU UUCP

[15.5. Security in BNU UUCP](#)

[15.5.3. uucheck: Checking Your Permissions File](#)

Boeing CERT : [F.3.4.5. Bellcore](#)

bogusns directive : [17.3.6.2. DNS nameserver attacks](#)

boot viruses : [11.1.5. Viruses](#)

Bootparams table (NIS+) : [19.5.3. NIS+ Tables](#)

Bourne shell

[C.5.3. Running the User's Shell](#)

(see also [sh program](#); [shells](#))

(see [sh](#))

Bourne shell (sh) : [C.5.3. Running the User's Shell](#)

bps (bits per second) : [14.1. Modems: Theory of Operation](#)

BREAK key : [14.5.3.2. Answer testing](#)

breakins

checklist for : [A.1.1.23. Chapter 24: Discovering a Break-in](#)

legal options following : [26.1. Legal Options After a Break-in](#)

responding to

[24. Discovering a Break-in](#)

[24.7. Damage Control](#)

resuming operation after : [24.6. Resuming Operation](#)

broadcast storm : [25.3.2. Message Flooding](#)

browsers : (see [Web browsers](#))

BSD UNIX

[Which UNIX System?](#)

[1.3. History of UNIX](#)

accounting with : [10.2.2. Accounting with BSD](#)

Fast Filesystem (FFS) : [25.2.2.6. Reserved space](#)

groups and : [4.1.3.3. Groups and BSD or SVR4 UNIX](#)

immutable files : [9.1.1. Immutable and Append-Only Files](#)

modems and : [14.5.1. Hooking Up a Modem to Your Computer](#)

programming references : [D.1.11. UNIX Programming and System Administration](#)

ps command with : [C.1.2.2. Listing processes with Berkeley-derived versions of UNIX](#)

published resources for : [D.1. UNIX Security References](#)

restricted shells : [8.1.4.2. Restricted shells under Berkeley versions](#)

SUID files, list of : [B.3. SUID and SGID Files](#)

sulog log under : [4.3.7.1. The sulog under Berkeley UNIX](#)

utmp and wtmp files : [10.1.2. utmp and wtmp Files](#)

BSD/OS (operating system) : [1.3. History of UNIX](#)

bsh (Bash shell) : [8.1.4.4. No restricted bash](#)

BSI/GISA : [F.3.4.15. Germany: government institutions](#)

buffers

checking boundaries : [23.2. Tips on Avoiding Security-related Bugs](#)

for editors : [11.1.4. Trojan Horses](#)

bugs

[1.1. What Is Computer Security?](#)

[1.4.2. Software Quality](#)

[23.1.2.1. What they found](#)

[27.2.3. Buggy Software](#)

[27.2.5. Security Bugs that Never Get Fixed](#)

Bugtraq mailing list : [E.1.3.3. Bugtraq](#)
hacker challenges : [27.2.4. Hacker Challenges](#)
hardware : [27.2.1. Hardware Bugs](#)
.htaccess file : [18.3.1. The access.conf and .htaccess Files](#)
keeping secret : [2.5. The Problem with Security Through Obscurity](#)
tips on avoiding : [23.2. Tips on Avoiding Security-related Bugs](#)
bugs (biological) : [12.2.1.7. Bugs \(biological\)](#)
bugs
 [Preface](#)
 (see also [security holes](#))
bulk erasers : [12.3.2.3. Sanitize your media before disposal](#)
byte-by-byte comparisons
 [9.2.1. Comparison Copies](#)
 [9.2.1.3. rdist](#)
bytes, zero-filled : [7.4. Software for Backups](#)

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

[Copyright](#) © 1999 [O'Reilly & Associates, Inc.](#) All Rights Reserved.

[[Library Home](#) | [DNS & BIND](#) | [TCP/IP](#) | [sendmail](#) | [sendmail Reference](#) | [Firewalls](#) | [Practical Security](#)]



Practical UNIX & Internet Security

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

Index: C

C programming language

[1.3. History of UNIX](#)

[23.2. Tips on Avoiding Security-related Bugs](#)

-Wall compiler option : [23.2. Tips on Avoiding Security-related Bugs](#)

C shell : (see [csh](#))

C2 audit : [10.1. The Basic Log Files](#)

cables, network

[12.2.4.2. Network cables](#)

[12.3.1.5. Fiber optic cable](#)

cutting : [25.1. Destructive Attacks](#)

tampering detectors for : [12.3.1.1. Wiretapping](#)

wiretapping : [12.3.1.1. Wiretapping](#)

cache, nameserver : [16.3.2. Security and Nameservice](#)

caching : [5.6. Device Files](#)

Caesar Cipher : [6.4.3. ROT13: Great for Encoding Offensive Jokes](#)

calculating costs of losses : [2.3.1. The Cost of Loss](#)

call forwarding : [14.5.4. Physical Protection of Modems](#)

Call Trace : [24.2.4. Tracing a Connection](#)

CALLBACK= command : [15.5.2. Permissions Commands](#)

callbacks

[14.4.2.](#)

[14.6. Additional Security for Modems](#)

BNU UUCP : [15.5.2. Permissions Commands](#)

Version 2 UUCP : [15.4.1.5. Requiring callback](#)

Caller-ID (CNID)

[14.4.3. Caller-ID \(CNID\)](#)

[14.6. Additional Security for Modems](#)

[24.2.4. Tracing a Connection](#)

Canada, export control in : [6.7.2. Cryptography and Export Controls](#)

carbon monoxide : [12.2.1.2. Smoke](#)

caret (^) in encrypted messages : [6.2. What Is Encryption?](#)

case in usernames : [3.1. Usernames](#)

cat command

[3.2.2. The /etc/passwd File and Network Databases](#)

[15.4.3. L.cmds: Providing Remote Command Execution](#)
-ve option : [5.5.4.1. The ncheck command](#)
-v option : [24.4.1.7. Hidden files and directories](#)
cat-passwd command : [3.2.2. The /etc/passwd File and Network Databases](#)
CBC (cipher block chaining)
[6.4.4.2. DES modes](#)
[6.6.2. des: The Data Encryption Standard](#)
CBW (Crypt Breaker's Workbench) : [6.6.1.1. The crypt program](#)
CCTA IT Security & Infrastructure Group : [F.3.4.39. UK: other government departments and agencies](#)
CD-ROM : [9.1.2. Read-only Filesystems](#)
CDFs (context-dependent files)
[5.9.2. Context-Dependent Files](#)
[24.4.1.7. Hidden files and directories](#)
ceilings, dropped : [12.2.3.1. Raised floors and dropped ceilings](#)
cellular telephones : [12.2.1.8. Electrical noise](#)
CERCUS (Computer Emergency Response Committee for Unclassified Systems) : [F.3.4.36. TRW network area and system administrators](#)
Cerf, Vint : [16.2. IPv4: The Internet Protocol Version 4](#)
CERN : [E.4.1. CERN HTTP Daemon](#)
CERT (Computer Emergency Response Team)
[6.5.2. Using Message Digests](#)
[27.3.5. Response Personnel?](#)
[F.3.4.1. All Internet sites](#)
CERT-NL (Netherlands) : [F.3.4.25. Netherlands: SURFnet-connected sites](#)
mailing list for : [E.1.3.4. CERT-advisory](#)
CFB (cipher feedback) : [6.4.4.2. DES modes](#)
CGI (Common Gateway Interface) : [18.1. Security and the World Wide Web](#)
scripts
[18.2. Running a Secure Server](#)
[18.2.3. Writing Secure CGI Scripts and Programs](#)
[18.2.4.1. Beware mixing HTTP with anonymous FTP](#)
cgi-bin directory : [18.2.2. Understand Your Server's Directory Structure](#)
chacl command : [5.2.5.2. HP-UX access control lists](#)
-f option : [5.2.5.2. HP-UX access control lists](#)
-r option : [5.2.5.2. HP-UX access control lists](#)
change detection
[9.2. Detecting Change](#)
[9.3. A Final Note](#)

character devices : [5.6. Device Files](#)

chat groups, harassment via : [26.4.7. Harassment, Threatening Communication, and Defamation](#)

chdir command

[23.2. Tips on Avoiding Security-related Bugs](#)

[25.2.2.8. Tree-structure attacks](#)

checklists for detecting changes

[9.2.2. Checklists and Metadata](#)

[9.2.3. Checksums and Signatures](#)

checksums

[6.5.5.1. Checksums](#)

[9.2.3. Checksums and Signatures](#)

Chesson, Greg : [15.2. Versions of UUCP](#)

chfn command : [8.2. Monitoring File Format](#)

chgrp command : [5.8. chgrp: Changing a File's Group](#)

child processes : [C.2. Creating Processes](#)

chkey command : [19.3.1.1. Proving your identity](#)

chmod command

[5.2.1. chmod: Changing a File's Permissions](#)

[5.2.4. Using Octal File Permissions](#)

[8.3. Restricting Logins](#)

-A option : [5.2.5.2. HP-UX access control lists](#)

-f option : [5.2.1. chmod: Changing a File's Permissions](#)

-h option : [5.2.1. chmod: Changing a File's Permissions](#)

-R option : [5.2.1. chmod: Changing a File's Permissions](#)

chokes : (see [firewalls](#))

chown command

[5.7. chown: Changing a File's Owner](#)

[23.2. Tips on Avoiding Security-related Bugs](#)

chroot system call

[8.1.5. Restricted Filesystem](#)

[8.1.5.2. Checking new software](#)

[11.1.4. Trojan Horses](#)

[23.4.1. Using chroot\(\)](#)

with anonymous FTP : [17.3.2.6. Setting up anonymous FTP with the standard UNIX FTP server](#)

chrootuid daemon : [E.4.2. chrootuid](#)

chsh command : [8.7.1. Integrating One-time Passwords with UNIX](#)

CIAC (Computer Incident Advisory Capability) : [F.3.4.43. U.S. Department of](#)

[Energy sites, Energy Sciences Network \(ESnet\), and DOE contractors](#)

CIDR (Classless InterDomain Routing)

[16.2.1.1. IP networks](#)

[16.2.1.3. CIDR addresses](#)

cigarettes : [12.2.1.2. Smoke](#)

cipher

[6.4.3. ROT13: Great for Encoding Offensive Jokes](#)

(see also [cryptography](#); [encryption](#))

block chaining (CBC)

[6.4.4.2. DES modes](#)

[6.6.2. des: The Data Encryption Standard](#)

ciphertext

[6.2. What Is Encryption?](#)

[8.6.1. The crypt\(\) Algorithm](#)

feedback (CFB) : [6.4.4.2. DES modes](#)

CISCO : [F.3.4.8. CISCO Systems](#)

civil actions (lawsuits) : [26.3. Civil Actions](#)

classified data and breakins

[26.1. Legal Options After a Break-in](#)

[26.2.2. Federal Jurisdiction](#)

Classless InterDomain Routing (CIDR)

[16.2.1.1. IP networks](#)

[16.2.1.3. CIDR addresses](#)

clear text : [8.6.1. The crypt\(\) Algorithm](#)

Clear to Send (CTS) : [14.3. The RS-232 Serial Protocol](#)

client flooding : [16.3.2. Security and Nameservice](#)

client/server model : [16.2.5. Clients and Servers](#)

clients, NIS : (see [NIS](#))

clock, system

[5.1.5. File Times](#)

[17.3.14. Network Time Protocol \(NTP\) \(UDP Port 123\)](#)

for random seeds : [23.8. Picking a Random Seed](#)

resetting : [9.2.3. Checksums and Signatures](#)

Secure RPC timestamp : [19.3.1.3. Setting the window](#)

clogging : [25.3.4. Clogging](#)

CMW (Compartmented-Mode Workstation) : ["Secure" Versions of UNIX](#)

CNID (Caller-ID)

[14.4.3. Caller-ID \(CNID\)](#)

[14.6. Additional Security for Modems](#)

[24.2.4. Tracing a Connection](#)

CO2 system (for fires) : [12.2.1.1. Fire](#)

COAST (Computer Operations, Audit, and Security Technology)

[E.3.2. COAST](#)

[E.4. Software Resources](#)

code breaking : (see [cryptography](#))

codebooks : [8.7.3. Code Books](#)

CodeCenter : [23.2. Tips on Avoiding Security-related Bugs](#)

cold, extreme : [12.2.1.6. Temperature extremes](#)

command shells : (see [shells](#))

commands

[8.1.3. Accounts That Run a Single Command](#)

(see also under specific command name)

accounts running single : [8.1.3. Accounts That Run a Single Command](#)

in addresses : [15.7. Early Security Problems with UUCP](#)

editor, embedded : [11.5.2.7. Other initializations](#)

remote execution of

[15.1.2. uux Command](#)

[15.4.3. L.cmds: Providing Remote Command Execution](#)

[17.3.17. rexec \(TCP Port 512\)](#)

running simultaneously

[23.2. Tips on Avoiding Security-related Bugs](#)

(see also [multitasking](#))

commands in <Directory> blocks : [18.3.2. Commands Within the <Directory> Block](#)

COMMANDS= command : [15.5.2. Permissions Commands](#)

commenting out services : [17.3. Primary UNIX Network Services](#)

comments in BNU UUCP : [15.5.1.3. A Sample Permissions file](#)

Common Gateway Interface : (see [CGI](#))

communications

modems : (see [modems](#))

national telecommunications : [26.2.2. Federal Jurisdiction](#)

threatening : [26.4.7. Harassment, Threatening Communication, and Defamation](#)

comparison copies

[9.2.1. Comparison Copies](#)

[9.2.1.3. rdist](#)

compress program : [6.6.1.2. Ways of improving the security of crypt](#)

Compressed SLIP (CSLIP) : [16.2. IPv4: The Internet Protocol Version 4](#)

Computer Emergency Response Committee for Unclassified Systems (CERCUS) : [F.3.4.36. TRW network area and system administrators](#)

Computer Emergency Response Team : (see [CERT](#))

Computer Incident Advisory Capability (CIAC) : [F.3.4.43. U.S. Department of Energy sites, Energy Sciences Network \(ESnet\), and DOE contractors](#)

computer networks : [1.4.3. Add-On Functionality Breeds Problems](#)

Computer Security Institute (CSI) : [F.1.3. Computer Security Institute \(CSI\)](#)

computers

assigning UUCP name : [15.5.2. Permissions Commands](#)

auxiliary ports : [12.3.1.4. Auxiliary ports on terminals](#)

backing up individual : [7.2.1. Individual Workstation](#)

contacting administrator of : [24.2.4.2. How to contact the system administrator of a computer you don't know](#)

cutting cables to : [25.1. Destructive Attacks](#)

failure of : [7.1.1.1. A taxonomy of computer failures](#)

hostnames for

[16.2.3. Hostnames](#)

[16.2.3.1. The /etc/hosts file](#)

modems : (see [modems](#))

multiple screens : [12.3.4.3. Multiple screens](#)

multiple suppliers of : [18.6. Dependence on Third Parties](#)

non-citizen access to : [26.4.1. Munitions Export](#)

operating after breakin : [24.6. Resuming Operation](#)

portable : [12.2.6.3. Portables](#)

remote command execution : [17.3.17. rexec \(TCP Port 512\)](#)

running NIS+ : [19.5.5. NIS+ Limitations](#)

screen savers : [12.3.5.2. X screen savers](#)

security

culture of : [D.1.10. Understanding the Computer Security "Culture"](#)

four steps toward : [2.4.4.7. Defend in depth](#)

physical : [12.2.6.1. Physically secure your computer](#)

references for : [D.1.7. General Computer Security](#)

resources on : [D.1.1. Other Computer References](#)

seized as evidence : [26.2.4. Hazards of Criminal Prosecution](#)

transferring files between : [15.1.1. uucp Command](#)

trusting

[27.1. Can you Trust Your Computer?](#)

[27.1.3. What the Superuser Can and Cannot Do](#)

unattended

[12.3.5. Unattended Terminals](#)

[12.3.5.2. X screen savers](#)

unplugging : [24.2.5. Getting Rid of the Intruder](#)

vacuums for : [12.2.1.3. Dust](#)

vandalism of : (see [vandalism](#))

virtual : (see [Telnet utility](#))

computing base (TCB) : [8.5.3.2. Trusted computing base](#)

conf directory : [18.2.2.1. Configuration files](#)

conf/access.conf : (see [access.conf file](#))

conf/srm.conf file : [18.3.1. The access.conf and .htaccess Files](#)

confidentiality : (see [encryption](#); [privacy](#))

configuration

errors : [9.1. Prevention](#)

files : [11.5.3. Abusing Automatic Mechanisms](#)

logging : [10.7.2.2. Informational material](#)

MCSA web server : [18.2.2.1. Configuration files](#)

UUCP version differences : [15.2. Versions of UUCP](#)

simplifying management of : [9.1.2. Read-only Filesystems](#)

connections

hijacking : [16.3. IP Security](#)

laundering : [16.1.1.1. Who is on the Internet?](#)

tracing

[24.2.4. Tracing a Connection](#)

[24.2.4.2. How to contact the system administrator of a computer you don't know](#)

unplugging : [24.2.5. Getting Rid of the Intruder](#)

connectors, network : [12.2.4.3. Network connectors](#)

consistency of software : [2.1. Planning Your Security Needs](#)

console device : [5.6. Device Files](#)

CONSOLE variable : [8.5.1. Secure Terminals](#)

constraining passwords : [8.8.2. Constraining Passwords](#)

consultants : [27.3.4. Your Consultants?](#)

context-dependent files (CDFs)

[5.9.2. Context-Dependent Files](#)

[24.4.1.7. Hidden files and directories](#)

control characters in usernames : [3.1. Usernames](#)

cookies

[17.3.21.4. Using Xauthority magic cookies](#)

[18.2.3.1. Do not trust the user's browser!](#)

COPS (Computer Oracle and Password System)

[19.5.5. NIS+ Limitations](#)

[E.4.3. COPS \(Computer Oracle and Password System\)](#)

copyright

[9.2.1. Comparison Copies](#)

[26.4.2. Copyright Infringement](#)

[26.4.2.1. Software piracy and the SPA](#)

notices of : [26.2.6. Other Tips](#)

CORBA (Common Object Request Broker Architecture) : [19.2. Sun's Remote Procedure Call \(RPC\)](#)

core files

[23.2. Tips on Avoiding Security-related Bugs](#)

[C.4. The kill Command](#)

cost-benefit analysis

[2.3. Cost-Benefit Analysis](#)

[2.3.4. Convincing Management](#)

costs of losses : [2.3.1. The Cost of Loss](#)

cp command : [7.4.1. Simple Local Copies](#)

cpio program

[7.3.2. Building an Automatic Backup System](#)

[7.4.2. Simple Archives](#)

crack program

[8.8.3. Cracking Your Own Passwords](#)

[18.3.3. Setting Up Web Users and Passwords](#)

cracking

backing up because of : [7.1.1.1. A taxonomy of computer failures](#)

passwords

[3.6.1. Bad Passwords: Open Doors](#)

[3.6.4. Passwords on Multiple Machines](#)

[8.6.1. The crypt\(\) Algorithm](#)

[8.8.3. Cracking Your Own Passwords](#)

[8.8.3.2. The dilemma of password crackers](#)

[17.3.3. TELNET \(TCP Port 23\)](#)

logging failed attempts : [10.5.3. syslog Messages](#)

responding to

[24. Discovering a Break-in](#)

[24.7. Damage Control](#)

using rexecd : [17.3.17. rexec \(TCP Port 512\)](#)

crashes, logging : [10.7.2.1. Exception and activity reports](#)

CRC checksums : (see [checksums](#))

Cred table (NIS+) : [19.5.3. NIS+ Tables](#)

criminal prosecution

[26.2. Criminal Prosecution](#)

[26.2.7. A Final Note on Criminal Actions](#)

cron file

[9.2.2.1. Simple listing](#)

[11.5.1.4. Filename attacks](#)

[11.5.3.1. crontab entries](#)

automating backups : [7.3.2. Building an Automatic Backup System](#)

cleaning up /tmp directory : [25.2.4. /tmp Problems](#)

collecting login times : [10.1.1. lastlog File](#)

symbolic links in : [10.3.7. Other Logs](#)

system clock and : [17.3.14. Network Time Protocol \(NTP\) \(UDP Port 123\)](#)

uucp scripts in : [15.6.2. Automatic Execution of Cleanup Scripts](#)

crontab file : [15.6.2. Automatic Execution of Cleanup Scripts](#)

Crypt Breaker's Workbench (CBW) : [6.6.1.1. The crypt program](#)

crypt command/algorithm

[6.4.1. Summary of Private Key Systems](#)

[6.6.1. UNIX crypt: The Original UNIX Encryption Command](#)

[6.6.1.3. Example](#)

[8.6. The UNIX Encrypted Password System](#)

[18.3.3. Setting Up Web Users and Passwords](#)

crypt function

[8.6. The UNIX Encrypted Password System](#)

[8.6.1. The crypt\(\) Algorithm](#)

[8.8.7. Algorithm and Library Changes](#)

[23.5. Tips on Using Passwords](#)

crypt16 algorithm : [8.6.4. Crypt16\(\) and Other Algorithms](#)

cryptography

[6. Cryptography](#)

[6.7.2. Cryptography and Export Controls](#)

[14.4.4.2. Protection against eavesdropping](#)

checklist for : [A.1.1.5. Chapter 6: Cryptography](#)

checksums : [6.5.5.1. Checksums](#)

digital signatures : (see [digital signatures](#))

export laws concerning : [6.7.2. Cryptography and Export Controls](#)

Message Authentication Codes (MACs) : [6.5.5.2. Message authentication codes](#)

message digests : (see [message digests](#))

PGP : (see [PGP](#))

private-key

[6.4. Common Cryptographic Algorithms](#)

[6.4.1. Summary of Private Key Systems](#)

public-key

[6.4. Common Cryptographic Algorithms](#)

[6.4.2. Summary of Public Key Systems](#)

[6.4.6. RSA and Public Key Cryptography](#)

[6.4.6.3. Strength of RSA](#)

[6.5.3. Digital Signatures](#)

[18.3. Controlling Access to Files on Your Server](#)

[18.6. Dependence on Third Parties](#)

references on : [D.1.5. Cryptography Books](#)

and U.S. patents : [6.7.1. Cryptography and the U.S. Patent System](#)

csh (C shell)

[5.5.2. Problems with SUID](#)

[11.5.1. Shell Features](#)

[23.2. Tips on Avoiding Security-related Bugs](#)

[C.5.3. Running the User's Shell](#)

(see also [shells](#))

autologout variable : [12.3.5.1. Built-in shell autologout](#)

history file : [10.4.1. Shell History](#)

uucp command : [15.1.1.1. uucp with the C shell](#)

.cshrc file

[11.5.2.2. .cshrc, .kshrc](#)

[12.3.5.1. Built-in shell autologout](#)

[24.4.1.6. Changes to startup files](#)

CSI (Computer Security Institute) : [F.1.3. Computer Security Institute \(CSI\)](#)

CSLIP (Compressed SLIP) : [16.2. IPv4: The Internet Protocol Version 4](#)

ctime

[5.1.2. Inodes](#)

[5.1.5. File Times](#)

[5.2.1. chmod: Changing a File's Permissions](#)

[7.4.7. inode Modification Times](#)

[9.2.3. Checksums and Signatures](#)

cu command

[14.5. Modems and UNIX](#)

[14.5.3.1. Originate testing](#)

[14.5.3.3. Privilege testing](#)

-l option : [14.5.3.1. Originate testing](#)

culture, computer security : [D.1.10. Understanding the Computer Security "Culture"](#)

current directory : [5.1.3. Current Directory and Paths](#)

Customer Warning System (CWS) : [F.3.4.34. Sun Microsystems customers](#)

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

[Copyright](#) © 1999 [O'Reilly & Associates, Inc.](#) All Rights Reserved.

[[Library Home](#) | [DNS & BIND](#) | [TCP/IP](#) | [sendmail](#) | [sendmail Reference](#) | [Firewalls](#) | [Practical Security](#)]



Practical UNIX & Internet Security

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

Index: D

DAC (Discretionary Access Controls) : [4.1.3. Groups and Group Identifiers \(GIDs\)](#)

daemon (user) : [4.1. Users and Groups](#)

damage, liability for : [26.4.6. Liability for Damage](#)

DARPA : (see [ARPA](#))

DAT (Digital Audio Tape) : [7.1.4. Guarding Against Media Failure](#)

data

 assigning owners to : [2.4.4.1. Assign an owner](#)

 availability of : [2.1. Planning Your Security Needs](#)

 communication equipment (DCE) : [14.3. The RS-232 Serial Protocol](#)

 confidential

[2.1. Planning Your Security Needs](#)

[2.5.2. Confidential Information](#)

 disclosure of : [11.2. Damage](#)

 giving away with NIS : [19.4.5. Unintended Disclosure of Site Information with NIS](#)

 identifying assets : [2.2.1.1. Identifying assets](#)

 integrity of : (see [integrity, data](#))

 spoofing : [16.3. IP Security](#)

 terminal equipment (DTE) : [14.3. The RS-232 Serial Protocol](#)

Data Carrier Detect (DCD) : [14.3. The RS-232 Serial Protocol](#)

Data Defense Network (DDN) : [F.3.4.20. MILNET](#)

Data Encryption Standard : (see [DES](#))

Data Set Ready (DSR) : [14.3. The RS-232 Serial Protocol](#)

Data Terminal Ready (DTR) : [14.3. The RS-232 Serial Protocol](#)

database files : [1.2. What Is an Operating System?](#)

databases : (see [network databases](#))

date command

[8.1.3. Accounts That Run a Single Command](#)

[24.5.1. Never Trust Anything Except Hardcopy](#)

day-zero backups : [7.1.3. Types of Backups](#)

dbx debugger : [C.4. The kill Command](#)

DCE (data communication equipment) : [14.3. The RS-232 Serial Protocol](#)

DCE (Distributed Computing Environment)

[3.2.2. The /etc/passwd File and Network Databases](#)

[8.7.3. Code Books](#)

[16.2.6.2. Other naming services](#)

[19.2. Sun's Remote Procedure Call \(RPC\)](#)

[19.7.1. DCE](#)

dd command

[6.6.1.2. Ways of improving the security of crypt](#)

[7.4.1. Simple Local Copies](#)

DDN (Data Defense Network) : [F.3.4.20. MILNET](#)

deadlock : [23.2. Tips on Avoiding Security-related Bugs](#)

debug command : [17.3.4.2. Using sendmail to receive email](#)

debugfs command : [25.2.2.8. Tree-structure attacks](#)

DEC (Digital Equipment Corporation) : [F.3.4.9. Digital Equipment Corporation and customers](#)

DECnet protocol : [16.4.3. DECnet](#)

decode aliases : [17.3.4.2. Using sendmail to receive email](#)

decryption : (see [encryption](#))

defamation : [26.4.7. Harassment, Threatening Communication, and Defamation](#)

default

accounts : [8.1.2. Default Accounts](#)

deny : [21.1.1. Default Permit vs. Default Deny](#)

domain : [16.2.3. Hostnames](#)

permit : [21.1.1. Default Permit vs. Default Deny](#)

defense in depth : (see [multilevel security](#))

DELETE key : [3.4. Changing Your Password](#)

deleting

destructive attack via : [25.1. Destructive Attacks](#)

files : [5.4. Using Directory Permissions](#)

demo accounts : [8.1.2. Default Accounts](#)

denial-of-service attacks

[1.5. Role of This Book](#)

[25. Denial of Service Attacks and Solutions](#)

[25.3.4. Clogging](#)

accidental : [25.2.5. Soft Process Limits: Preventing Accidental Denial of Service](#)

automatic logout : [3.3. Entering Your Password](#)

checklist for : [A.1.1.24. Chapter 25: Denial of Service Attacks and Solutions](#)

inodes : [25.2.2.3. Inode problems](#)

internal inetd services : [17.1.3. The /etc/inetd Program](#)
on networks
 [25.3. Network Denial of Service Attacks](#)
 [25.3.4. Clogging](#)
via syslog : [10.5.1. The syslog.conf Configuration File](#)
X Window System : [17.3.21.5. Denial of service attacks under X](#)
departure of employees : [13.2.6. Departure](#)
depository directories, FTP : [17.3.2.6. Setting up anonymous FTP with the
standard UNIX FTP server](#)
DES (Data Encryption Standard)
 [6.4.1. Summary of Private Key Systems](#)
 [6.4.4. DES](#)
 [6.4.5.2. Triple DES](#)
 [8.6.1. The crypt\(\) Algorithm](#)
authentication (NIS+) : [19.5.4. Using NIS+](#)
improving security of
 [6.4.5. Improving the Security of DES](#)
 [6.4.5.2. Triple DES](#)
des program
 [6.4.4. DES](#)
 [6.6.2. des: The Data Encryption Standard](#)
 [7.4.4. Encrypting Your Backups](#)
destroying media : [12.3.2.3. Sanitize your media before disposal](#)
destructive attacks : [25.1. Destructive Attacks](#)
detached signatures : [6.6.3.6. PGP detached signatures](#)
detectors
 cable tampering : [12.3.1.1. Wiretapping](#)
 carbon-monoxide : [12.2.1.2. Smoke](#)
 humidity : [12.2.1.11. Humidity](#)
 logging alarm systems : [10.7.1.1. Exception and activity reports](#)
 smoke : [12.2.1.2. Smoke](#)
 temperature alarms : [12.2.1.6. Temperature extremes](#)
 water sensors : [12.2.1.12. Water](#)
Deutsches Forschungsnetz : [F.3.4.14. Germany: DFN-WiNet Internet sites](#)
/dev directory : [14.5.1. Hooking Up a Modem to Your Computer](#)
 /dev/audio device : [23.8. Picking a Random Seed](#)
 /dev/console device : [5.6. Device Files](#)
 /dev/kmem device
 [5.6. Device Files](#)

[11.1.2. Back Doors and Trap Doors](#)

/dev/null device : [5.6. Device Files](#)

/dev/random device : [23.7.4. Other random number generators](#)

/dev/swap device : [5.5.1. SUID, SGID, and Sticky Bits](#)

/dev/urandom device : [23.7.4. Other random number generators](#)

device files : [5.6. Device Files](#)

devices

managing with SNMP : [17.3.15. Simple Network Management Protocol \(SNMP\) \(UDP Ports 161 and 162\)](#)

modem control : [14.5.2. Setting Up the UNIX Device](#)

Devices file : [14.5.1. Hooking Up a Modem to Your Computer](#)

df -i command : [25.2.2.3. Inode problems](#)

dictionary attack : [8.6.1. The crypt\(\) Algorithm](#)

Diffie-Hellman key exchange system

[6.4.2. Summary of Public Key Systems](#)

[18.6. Dependence on Third Parties](#)

[19.3. Secure RPC \(AUTH DES\)](#)

breaking key : [19.3.4. Limitations of Secure RPC](#)

exponential key exchange : [19.3.1. Secure RPC Authentication](#)

Digital Audio Tape (DAT) : [7.1.4. Guarding Against Media Failure](#)

digital computers : [6.1.2. Cryptography and Digital Computers](#)

Digital Equipment Corporation (DEC) : [F.3.4.9. Digital Equipment Corporation and customers](#)

Digital Signature Algorithm : (see [DSA](#))

digital signatures

[6.4. Common Cryptographic Algorithms](#)

[6.5. Message Digests and Digital Signatures](#)

[6.5.5.2. Message authentication codes](#)

[9.2.3. Checksums and Signatures](#)

checksums : [6.5.5.1. Checksums](#)

detached signatures : [6.6.3.6. PGP detached signatures](#)

with PGP : [6.6.3.4. Adding a digital signature to an announcement](#)

Digital UNIX

[1.3. History of UNIX](#)

(see also [Ultrix](#))

directories

[5.1.1. Directories](#)

[5.1.3. Current Directory and Paths](#)

ancestor : [9.2.2.2. Ancestor directories](#)

backing up by : [7.1.3. Types of Backups](#)
CDFs (context-dependent files) : [24.4.1.7. Hidden files and directories](#)
checklist for : [A.1.1.4. Chapter 5: The UNIX Filesystem](#)
dot, dot-dot, and / : [5.1.1. Directories](#)
FTP depositories : [17.3.2.6. Setting up anonymous FTP with the standard UNIX FTP server](#)
immutable : [9.1.1. Immutable and Append-Only Files](#)
listing automatically (Web) : [18.2.2.2. Additional configuration issues](#)
mounted : [5.5.5. Turning Off SUID and SGID in Mounted Filesystems](#)
mounting secure : [19.3.2.5. Mounting a secure filesystem](#)
nested : [25.2.2.8. Tree-structure attacks](#)
NFS : (see [NFS](#))
permissions : [5.4. Using Directory Permissions](#)
read-only : [9.1.2. Read-only Filesystems](#)
restricted
 [8.1.5. Restricted Filesystem](#)
 [8.1.5.2. Checking new software](#)
root : (see [root directory](#))
SGI and sticky bits on : [5.5.6. SGID and Sticky Bits on Directories](#)
Web server structure of
 [18.2.2. Understand Your Server's Directory Structure](#)
 [18.2.2.2. Additional configuration issues](#)
world-writable : [11.6.1.1. World-writable user files and directories](#)
<Directory> blocks
 [18.3.1. The access.conf and .htaccess Files](#)
 [18.3.2. Commands Within the <Directory> Block](#)
 [18.3.2.1. Examples](#)
disaster recovery : [12.2.6.4. Minimizing downtime](#)
disk attacks
 [25.2.2. Disk Attacks](#)
 [25.2.2.8. Tree-structure attacks](#)
disk quotas : [25.2.2.5. Using quotas](#)
diskettes : (see [backups](#); [media](#))
dismissed employees : [13.2.6. Departure](#)
disposing of materials : [12.3.3. Other Media](#)
Distributed Computing Environment : (see [DCE](#))
DNS (Domain Name System)
 [16.2.6. Name Service](#)
 [16.2.6.2. Other naming services](#)

[17.3.6. Domain Name System \(DNS\) \(TCP and UDP Port 53\)](#)

[17.3.6.2. DNS nameserver attacks](#)

nameserver attacks : [17.3.6.2. DNS nameserver attacks](#)

rogue servers : [16.3.2. Security and Nameservice](#)

security and : [16.3.2. Security and Nameservice](#)

zone transfers

[17.3.6. Domain Name System \(DNS\) \(TCP and UDP Port 53\)](#)

[17.3.6.1. DNS zone transfers](#)

documentation

[2.5. The Problem with Security Through Obscurity](#)

[23.2. Tips on Avoiding Security-related Bugs](#)

domain name : [16.2.3. Hostnames](#)

Domain Name System : (see [DNS](#))

domainname command : [19.4.3. NIS Domains](#)

domains : [19.4.3. NIS Domains](#)

dormant accounts

[8.4. Managing Dormant Accounts](#)

[8.4.3. Finding Dormant Accounts](#)

dot (.) directory : [5.1.1. Directories](#)

dot-dot (..) directory : [5.1.1. Directories](#)

Double DES : [6.4.5. Improving the Security of DES](#)

double reverse lookup : [16.3.2. Security and Nameservice](#)

DOW USA : [F.3.4.10. DOW USA](#)

downloading files : [12.3.4. Protecting Local Storage](#)

logging

[10.3.3. xferlog Log File](#)

[10.3.5. access_log Log File](#)

downtime : [12.2.6.4. Minimizing downtime](#)

due to criminal investigations : [26.2.4. Hazards of Criminal Prosecution](#)

logging : [10.7.2.1. Exception and activity reports](#)

drand48 function : [23.7.3. drand48 \(\), lrand48 \(\), and mrand48 \(\)](#)

drills, security : [24.1.3. Rule #3: PLAN AHEAD](#)

drink : [12.2.2.1. Food and drink](#)

DSA (Digital Signature Algorithm)

[6.4.2. Summary of Public Key Systems](#)

[6.5.3. Digital Signatures](#)

DTE (data terminal equipment) : [14.3. The RS-232 Serial Protocol](#)

du command : [25.2.2.1. Disk-full attacks](#)

dual universes : [5.9.1. Dual Universes](#)

ducts, air : [12.2.3.2. Entrance through air ducts](#)

dump/restore program

[7.1.3. Types of Backups](#)

[7.4.3. Specialized Backup Programs](#)

[7.4.4. Encrypting Your Backups](#)

dumpster diving : [12.3.3. Other Media](#)

duress code : [8.7.2. Token Cards](#)

dust : [12.2.1.3. Dust](#)

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

[Copyright](#) © 1999 [O'Reilly & Associates, Inc.](#) All Rights Reserved.

[[Library Home](#) | [DNS & BIND](#) | [TCP/IP](#) | [sendmail](#) | [sendmail Reference](#) | [Firewalls](#) | [Practical Security](#)]



Practical UNIX & Internet Security

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

Index: E

earthquakes : [12.2.1.4. Earthquake](#)

eavesdropping

[12.3.1. Eavesdropping](#)

[12.3.1.5. Fiber optic cable](#)

[12.4.1.2. Potential for eavesdropping and data theft](#)

[14.4.4. Protecting Against Eavesdropping](#)

[14.4.4.2. Protection against eavesdropping](#)

[16.3.1. Link-level Security](#)

IP packets

[16.3.1. Link-level Security](#)

[17.3.3. TELNET \(TCP Port 23\)](#)

through log files : [18.4.2. Eavesdropping Through Log Files](#)

on the Web

[18.4. Avoiding the Risks of Eavesdropping](#)

[18.4.2. Eavesdropping Through Log Files](#)

X clients : [17.3.21.2. X security](#)

ECB (electronic code book)

[6.4.4.2. DES modes](#)

[6.6.2. des: The Data Encryption Standard](#)

echo command : [23.5. Tips on Using Passwords](#)

ECPA (Electronic Communications Privacy Act) : [26.2.3. Federal Computer Crime Laws](#)

editing wtmp file : [10.1.3.1. Pruning the wtmp file](#)

editors : [11.5.2.7. Other initializations](#)

buffers for : [11.1.4. Trojan Horses](#)

Emacs : [11.5.2.3. GNU .emacs](#)

ex

[5.5.3.2. Another SUID example: IFS and the /usr/lib/preserve hole](#)

[11.5.2.4. .exrc](#)

[11.5.2.7. Other initializations](#)

startup file attacks : [11.5.2.4. .exrc](#)

vi

[5.5.3.2. Another SUID example: IFS and the /usr/lib/preserve hole](#)

[11.5.2.4. .exrc](#)

[11.5.2.7. Other initializations](#)
edquota command : [25.2.2.5. Using quotas](#)
EDS : [F.3.4.11. EDS and EDS customers worldwide](#)
education : (see [security, user awareness of](#))
effective UIDs/GIDs
 [4.3.1. Real and Effective UIDs](#)
 [5.5. SUID](#)
 [10.1.2.1. su command and /etc/utmp and /var/adm/wtmp files](#)
 [C.1.3.2. Process real and effective UID](#)
8mm video tape : [7.1.4. Guarding Against Media Failure](#)
electrical fires
 [12.2.1.2. Smoke](#)
 (see also [fires](#); [smoke and smoking](#))
electrical noise : [12.2.1.8. Electrical noise](#)
electronic
 breakins : (see [breakins](#); [cracking](#))
 code book (ECB)
 [6.4.4.2. DES modes](#)
 [6.6.2. des: The Data Encryption Standard](#)
 mail : (see [mail](#))
Electronic Communications Privacy Act (ECPA) : [26.2.3. Federal Computer Crime Laws](#)
ElGamal algorithm
 [6.4.2. Summary of Public Key Systems](#)
 [6.5.3. Digital Signatures](#)
elm (mail system) : [11.5.2.5. .forward, .procmailrc](#)
emacs editor : [11.5.2.7. Other initializations](#)
.emacs file : [11.5.2.3. GNU .emacs](#)
email : (see [mail](#))
embedded commands : (see [commands](#))
embezzlers : [11.3. Authors](#)
emergency response organizations : (see [response teams](#))
employees
 [11.3. Authors](#)
 [13. Personnel Security](#)
 [13.3. Outsiders](#)
 departure of : [13.2.6. Departure](#)
 phonebook of : [12.3.3. Other Media](#)
 security checklist for : [A.1.1.12. Chapter 13: Personnel Security](#)

targeted in legal investigation : [26.2.5. If You or One of Your Employees Is a Target of an Investigation...](#)

trusting : [27.3.1. Your Employees?](#)

written authorization for : [26.2.6. Other Tips](#)

encryption

[6.2. What Is Encryption?](#)

[6.2.2. The Elements of Encryption](#)

[12.2.6.2. Encryption](#)

(see also [cryptography](#))

algorithms : [2.5. The Problem with Security Through Obscurity](#)

crypt

[6.6.1. UNIX crypt: The Original UNIX Encryption Command](#)

[6.6.1.3. Example](#)

Digital Signature Algorithm

[6.4.2. Summary of Public Key Systems](#)

[6.5.3. Digital Signatures](#)

ElGamal : [6.4.2. Summary of Public Key Systems](#)

IDEA : [6.4.1. Summary of Private Key Systems](#)

RC2, RC4, and RC5

[6.4.1. Summary of Private Key Systems](#)

[6.4.8. Proprietary Encryption Systems](#)

ROT13 : [6.4.3. ROT13: Great for Encoding Offensive Jokes](#)

RSA

[6.4.2. Summary of Public Key Systems](#)

[6.4.6. RSA and Public Key Cryptography](#)

[6.4.6.3. Strength of RSA](#)

application-level : [16.3.1. Link-level Security](#)

of backups

[7.1.6.3. Data security for backups](#)

[7.4.4. Encrypting Your Backups](#)

[12.3.2.4. Backup encryption](#)

checklist for : [A.1.1.5. Chapter 6: Cryptography](#)

Data Encryption Standard (DES)

[6.4.1. Summary of Private Key Systems](#)

[6.4.4. DES](#)

[6.4.5.2. Triple DES](#)

[6.6.2. des: The Data Encryption Standard](#)

DCE and : [3.2.2. The /etc/passwd File and Network Databases](#)

Diffie-Hellman : (see [Diffie-Hellman key exchange system](#))

end-to-end : [16.3.1. Link-level Security](#)
Enigma system
 [6.3. The Enigma Encryption System](#)
 [6.6.1.1. The crypt program](#)
 (see also [crypt command/algorithm](#))
escrowing keys
 [6.1.3. Modern Controversy](#)
 [7.1.6.3. Data security for backups](#)
exporting software : [26.4.1. Munitions Export](#)
of hypertext links : [18.4.1. Eavesdropping Over the Wire](#)
laws about
 [6.7. Encryption and U.S. Law](#)
 [6.7.2. Cryptography and Export Controls](#)
link-level : [16.3.1. Link-level Security](#)
of modems : [14.6. Additional Security for Modems](#)
Netscape Navigator system : [18.4.1. Eavesdropping Over the Wire](#)
with network services : [17.4. Security Implications of Network Services](#)
one-time pad mechanism : [6.4.7. An Unbreakable Encryption Algorithm](#)
of passwords
 [8.6. The UNIX Encrypted Password System](#)
 [8.6.4. Crypt16\(\) and Other Algorithms](#)
 [23.5. Tips on Using Passwords](#)
PGP : (see [PGP](#))
programs for UNIX
 [6.6. Encryption Programs Available for UNIX](#)
 [6.6.3.6. PGP detached signatures](#)
proprietary algorithms : [6.4.8. Proprietary Encryption Systems](#)
RC4 and RC5 algorithms : [6.4.1. Summary of Private Key Systems](#)
references on : [D.1.5. Cryptography Books](#)
Skipjack algorithm : [6.4.1. Summary of Private Key Systems](#)
superencryption : [6.4.5. Improving the Security of DES](#)
and superusers : [6.2.4. Why Use Encryption with UNIX?](#)
of Web information : [18.4.1. Eavesdropping Over the Wire](#)
end-to-end encryption : [16.3.1. Link-level Security](#)
Energy Sciences Network (ESnet) : [F.3.4.43. U.S. Department of Energy sites, Energy Sciences Network \(ESnet\), and DOE contractors](#)
Enigma encryption system
 [6.3. The Enigma Encryption System](#)
 [6.6.1.1. The crypt program](#)

Enterprise Networks : [16.1. Networking](#)

environment variables

[11.5.2.7. Other initializations](#)

[23.2. Tips on Avoiding Security-related Bugs](#)

environment, physical

[12.2.1. The Environment](#)

[12.2.1.13. Environmental monitoring](#)

erasing disks : [12.3.2.3. Sanitize your media before disposal](#)

erotica, laws governing : [26.4.5. Pornography and Indecent Material](#)

errno variable : [23.2. Tips on Avoiding Security-related Bugs](#)

errors : [7.1.1.1. A taxonomy of computer failures](#)

in ACLs : [5.2.5.1. AIX Access Control Lists](#)

configuration : [9.1. Prevention](#)

human : [7.1.4. Guarding Against Media Failure](#)

errors

[Preface](#)

(see also [auditing, system activity](#))

escape sequences, modems and : [14.5.3.1. Originate testing](#)

escrowing encryption keys

[6.1.3. Modern Controversy](#)

[7.1.6.3. Data security for backups](#)

ESnet (Energy Sciences Network) : [E.3.4.43. U.S. Department of Energy sites,](#)

[Energy Sciences Network \(ESnet\), and DOE contractors](#)

espionage : [11.3. Authors](#)

/etc directory

[11.1.2. Back Doors and Trap Doors](#)

[11.5.3.5. System initialization files](#)

backups of : [7.1.3. Types of Backups](#)

/etc/aliases file : [11.5.3.3. /usr/lib/aliases, /etc/aliases, /etc/sendmail/aliases, aliases.dir, or aliases.pag](#)

/etc/default/login file : [8.5.1. Secure Terminals](#)

/etc/exports file

[11.6.1.2. Writable system files and directories](#)

[19.3.2.4. Using Secure NFS](#)

making changes to : [20.2.1.2. /usr/etc/exports](#)

/etc/fstab file : [17.3.21.1. /etc/fstab and /etc/logindevperm](#)

/etc/fingerd program : (see [finger command](#))

/etc/fsck program : [24.4.1.7. Hidden files and directories](#)

/etc/fstab file

[11.1.2. Back Doors and Trap Doors](#)

[19.3.2.5. Mounting a secure filesystem](#)

/etc/ftpd : (see [ftpd server](#))

/etc/ftpusers file : [17.3.2.5. Restricting FTP with the standard UNIX FTP server](#)

/etc/group file

[1.2. What Is an Operating System?](#)

[4.1.3.1. The /etc/group file](#)

[4.2.3. Impact of the /etc/passwd and /etc/group Files on Security](#)

[8.1.6. Group Accounts](#)

/etc/halt command : [24.2.6. Anatomy of a Break-in](#)

/etc/hosts file : [16.2.3.1. The /etc/hosts file](#)

/etc/hosts.equiv : (see [hosts.equiv file](#))

/etc/hosts.lpd file : [17.3.18.6. /etc/hosts.lpd file](#)

/etc/inetd : (see [inetd daemon](#))

/etc/inetd.conf file : [17.3. Primary UNIX Network Services](#)

/etc/init program : [C.5.1. Process #1: /etc/init](#)

/etc/inittab : (see [inittab program](#))

/etc/keystore file : [19.3.1.1. Proving your identity](#)

/etc/logindevperm file : [17.3.21.1. /etc/fstab and /etc/logindevperm](#)

/etc/motd file : [26.2.6. Other Tips](#)

/etc/named.boot file

[17.3.6.1. DNS zone transfers](#)

[17.3.6.2. DNS nameserver attacks](#)

/etc/passwd file

[1.2. What Is an Operating System?](#)

[3.2.1. The /etc/passwd File](#)

[3.2.2. The /etc/passwd File and Network Databases](#)

[4.2.3. Impact of the /etc/passwd and /etc/group Files on Security](#)

[8.1.1. Accounts Without Passwords](#)

[8.6. The UNIX Encrypted Password System](#)

[C.5.1. Process #1: /etc/init](#)

+ in : (see [NIS](#))

accounts without passwords : [8.1.1. Accounts Without Passwords](#)

backing up : [7.1.2. What Should You Back Up?](#)

new accounts : [24.4.1. New Accounts](#)

NFS : [20.2.1.1. /etc/exports](#)

uucp user and : [15.1.4. How the UUCP Commands Work](#)

/etc/profile file

[11.5.2.1. .login, .profile, /etc/profile](#)
[24.4.1.6. Changes to startup files](#)
/etc/publickey file : [19.3.2.1. Creating passwords for users](#)
/etc/rc directory
[11.5.3.5. System initialization files](#)
[17.1.2. Starting the Servers](#)
[C.5.1. Process #1: /etc/init](#)
commenting out services : [17.3. Primary UNIX Network Services](#)
/etc/remote file
[10.3.1. aculog File](#)
[14.5.1. Hooking Up a Modem to Your Computer](#)
/etc/renice : (see [renice command](#))
/etc/secure/passwd file : [8.1.1. Accounts Without Passwords](#)
/etc/security/passwd.adjunct file : [8.8.5. Shadow Password Files](#)
/etc/sendmail/aliases file : [11.5.3.3. /usr/lib/aliases, /etc/aliases, /etc/sendmail/aliases, aliases.dir, or aliases.pag](#)
/etc/services file : [17.1.1. The /etc/services File](#)
/etc/services file : [17.1.1. The /etc/services File](#)
/etc/shadow file
[8.1.1. Accounts Without Passwords](#)
[8.8.5. Shadow Password Files](#)
/etc/shells file : [8.4.2. Changing the Account's Login Shell](#)
/etc/syslogd : (see [syslog facility](#))
/etc/tty file, backing up : [7.1.2. What Should You Back Up?](#)
/etc/ttys file
[8.5.1. Secure Terminals](#)
[14.5.1. Hooking Up a Modem to Your Computer](#)
/etc/ttytab file : [C.5.1. Process #1: /etc/init](#)
/etc/utmp file
[10.1.2. utmp and wtmp Files](#)
[10.1.2.1. su command and /etc/utmp and /var/adm/wtmp files](#)
[24.2.1. Catching One in the Act](#)
[24.2.4. Tracing a Connection](#)
/etc/uucp directory : [15.4.2.1. Some bad examples](#)
/etc/yp/makedbm program : [19.4.4.1. Setting up netgroups](#)
in restricted filesystems : [8.1.5. Restricted Filesystem](#)
Ethernet : [16.1. Networking](#)
addresses for random seeds : [23.8. Picking a Random Seed](#)
cables : (see [cables, network](#))

eavesdropping by : [12.3.1.2. Eavesdropping by Ethernet and 10Base-T Ethers table \(NIS+\)](#) : [19.5.3. NIS+ Tables](#)

Euler Totient Function : [6.4.6.1. How RSA works](#)

eval function

[18.2.3.2. Testing is not enough!](#)

[18.2.3.3. Sending mail](#)

evidence, equipment seized as : [26.2.4. Hazards of Criminal Prosecution](#)

ex editor

[5.5.3.2. Another SUID example: IFS and the /usr/lib/preserve hole](#)

[11.5.2.4. .exrc](#)

[11.5.2.7. Other initializations](#)

exceptions : [C.2. Creating Processes](#)

exclamation mark (!) and mail command : [15.1.3. mail Command](#)

exclusive OR (XOR) : [6.4.7. An Unbreakable Encryption Algorithm](#)

exec (in Swatch program) : [10.6.2. The Swatch Configuration File](#)

exec system call

[5.1.7. File Permissions in Detail](#)

[18.2.3.3. Sending mail](#)

[23.2. Tips on Avoiding Security-related Bugs](#)

[25.2.1.1. Too many processes](#)

ExecCGI option : [18.3.2. Commands Within the <Directory> Block](#)

execl system call : [23.4. Tips on Writing SUID/SGID Programs](#)

execvp system call : [23.4. Tips on Writing SUID/SGID Programs](#)

execute permission

[5.1.7. File Permissions in Detail](#)

[5.4. Using Directory Permissions](#)

execv system call : [23.4. Tips on Writing SUID/SGID Programs](#)

execve system call : [23.4. Tips on Writing SUID/SGID Programs](#)

execvp system call : [23.4. Tips on Writing SUID/SGID Programs](#)

expiring

accounts : [8.4.3. Finding Dormant Accounts](#)

FTP depositories : [17.3.2.6. Setting up anonymous FTP with the standard UNIX FTP server](#)

passwords : [8.8.6. Password Aging and Expiration](#)

explosions : [12.2.1.5. Explosion](#)

export laws : [26.4.1. Munitions Export](#)

cryptography

[6.4.4.1. Use and export of DES](#)

[6.7.2. Cryptography and Export Controls](#)

exportfs command : [20.2.1.2. /usr/etc/exportfs](#)

exports file

[11.6.1.2. Writable system files and directories](#)

[19.3.2.4. Using Secure NFS](#)

[20.2.1.1. /etc/exports](#)

[20.2.1.2. /usr/etc/exportfs](#)

.exrc file : [11.5.2.4. .exrc](#)

ext2 filesystem (Linux) : [25.2.2.6. Reserved space](#)

external data representation (XDR) : [19.2. Sun's Remote Procedure Call \(RPC\)](#)

extinguishers, fire : (see [fires](#))

extortion : [11.3. Authors](#)

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

[Copyright](#) © 1999 [O'Reilly & Associates, Inc.](#) All Rights Reserved.

[[Library Home](#) | [DNS & BIND](#) | [TCP/IP](#) | [sendmail](#) | [sendmail Reference](#) | [Firewalls](#) | [Practical Security](#)]



Practical UNIX & Internet Security

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

Index: F

factoring numbers

[6.4.6. RSA and Public Key Cryptography](#)

[6.4.6.3. Strength of RSA](#)

(see also [RSA algorithm](#))

failed login attempts : (see [logging in](#))

failures, computer

[7.1.1.1. A taxonomy of computer failures](#)

[23.2. Tips on Avoiding Security-related Bugs](#)

(see also [bugs](#))

fair use laws : [26.4.2. Copyright Infringement](#)

Fast Filesystem (FFS) : [25.2.2.6. Reserved space](#)

FBI (Federal Bureau of Investigation)

[26.2.2. Federal Jurisdiction](#)

[F.3.2. Federal Bureau of Investigation \(FBI\)](#)

fbtab file : [17.3.21.1. /etc/fstab and /etc/logindevperm](#)

Federal Information Processing Standard (FIPS) : [6.4.2. Summary of Public Key Systems](#)

federal law enforcement

[26.2.2. Federal Jurisdiction](#)

[26.2.3. Federal Computer Crime Laws](#)

FFS (Fast File System) : [25.2.2.6. Reserved space](#)

fgets function : [23.1.1. The Lesson of the Internet Worm](#)

fiber optic cables : (see [cables, network](#))

File Handles : [20.1.2. File Handles](#)

File Transfer Protocol : (see [FTP](#))

filenames, attacks via : [11.5.1.4. Filename attacks](#)

files : [5.1. Files](#)

automatic directory listings : [18.2.2.2. Additional configuration issues](#)

backing up

[7. Backups](#)

[7.4.7. inode Modification Times](#)

automatic system for

[7.3.2. Building an Automatic Backup System](#)

[18.2.3.5. Beware stray CGI scripts](#)

critical files
 [7.3. Backing Up System Files](#)
 [7.3.2. Building an Automatic Backup System](#)
prioritizing : [7.3.1. What Files to Back Up?](#)
changing owner of : [5.7. chown: Changing a File's Owner](#)
context-dependent (CDFs)
 [5.9.2. Context-Dependent Files](#)
 [24.4.1.7. Hidden files and directories](#)
core : [C.4. The kill Command](#)
descriptors : [23.2. Tips on Avoiding Security-related Bugs](#)
detecting changes to
 [9.2. Detecting Change](#)
 [9.3. A Final Note](#)
device : [5.6. Device Files](#)
downloading, logs of
 [10.3.3. xferlog Log File](#)
 [10.3.5. access_log Log File](#)
finding all SUID/SGID
 [5.5.4. Finding All of the SUID and SGID Files](#)
 [5.5.4.1. The ncheck command](#)
format, monitoring : [8.2. Monitoring File Format](#)
group-writable : [11.6.1.2. Writable system files and directories](#)
hidden : [24.4.1.7. Hidden files and directories](#)
hidden space : [25.2.2.7. Hidden space](#)
history : [10.4.1. Shell History](#)
immutable : [9.1.1. Immutable and Append-Only Files](#)
integrity of : (see [integrity](#))
intruder's changes to : [24.4.1.1. Changes in file contents](#)
locating largest : [25.2.2.1. Disk-full attacks](#)
locking : [23.2. Tips on Avoiding Security-related Bugs](#)
log : (see [log files](#))
mail sent directly to : [15.7. Early Security Problems with UUCP](#)
modification times of
 [5.1.2. Inodes](#)
 [5.1.5. File Times](#)
 [7.4.7. inode Modification Times](#)
 [9.2.2. Checklists and Metadata](#)
network configuration : [10.4.3. Network Setup](#)
permissions to : (see [permissions](#))

remote access to

[15.4.1. USERFILE: Providing Remote File Access](#)

[15.4.2.1. Some bad examples](#)

SGID bit on : [5.5.7. SGID Bit on Files \(System V UNIX Only\): Mandatory Record Locking](#)

startup

[11.5.2. Start-up File Attacks](#)

[11.5.2.7. Other initializations](#)

system database : [1.2. What Is an Operating System?](#)

transferring between systems : [15.1.1. uucp Command](#)

types of : [5.1.6. Understanding File Permissions](#)

unowned : [24.4.1.8. Unowned files](#)

on Web servers : (see [Web servers](#))

world-writable : [11.6.1.1. World-writable user files and directories](#)

zero-filled bytes in : [7.4. Software for Backups](#)

filesystems : (see [directories](#))

filter files (mail) : [11.5.2.5. .forward, .procmailrc](#)

filters, air : [12.2.1.3. Dust](#)

find command

[5.5.4. Finding All of the SUID and SGID Files](#)

[11.5.1.4. Filename attacks](#)

-H option : [5.9.2. Context-Dependent Files](#)

-ls option : [9.2.2.1. Simple listing](#)

-size option : [25.2.2.1. Disk-full attacks](#)

-H option : [24.4.1.7. Hidden files and directories](#)

-print option : [5.5.4. Finding All of the SUID and SGID Files](#)

type -f option : [5.5.4. Finding All of the SUID and SGID Files](#)

-xdev option : [5.5.4. Finding All of the SUID and SGID Files](#)

finger command

[8.1.3. Accounts That Run a Single Command](#)

[10.1.1. lastlog File](#)

[10.1.2. utmp and wtmp Files](#)

[15.3.1. Assigning Additional UUCP Logins](#)

[15.4.3. L.cmds: Providing Remote Command Execution](#)

[17.3.4.3. Improving the security of Berkeley sendmail V8](#)

[17.3.8. finger \(TCP Port 79\)](#)

[17.3.8.3. Replacing finger](#)

[21.4.4.1. Creating an ftpout account to allow FTP without proxies.](#)

[23.1.1. The Lesson of the Internet Worm](#)

[24.2.1. Catching One in the Act](#)

[24.2.4.2. How to contact the system administrator of a computer you don't know](#)

(see also [Internet, Worm program](#))

disabling : [17.3.8.2. Disabling finger](#)

FIPS (Federal Information Processing Standard) : [6.4.2. Summary of Public Key Systems](#)

fired employees : [13.2.6. Departure](#)

fires

[12.2.1.1. Fire](#)

[12.2.1.2. Smoke](#)

[12.4.1.1. Fire hazards](#)

extinguishers and radio transmitters : [12.2.1.8. Electrical noise](#)

firewalls

[8.8.9. Account Names Revisited: Using Aliases for Increased Security](#)

[17.2. Controlling Access to Servers](#)

[21. Firewalls](#)

[21.4.2. Electronic Mail](#)

[21.5. Special Considerations](#)

checklist for : [A.1.1.20. Chapter 21: Firewalls](#)

mailing list for

[E.1.3.1. Academic-Firewalls](#)

[E.1.3.7. Firewalls](#)

nameservers and : [17.3.6.2. DNS nameserver attacks](#)

for NIS sites : [19.4.5. Unintended Disclosure of Site Information with NIS](#)

portmapper program and : [19.2.1. Sun's portmap/rpcbind](#)

for specific network services : [G. Table of IP Services](#)

FIRST teams

[24.6. Resuming Operation](#)

[E.3.3. FIRST](#)

Fitzgerald, Tom : [22.5. UDP Relayer](#)

flooding

client : [16.3.2. Security and Nameservice](#)

messages : [25.3.2. Message Flooding](#)

servers with requests : [25.3.1. Service Overloading](#)

water : (see [water](#))

floors, raised : [12.2.3.1. Raised floors and dropped ceilings](#)

floppy disks : (see [backups](#); [media](#))

folders : (see [directories](#))

FollowSymLinks option : [18.3.2. Commands Within the <Directory> Block](#)

food : [12.2.2.1. Food and drink](#)

fork command

[23.2. Tips on Avoiding Security-related Bugs](#)

[25.2.1.1. Too many processes](#)

[C.2. Creating Processes](#)

format

file, monitoring : [8.2. Monitoring File Format](#)

redoing as destructive attack : [25.1. Destructive Attacks](#)

USERFILE entries : [15.4.1.3. Format of USERFILE entry without system name](#)

.forward file

[11.5.2.5. .forward, .procmailrc](#)

[21.4.2. Electronic Mail](#)

[24.4.1.6. Changes to startup files](#)

Frame Ground (FG) : [14.3. The RS-232 Serial Protocol](#)

fraud

[14.4.1. One-Way Phone Lines](#)

[26.2.2. Federal Jurisdiction](#)

fscanf function : [23.2. Tips on Avoiding Security-related Bugs](#)

fsck program

[24.4.1.7. Hidden files and directories](#)

[25.2.2.8. Tree-structure attacks](#)

fsrand command : [20.4.8. Use fsrand](#)

fstab file

[11.1.2. Back Doors and Trap Doors](#)

[19.3.2.5. Mounting a secure filesystem](#)

FTP (File Transfer Protocol)

[17.3.2. \(FTP\) File Transfer Protocol \(TCP Ports 20 and 21\)](#)

[17.3.2.7. Allowing only FTP access](#)

anonymous

[4.1. Users and Groups](#)

[17.3.2.1. Using anonymous FTP](#)

[17.3.2.6. Setting up anonymous FTP with the standard UNIX FTP server](#)

anonymous

and HTTP : [18.2.4.1. Beware mixing HTTP with anonymous FTP](#)

~ftp/bin directory : [17.3.2.6. Setting up anonymous FTP with the standard UNIX FTP server](#)

~ftp/etc directory : [17.3.2.6. Setting up anonymous FTP with the standard UNIX FTP server](#)
~ftp/pub directory : [17.3.2.6. Setting up anonymous FTP with the standard UNIX FTP server](#)
logging transferred files : [10.3.3. xferlog Log File](#)
passive mode
 [17.3.2.2. Passive vs. active FTP](#)
 [17.3.2.3. FTP passive mode](#)
setting up server
 [17.3.2.4. Setting up an FTP server](#)
 [17.3.2.6. Setting up anonymous FTP with the standard UNIX FTP server](#)
ftp account : (see [anonymous FTP](#))
ftpd server
 [8.4.2. Changing the Account's Login Shell](#)
 [11.1.2. Back Doors and Trap Doors](#)
 [17.3.2. \(FTP\) File Transfer Protocol \(TCP Ports 20 and 21\)](#)
 [17.3.2.4. Setting up an FTP server](#)
for backups : [7.4.5. Backups Across the Net](#)
security hole : [6.5.2. Using Message Digests](#)
UUCP enabled on : [15.8. UUCP Over Networks](#)
ftpout account, firewalls : [21.4.4.1. Creating an ftpout account to allow FTP without proxies.](#)
ftpusers file : [17.3.2.5. Restricting FTP with the standard UNIX FTP server](#)
ftruncate system call : [5.1.7. File Permissions in Detail](#)
full backups : [7.1.3. Types of Backups](#)
function keys : [12.3.4.5. Function keys](#)
functionality, add-on : [1.4.3. Add-On Functionality Breeds Problems](#)

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

[Copyright](#) © 1999 [O'Reilly & Associates, Inc.](#) All Rights Reserved.

[[Library Home](#) | [DNS & BIND](#) | [TCP/IP](#) | [sendmail](#) | [sendmail Reference](#) | [Firewalls](#) | [Practical Security](#)]



Practical UNIX & Internet Security

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

Index: G

games

[8.1.4. Open Accounts](#)

[17.3.23. Other TCP Ports: MUDs and Internet Relay Chat \(IRC\)](#)

gas, natural : [12.2.1.5. Explosion](#)

gated daemon : [17.3.19. Routing Internet Protocol \(RIP routed\) \(UDP Port 520\)](#)

gateways : [16.2.2. Routing](#)

gcore program : [C.4. The kill Command](#)

GCT tool : [23.2. Tips on Avoiding Security-related Bugs](#)

gdb debugger : [C.4. The kill Command](#)

GECOS (or GCOS) : [3.2.1. The /etc/passwd File](#)

Geer, Dan : [27.2.6. Network Providers that Network Too Well](#)

General Electric Company : [F.3.4.13. General Electric](#)

generating

passwords automatically : [8.8.4. Password Generators](#)

random numbers : [23.6. Tips on Generating Random Numbers](#)

German government institutions : [F.3.4.25. Netherlands: SURFnet-connected sites](#)

gethostbyaddresses function : [16.2.6.1. DNS under UNIX](#)

gethostbyname function : [16.2.6.1. DNS under UNIX](#)

getopt function : [23.2. Tips on Avoiding Security-related Bugs](#)

getpass function

[23.2. Tips on Avoiding Security-related Bugs](#)

[23.5. Tips on Using Passwords](#)

getpwuid function : [19.4.1. Including or excluding specific accounts:](#)

gets function : [23.1.1. The Lesson of the Internet Worm](#)

getservicebyname function : [17.1.1. The /etc/services File](#)

getstats program : [10.3.5. access_log Log File](#)

getty program : [C.5.2. Logging In](#)

GIDs (group identifiers)

[1.4.3. Add-On Functionality Breeds Problems](#)

[4.1.3. Groups and Group Identifiers \(GIDs\)](#)

[4.1.3.3. Groups and BSD or SVR4 UNIX](#)

real versus effective : [4.3.1. Real and Effective UIDs](#)

GIP RENATER : [F.3.4.12. France: universities, Ministry of Research and](#)

[Education in France, CNRS, CEA, INRIA, CNES, INRA, IFREMER, and EDF](#)

glass walls : [12.2.3.3. Glass walls](#)

GNU Emacs : [11.5.2.3. GNU .emacs](#)

GNU utilities : [23.1.2.1. What they found](#)

Goldman, Sachs, and Company : [F.3.4.38. U.K. JANET network](#)

granularity, time : [23.8. Picking a Random Seed](#)

grounding signals : [25.3.3. Signal Grounding](#)

group disk quotas : [25.2.2.5. Using quotas](#)

group file

[1.2. What Is an Operating System?](#)

[4.1.3.1. The /etc/group file](#)

[4.2.3. Impact of the /etc/passwd and /etc/group Files on Security](#)

[8.1.6. Group Accounts](#)

group IDs : (see [GIDs](#))

Group table (NIS+) : [19.5.3. NIS+ Tables](#)

groups

[4.1.3. Groups and Group Identifiers \(GIDs\)](#)

[4.1.3.3. Groups and BSD or SVR4 UNIX](#)

accounts for : [8.1.6. Group Accounts](#)

changing : [5.8. chgrp: Changing a File's Group](#)

checklist for : [A.1.1.3. Chapter 4: Users, Groups, and the Superuser](#)

files writable by : [11.6.1.2. Writable system files and directories](#)

identifiers for : (see [GIDs](#))

NIS netgroups

[19.4.4. NIS Netgroups](#)

[19.4.4.6. NIS is confused about "+"](#)

umask for group projects : [5.3.1. The umask Command](#)

wheel : (see [wheel group](#))

grpck command : [8.2. Monitoring File Format](#)

guessing passwords : (see [cracking, passwords](#))

guest accounts

[4.1. Users and Groups](#)

[8.1.4. Open Accounts](#)

[8.1.4.6. Potential problems with rsh](#)

[8.8.7. Algorithm and Library Changes](#)

[Copyright](#) © 1999 [O'Reilly & Associates, Inc.](#) All Rights Reserved.

[[Library Home](#) | [DNS & BIND](#) | [TCP/IP](#) | [sendmail](#) | [sendmail Reference](#) | [Firewalls](#) | [Practical Security](#)]



Practical UNIX & Internet Security

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

Index: H

hacker challenges : [27.2.4. Hacker Challenges](#)
hackers : [1. Introduction](#)
Haley, Chuck : [1.3. History of UNIX](#)
Halon fire extinguishers : [12.2.1.1. Fire](#)
 and radio transmitters : [12.2.1.8. Electrical noise](#)
halt command : [24.2.6. Anatomy of a Break-in](#)
hanging up modem : (see [signals](#))
harassment : [26.4.7. Harassment, Threatening Communication, and Defamation](#)
hard copy : (see [paper](#))
hard disks : (see [media](#))
hardcopy device, logging to : [10.5.2.1. Logging to a printer](#)
hardware
 bugs in : [27.2.1. Hardware Bugs](#)
 failure of : [7.1.1.1. A taxonomy of computer failures](#)
 food and drink threats : [12.2.2.1. Food and drink](#)
 modems
 [14. Telephone Security](#)
 [14.6. Additional Security for Modems](#)
 physical security of
 [12.2. Protecting Computer Hardware](#)
 [12.2.7. Related Concerns](#)
 read-only filesystems : [9.1.2. Read-only Filesystems](#)
 seized as evidence : [26.2.4. Hazards of Criminal Prosecution](#)
hash functions : [6.5.1. Message Digests](#)
hash mark (#), disabling services with : [17.3. Primary UNIX Network Services](#)
HAVAL algorithm : [6.5.4.3. HAVAL](#)
HAVAL algorithm : [23.9. A Good Random Seed Generator](#)
HDB UUCP : [15.2. Versions of UUCP](#)
header, packet : [16.2. IPv4: The Internet Protocol Version 4](#)
heat, extreme : [12.2.1.6. Temperature extremes](#)
Hellman, Martin : [6.4.5.1. Double DES](#)
Hellman-Merkle : [18.6. Dependence on Third Parties](#)
Hewlett-Packard (HP) : [F.3.4.17. Hewlett-Packard customers](#)
hidden

data, in CGI scripts : [18.2.3.1. Do not trust the user's browser!](#)
files, created by intruders : [24.4.1.7. Hidden files and directories](#)
space : [25.2.2.7. Hidden space](#)
hijacking Telnet sessions : [17.3.3. TELNET \(TCP Port 23\)](#)
history file (csh)
 [10.4.1. Shell History](#)
 [15.1.1.1. uucp with the C shell](#)
hit lists of passwords : [3.6.1. Bad Passwords: Open Doors](#)
holes, security : (see [security holes](#))
HOME variable, attacks via : [11.5.1.3. \\$HOME attacks](#)
HoneyDanBer (HDB) UUCP : [15.2. Versions of UUCP](#)
Honeyman, Peter : [15.2. Versions of UUCP](#)
hostnames
 [16.2.3. Hostnames](#)
 [16.2.3.1. The /etc/hosts file](#)
controlling access to : [17.2. Controlling Access to Servers](#)
name service and
 [16.2.6. Name Service](#)
 [16.2.6.2. Other naming services](#)
hosts
 NID passwords for : [19.3.2.2. Creating passwords for hosts](#)
 trusted : (see [trusted, hosts](#))
hosts file : [16.2.3.1. The /etc/hosts file](#)
hosts.equiv file
 [17.3.18.4. The ~/.rhosts file](#)
 [17.3.18.6. /etc/hosts.lpd file](#)
 [24.4.1.5. Changes to the /etc/hosts.equiv file](#)
hosts.lpd file : [17.3.18.6. /etc/hosts.lpd file](#)
HP (Hewlett-Packard) : [F.3.4.17. Hewlett-Packard customers](#)
HP-UX
 access control lists : [5.2.5.2. HP-UX access control lists](#)
 context-dependent files : [5.9.2. Context-Dependent Files](#)
.htaccess file : [18.3.1. The access.conf and .htaccess Files](#)
HTML documents
 controlling access to
 [18.3. Controlling Access to Files on Your Server](#)
 [18.3.3. Setting Up Web Users and Passwords](#)
 encrypting : [18.4.1. Eavesdropping Over the Wire](#)
server-side includes

[18.2.2.2. Additional configuration issues](#)

[18.3.2. Commands Within the <Directory> Block](#)

htpasswd program : [18.3.3. Setting Up Web Users and Passwords](#)

HTTP (Hypertext Transfer Protocol) : [17.3.9. HyperText Transfer Protocol \(HTTP\) \(TCP Port 80\)](#)

and anonymous FTP : [18.2.4.1. Beware mixing HTTP with anonymous FTP](#)

logging downloaded files : [10.3.5. access_log Log File](#)

Secure : (see [Secure HTTP](#))

http server

group file : [18.3.2. Commands Within the <Directory> Block](#)

log files of : [18.4.2. Eavesdropping Through Log Files](#)

password file : [18.3.2. Commands Within the <Directory> Block](#)

httpd.conf file : [18.2.1. The Server's UID](#)

human error and backups : [7.1.4. Guarding Against Media Failure](#)

humidity : [12.2.1.11. Humidity](#)

hypertext links, encrypting : [18.4.1. Eavesdropping Over the Wire](#)

Hypertext Transfer Protocol : (see [HTTP](#))

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

[Copyright](#) © 1999 [O'Reilly & Associates, Inc.](#) All Rights Reserved.

[[Library Home](#) | [DNS & BIND](#) | [TCP/IP](#) | [sendmail](#) | [sendmail Reference](#) | [Firewalls](#) | [Practical Security](#)]



Practical UNIX & Internet Security

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

Index: I

I/O : (see [input/output](#))

ICMP (Internet Control Message Protocol) : [16.2.4.1. ICMP](#)

IDEA (International Data Encryption Algorithm)

[6.4.1. Summary of Private Key Systems](#)

[6.6.3.1. Encrypting files with IDEA](#)

identd daemon : [17.3.12. Identification Protocol \(auth\) \(TCP Port 113\)](#)

identification protocol : [17.3.12. Identification Protocol \(auth\) \(TCP Port 113\)](#)

identifiers : [3.1. Usernames](#)

IEEE Computer Society : [F.1.7. IEEE Computer Society](#)

IFS variable

[5.5.3.2. Another SUID example: IFS and the /usr/lib/preserve hole](#)

[23.4. Tips on Writing SUID/SGID Programs](#)

attacks via : [11.5.1.2. IFS attacks](#)

ignore (in Swatch command) : [10.6.2. The Swatch Configuration File](#)

immutable files : [9.1.1. Immutable and Append-Only Files](#)

importing NIS accounts

[19.4.1. Including or excluding specific accounts:](#)

[19.4.4.2. Using netgroups to limit the importing of accounts](#)

in.named daemon : [16.2.6.1. DNS under UNIX](#)

includes : (see [server-side includes](#))

Includes option : [18.3.2. Commands Within the <Directory> Block](#)

IncludesNoExec option : [18.3.2. Commands Within the <Directory> Block](#)

incremental backups : [7.1.3. Types of Backups](#)

indecent material : [26.4.5. Pornography and Indecent Material](#)

index.html file, absence of : [18.2.2.2. Additional configuration issues](#)

inetd daemon

[17.1.2. Starting the Servers](#)

[17.1.3. The /etc/inetd Program](#)

-nowait option : [25.3.1. Service Overloading](#)

-t (trace) option : [10.3.6. Logging Network Services](#)

denial-of-service attacks : [17.1.3. The /etc/inetd Program](#)

inetd.conf file

[11.5.3.2. inetd.conf](#)

[17.3. Primary UNIX Network Services](#)

information : (see [data](#))

init program

[5.3.2. Common umask Values](#)

[C.5.1. Process #1: /etc/init](#)

initialization vector (IV) : [6.4.4.2. DES modes](#)

initializing

environment variables : [11.5.2.7. Other initializations](#)

system, files for : [11.5.3.5. System initialization files](#)

inittab program

[14.5.1. Hooking Up a Modem to Your Computer](#)

[C.5.1. Process #1: /etc/init](#)

INND program : [17.3.13. Network News Transport Protocol \(NNTP\) \(TCP Port 119\)](#)

inodes

[5.1. Files](#)

[5.1.2. Inodes](#)

change time : (see [ctime](#))

for device files : [5.6. Device Files](#)

problems with : [25.2.2.3. Inode problems](#)

input/output (I/O)

checking for meta characters : [23.2. Tips on Avoiding Security-related Bugs](#)

portable library : [1.3. History of UNIX](#)

insects : [12.2.1.7. Bugs \(biological\)](#)

installing

cables : [12.2.4.2. Network cables](#)

Kerberos : [19.6.3. Installing Kerberos](#)

logging installations : [10.7.2.1. Exception and activity reports](#)

physical security plan for : [12.1.1. The Physical Security Plan](#)

insurance

[26.1. Legal Options After a Break-in](#)

[26.2.6. Other Tips](#)

integrity

[2.1. Planning Your Security Needs](#)

[9. Integrity Management](#)

[9.3. A Final Note](#)

[11.1.5. Viruses](#)

[12.3. Protecting Data](#)

[12.3.6. Key Switches](#)

Kerberos : [19.6.1.3. Authentication, data integrity, and secrecy](#)

management checklist : [A.1.1.8. Chapter 9: Integrity Management](#)
Secure RPC : [19.3.4. Limitations of Secure RPC](#)
software for checking : [19.5.5. NIS+ Limitations](#)
international cryptography export
 [6.4.4.1. Use and export of DES](#)
 [6.7.2. Cryptography and Export Controls](#)
International Data Encryption Algorithm (IDEA)
 [6.4.1. Summary of Private Key Systems](#)
 [6.6.3.1. Encrypting files with IDEA](#)
Internet
 [16.1.1. The Internet](#)
 [18. WWW Security](#)
 (see also [World Wide Web](#))
 addresses
 [16.2.1. Internet Addresses](#)
 [16.2.1.3. CIDR addresses](#)
 daemon : (see [inetd daemon](#))
 domain as NIS domain : [19.4.3. NIS Domains](#)
 firewalls : (see [firewalls](#))
 servers : (see [servers, Internet](#))
 Worm program : [1. Introduction](#)
 Worm program Worm program : [23.1.1. The Lesson of the Internet Worm](#)
Internet Control Message Protocol (ICMP) : [16.2.4.1. ICMP](#)
Internet Packet Exchange (IPX) : [16.4.1. IPX](#)
Internet Relay Chat (IRC) : [17.3.23. Other TCP Ports: MUDs and Internet Relay Chat \(IRC\)](#)
Internet Security Scanner (ISS) : [17.6.2. ISS](#)
intruders : [1. Introduction](#)
 confronting : [24.2.2. What to Do When You Catch Somebody](#)
 creating hidden files : [24.4.1.7. Hidden files and directories](#)
 discovering
 [24.2. Discovering an Intruder](#)
 [24.2.6. Anatomy of a Break-in](#)
 legal options regarding : [26.1. Legal Options After a Break-in](#)
 responding to
 [24. Discovering a Break-in](#)
 [24.7. Damage Control](#)
 tracking from log files : [24.3. The Log Files: Discovering an Intruder's Tracks](#)

ioctl system call : [C.1.3.4. Process groups and sessions](#)

IP addresses

controlling access by : [17.2. Controlling Access to Servers](#)

name service and

[16.2.6. Name Service](#)

[16.2.6.2. Other naming services](#)

restricting access by : [18.3. Controlling Access to Files on Your Server](#)

IP numbers, monitoring : [12.3.1.2. Eavesdropping by Ethernet and 10Base-T](#)

IP packets

[16.2. IPv4: The Internet Protocol Version 4](#)

[16.2.4. Packets and Protocols](#)

[16.2.4.3. UDP](#)

eavesdropping : [16.3.1. Link-level Security](#)

monitoring : [12.3.1.2. Eavesdropping by Ethernet and 10Base-T](#)

sniffing

[16.3.1. Link-level Security](#)

[17.3.3. TELNET \(TCP Port 23\)](#)

IP protocols

[1.4.3. Add-On Functionality Breeds Problems](#)

[16.2.4. Packets and Protocols](#)

[16.2.4.3. UDP](#)

IP security

[16.3. IP Security](#)

[16.3.3. Authentication](#)

IP services : (see [network services](#))

IP spoofing

[1.4.3. Add-On Functionality Breeds Problems](#)

[16.3. IP Security](#)

IPv4 (IP Version 4)

[16.2. IPv4: The Internet Protocol Version 4](#)

[16.2.6.2. Other naming services](#)

IPX (Internet Packet Exchange) : [16.4.1. IPX](#)

IRC (Internet Relay Chat) : [17.3.23. Other TCP Ports: MUDs and Internet Relay Chat \(IRC\)](#)

IRIX wtmpx file : [10.1.2. utmp and wtmp Files](#)

ISS (Internet Security Scanner)

[17.6.2. ISS](#)

[E.4.4. ISS \(Internet Security Scanner\)](#)

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

[Copyright](#) © 1999 [O'Reilly & Associates, Inc.](#) All Rights Reserved.

[[Library Home](#) | [DNS & BIND](#) | [TCP/IP](#) | [sendmail](#) | [sendmail Reference](#) | [Firewalls](#) | [Practical Security](#)]



Practical UNIX & Internet Security

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

Index: J

Java programming language

[11.1.5. Viruses](#)

[18.5.1. Executing Code from the Net](#)

Joe accounts

[3.6.2. Smoking Joes](#)

[8.8.3.1. Joetest: a simple password cracker](#)

Joy, Bill : [1.3. History of UNIX](#)

JP Morgan : [F.3.4.18. JP Morgan employees and customers](#)

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

[Copyright](#) © 1999 [O'Reilly & Associates, Inc.](#) All Rights Reserved.

[[Library Home](#) | [DNS & BIND](#) | [TCP/IP](#) | [sendmail](#) | [sendmail Reference](#) | [Firewalls](#) | [Practical Security](#)]



Practical UNIX & Internet Security

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

Index: K

Karn, Phil : [6.6.2. des: The Data Encryption Standard](#)

Kerberos system

[8.7.3. Code Books](#)

[19.6. Kerberos](#)

[19.6.5. Kerberos Limitations](#)

[E.4.5. Kerberos](#)

installing : [19.6.3. Installing Kerberos](#)

RPC system and : [19.2.2.4. AUTH_KERB](#)

Versions 4 and 5 : [19.6.1.4. Kerberos 4 vs. Kerberos 5](#)

versus Secure RPC : [19.6.2. Kerberos vs. Secure RPC](#)

kermi program

[14.5. Modems and UNIX](#)

[14.5.3.3. Privilege testing](#)

kernel

[1.2. What Is an Operating System?](#)

[5.5.3. SUID Shell Scripts](#)

key

escrow : [6.1.3. Modern Controversy](#)

fingerprints : [6.6.3.6. PGP detached signatures](#)

search

[6.2.3. Cryptographic Strength](#)

[8.6.1. The crypt\(\) Algorithm](#)

switches : [12.3.6. Key Switches](#)

keylogin program

[19.3.3. Using Secure RPC](#)

[19.5.4. Using NIS+](#)

keylogout program : [19.3.3. Using Secure RPC](#)

keyserv process

[19.3.1.1. Proving your identity](#)

[19.3.2.3. Making sure Secure RPC programs are running on every workstation](#)

[19.5.4. Using NIS+](#)

keystore file : [19.3.1.1. Proving your identity](#)

keystrokes

monitoring
 [17.3.21.2. X security](#)
 [24.2.3. Monitoring the Intruder](#)
monitoring
 [17.3.21.2. X security](#)
 (see also [sniffers](#))
time between : [23.8. Picking a Random Seed](#)
kill command
 [17.3.4.2. Using sendmail to receive email](#)
 [24.2.5. Getting Rid of the Intruder](#)
 [C.4. The kill Command](#)
to stop process overload
 [25.2.1.1. Too many processes](#)
 [25.2.1.2. System overload attacks](#)
kinit program : [19.6.4. Using Kerberos](#)
kmem device
 [5.6. Device Files](#)
 [11.1.2. Back Doors and Trap Doors](#)
known text attacks : [6.2.3. Cryptographic Strength](#)
Koblas, David : [22.4. SOCKS](#)
Koblas, Michelle : [22.4. SOCKS](#)
ksh (Korn shell)
 [11.5.1. Shell Features](#)
 [24.4.1.7. Hidden files and directories](#)
 [C.5.3. Running the User's Shell](#)
 (see also [shells](#))
history file : [10.4.1. Shell History](#)
restricted shell : [8.1.4.3. Restricted Korn shell](#)
TMOUT variable : [12.3.5.1. Built-in shell autologout](#)
umask and : [5.3.1. The umask Command](#)
ksh93 shell
 [23.2. Tips on Avoiding Security-related Bugs](#)
 [24.4.1.7. Hidden files and directories](#)
.kshrc file : [11.5.2.2. .cshrc, .kshrc](#)

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

[Copyright](#) © 1999 [O'Reilly & Associates, Inc.](#) All Rights Reserved.

[[Library Home](#) | [DNS & BIND](#) | [TCP/IP](#) | [sendmail](#) | [sendmail Reference](#) | [Firewalls](#) | [Practical Security](#)]



Practical UNIX & Internet Security

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

Index: L

L-devices file : [14.5.1. Hooking Up a Modem to Your Computer](#)

L.cmds file : [15.4.3. L.cmds: Providing Remote Command Execution](#)

L.sys file : [15.3.3. Security of L.sys and Systems Files](#)

Lai, Xuejia : [6.4.1. Summary of Private Key Systems](#)

laid-off employees : [13.2.6. Departure](#)

LaMacchia, Brian : [19.3.4. Limitations of Secure RPC](#)

LANs (local area networks)

[16.1. Networking](#)

[16.2. IPv4: The Internet Protocol Version 4](#)

laptop computers : [12.2.6.3. Portables](#)

last program

[8.4.3. Finding Dormant Accounts](#)

[10.1.2. utmp and wtmp Files](#)

[10.1.3. last Program](#)

[10.1.3.1. Pruning the wtmp file](#)

[15.3.1. Assigning Additional UUCP Logins](#)

-f option : [10.1.3.1. Pruning the wtmp file](#)

lastcomm program

[10.2. The acct/pacct Process Accounting File](#)

[10.2.2. Accounting with BSD](#)

lastlog file : [10.1.1. lastlog File](#)

laws

[26. Computer Security and U.S. Law](#)

[26.4.7. Harassment, Threatening Communication, and Defamation](#)

backups and : [7.1.7. Legal Issues](#)

checklist for : [A.1.1.25. Chapter 26: Computer Security and U.S. Law](#)

copyright

[9.2.1. Comparison Copies](#)

[26.4.2. Copyright Infringement](#)

[26.4.2.1. Software piracy and the SPA](#)

criminal prosecution

[26.2. Criminal Prosecution](#)

[26.2.7. A Final Note on Criminal Actions](#)

Electronic Communications Privacy Act (ECPA) : [26.2.3. Federal](#)

[Computer Crime Laws](#)

encryption

[6.7. Encryption and U.S. Law](#)

[6.7.2. Cryptography and Export Controls](#)

[12.2.6.3. Portables](#)

enforcement agencies : [14.4.4.1. Kinds of eavesdropping](#)

export

[6.4.4.1. Use and export of DES](#)

[6.7.2. Cryptography and Export Controls](#)

[26.4.1. Munitions Export](#)

federal enforcement

[26.2.2. Federal Jurisdiction](#)

[26.2.3. Federal Computer Crime Laws](#)

indecent material : [26.4.5. Pornography and Indecent Material](#)

liability

[26.4. Other Liability](#)

[26.4.7. Harassment, Threatening Communication, and Defamation](#)

monitoring keystrokes : [24.2.3. Monitoring the Intruder](#)

non-citizen access : [26.4.1. Munitions Export](#)

patents : [26.4.4. Patent Concerns](#)

for portable computers : [12.2.6.3. Portables](#)

resources on : [D.1.1. Other Computer References](#)

search warrants

[26.2.4. Hazards of Criminal Prosecution](#)

[26.2.5. If You or One of Your Employees Is a Target of an Investigation...](#)

smoking : [12.2.1.2. Smoke](#)

state and local enforcement : [26.2.1. The Local Option](#)

trademarks : [26.4.3. Trademark Violations](#)

vendor liability : [18.5.2. Trusting Your Software Vendor](#)

lawsuits (civil) : [26.3. Civil Actions](#)

leased telephone lines : [14.5.4. Physical Protection of Modems](#)

least privilege

[5.5.3.2. Another SUID example: IFS and the /usr/lib/preserve hole](#)

[13.2.5. Least Privilege and Separation of Duties](#)

Lee, Ying-Da : [22.4. SOCKS](#)

Lesk, Mike

[1.3. History of UNIX](#)

[15.2. Versions of UUCP](#)

liability, legal

[26.4. Other Liability](#)

[26.4.7. Harassment, Threatening Communication, and Defamation](#)

/lib directory : [11.5.3.6. Other files](#)

license agreements : [18.5.2. Trusting Your Software Vendor](#)

comparison copies and : [9.2.1. Comparison Copies](#)

lie-detector tests : [13.1. Background Checks](#)

lightning

[12.2. Protecting Computer Hardware](#)

[12.2.1.9. Lightning](#)

limit command : [25.2.5. Soft Process Limits: Preventing Accidental Denial of Service](#)

Limit command (<Directory>) : [18.3.2. Commands Within the <Directory> Block](#)

limited user access : [8.1.5.1. Limited users](#)

link-level security : [16.3.1. Link-level Security](#)

links

encryption of : [18.4.1. Eavesdropping Over the Wire](#)

link-level security : [16.3.1. Link-level Security](#)

static : [23.4. Tips on Writing SUID/SGID Programs](#)

symbolic, following (Web)

[18.2.2.2. Additional configuration issues](#)

[18.3.2. Commands Within the <Directory> Block](#)

lint program : [23.2. Tips on Avoiding Security-related Bugs](#)

LINUX operating system

[1.3. History of UNIX](#)

[3.3. Entering Your Password](#)

[23.1.2.1. What they found](#)

ext2 filesystem : [25.2.2.6. Reserved space](#)

random number generators : [23.7.4. Other random number generators](#)

Live Script : [18.5.2. Trusting Your Software Vendor](#)

load shedding : [23.3. Tips on Writing Network Programs](#)

local

area networks (LANs)

[16.1. Networking](#)

[16.2. IPv4: The Internet Protocol Version 4](#)

authentication (NIS+) : [19.5.4. Using NIS+](#)

law enforcement : [26.2.1. The Local Option](#)

storage

[12.3.4. Protecting Local Storage](#)

[12.3.4.5. Function keys](#)

users, and USERFILE : [15.4.1.2. USERFILE entries for local users](#)

lock program : [12.3.5.2. X screen savers](#)

locked accounts : [3.3. Entering Your Password](#)

locking files : [23.2. Tips on Avoiding Security-related Bugs](#)

log files

[11.5.3.5. System initialization files](#)

(see also [logging](#))

access_log

[10.3.5. access_log Log File](#)

[18.4.2. Eavesdropping Through Log Files](#)

aculog : [10.3.1. aculog File](#)

agent_log file : [18.4.2. Eavesdropping Through Log Files](#)

backing up : [10.2.2. Accounting with BSD](#)

lastlog : [10.1.1. lastlog File](#)

managing : [10.8. Managing Log Files](#)

manually generated

[10.7. Handwritten Logs](#)

[10.7.2.2. Informational material](#)

per-machine : [10.7.2. Per-Machine Logs](#)

per-site : [10.7.1. Per-Site Logs](#)

refer_log file : [18.4.2. Eavesdropping Through Log Files](#)

sulog : (see [sulog file](#))

system clock and : [17.3.14. Network Time Protocol \(NTP\) \(UDP Port 123\)](#)

tracking intruders with : [24.3. The Log Files: Discovering an Intruder's Tracks](#)

/usr/adm/messages : [10.2.3. messages Log File](#)

utmp and wtmp

[10.1.2. utmp and wtmp Files](#)

[10.1.3.1. Pruning the wtmp file](#)

uucp : [10.3.4. uucp Log Files](#)

/var/adm/acct : [10.2. The acct/pacct Process Accounting File](#)

/var/adm/loginlog : [10.1.4. loginlog File](#)

of Web servers : [18.4.2. Eavesdropping Through Log Files](#)

xferlog : [10.3.3. xferlog Log File](#)

logdaemon package : [17.3.18.5. Searching for .rhosts files](#)

logger command : [10.5.3. syslog Messages](#)

logging

[7.1.1.1. A taxonomy of computer failures](#)

[10. Auditing and Logging](#)

[10.8. Managing Log Files](#)

[11.5.3.5. System initialization files](#)

[21.5. Special Considerations](#)

[23.2. Tips on Avoiding Security-related Bugs](#)

(see also [log files](#))

across networks : [10.5.2.2. Logging across the network](#)

archiving information : [7.4.2. Simple Archives](#)

breakins : [24.1.2. Rule #2: DOCUMENT](#)

C2 audit : [10.1. The Basic Log Files](#)

checklist for : [A.1.1.9. Chapter 10: Auditing and Logging](#)

critical messages

[10.5.3. syslog Messages](#)

[10.5.3.1. Beware false log entries](#)

downloaded files

[10.3.3. xferlog Log File](#)

[10.3.5. access_log Log File](#)

failed su attempts : [4.3.7. The Bad su Log](#)

file format : [8.2. Monitoring File Format](#)

files transferred by FTP : [10.3.3. xferlog Log File](#)

to hardcopy device : [10.5.2.1. Logging to a printer](#)

individual users

[10.4. Per-User Trails in the Filesystem](#)

[10.4.3. Network Setup](#)

manually

[10.7. Handwritten Logs](#)

[10.7.2.2. Informational material](#)

mistyped passwords : [10.5.3. syslog Messages](#)

network services : [10.3.6. Logging Network Services](#)

outgoing mail : [10.4.2. Mail](#)

potentially criminal activity : [26.2.6. Other Tips](#)

Swatch program

[10.6. Swatch: A Log File Tool](#)

[10.6.2. The Swatch Configuration File](#)

[E.4.9. Swatch](#)

syslog facility

[10.5. The UNIX System Log \(syslog\) Facility](#)

[10.5.3.1. Beware false log entries](#)

UUCP : [10.3.4. uucp Log Files](#)

what not to log : [10.5.3. syslog Messages](#)

logging in

[C.5. Starting Up UNIX and Logging In](#)

[C.5.3. Running the User's Shell](#)

FTP access without : [17.3.2.7. Allowing only FTP access](#)

Kerberos system : [19.6.1.1. Initial login](#)

last program

[10.1.3. last Program](#)

[10.1.3.1. Pruning the wtmp file](#)

lastlog file : [10.1.1. lastlog File](#)

passwords : [3.3. Entering Your Password](#)

preventing

[8.4. Managing Dormant Accounts](#)

[8.4.3. Finding Dormant Accounts](#)

restricting : [8.3. Restricting Logins](#)

with Secure RPC : [19.3.3. Using Secure RPC](#)

startup file attacks

[11.5.2. Start-up File Attacks](#)

[11.5.2.7. Other initializations](#)

logging out with Secure RPC[logging out:Secure RPC] : [19.3.3. Using Secure RPC](#)

logic bombs

[11.1. Programmed Threats: Definitions](#)

[11.1.3. Logic Bombs](#)

[27.2.2. Viruses on the Distribution Disk](#)

.login file

[8.5.1. Secure Terminals](#)

[11.5.2.1. .login, .profile, /etc/profile](#)

[24.4.1.6. Changes to startup files](#)

login program

[8.6. The UNIX Encrypted Password System](#)

[11.1.2. Back Doors and Trap Doors](#)

[19.5.4. Using NIS+](#)

[26.2.6. Other Tips](#)

[27.1.2. Trusting Trust](#)

logindevperm file : [17.3.21.1. /etc/fstab and /etc/logindevperm](#)

loginlog file : [10.1.4. loginlog File](#)

logins

authentication : [17.3.5. TACACS \(UDP Port 49\)](#)
FTP : [17.3.2. \(FTP\) File Transfer Protocol \(TCP Ports 20 and 21\)](#)
UUCP, additional : [15.3.1. Assigning Additional UUCP Logins](#)
logins command : [8.1.1. Accounts Without Passwords](#)
-d option : [8.2. Monitoring File Format](#)
-p option : [8.2. Monitoring File Format](#)
LOGNAME= command
[15.5.1.3. A Sample Permissions file](#)
[15.5.2. Permissions Commands](#)
.logout file : [19.3.3. Using Secure RPC](#)
long distance service
[14.5.4. Physical Protection of Modems](#)
[17.3.3. TELNET \(TCP Port 23\)](#)
losses, cost of preventing
[2.3. Cost-Benefit Analysis](#)
[2.3.4. Convincing Management](#)
lp (user) : [4.1. Users and Groups](#)
lpd system : [17.3.18.6. /etc/hosts.lpd file](#)
lrand48 function : [23.7.3. drand48 \(\), lrand48 \(\), and mrand48 \(\)](#)
ls command
[5.1.4. Using the ls Command](#)
[5.1.5. File Times](#)
[9.2.2. Checklists and Metadata](#)
-c option : [5.1.5. File Times](#)
-d option : [9.2.2.1. Simple listing](#)
-e option : [5.2.5.1. AIX Access Control Lists](#)
-F option : [5.1.4. Using the ls Command](#)
-g option : [5.1.4. Using the ls Command](#)
-H option : [5.9.2. Context-Dependent Files](#)
-i option : [9.2.2.1. Simple listing](#)
-l option
[5.1.4. Using the ls Command](#)
[5.2.5.1. AIX Access Control Lists](#)
[5.5.1. SUID, SGID, and Sticky Bits](#)
-q option : [5.4. Using Directory Permissions](#)
-u option : [5.1.5. File Times](#)
-c option : [24.4.1.6. Changes to startup files](#)
-H option : [24.4.1.7. Hidden files and directories](#)
-l option : [24.4.1.6. Changes to startup files](#)

lsacl command : [5.2.5.2. HP-UX access control lists](#)

lsof program : [25.2.2.7. Hidden space](#)

lstat function : [23.2. Tips on Avoiding Security-related Bugs](#)

Lucifer algorithm

[6.4.4. DES](#)

[6.4.4.3. DES strength](#)

LUCIFER cipher : [6.4.4. DES](#)

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

[Copyright](#) © 1999 [O'Reilly & Associates, Inc.](#) All Rights Reserved.

[[Library Home](#) | [DNS & BIND](#) | [TCP/IP](#) | [sendmail](#) | [sendmail Reference](#) | [Firewalls](#) | [Practical Security](#)]



Practical UNIX & Internet Security

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

Index: M

MAC (Mandatory Access Controls) : [4.1.3. Groups and Group Identifiers \(GIDs\)](#)

MACH operating system : [1.3. History of UNIX](#)

machine name : [16.2.3. Hostnames](#)

MACHINE= command

[15.5.1.2. Name-value pairs](#)

[15.5.2. Permissions Commands](#)

Macintosh, Web server on : [18.2. Running a Secure Server](#)

macro virus : (see [viruses](#))

magic cookies : [17.3.21.4. Using Xauthority magic cookies](#)

magic number : [5.1.7. File Permissions in Detail](#)

mail

[11.5.3.3. /usr/lib/aliases, /etc/aliases, /etc/sendmail/aliases, aliases.dir, or aliases.pag](#)

(see also [sendmail](#))

accepted by programs : [17.3.4.1. sendmail and security](#)

action, in Swatch program : [10.6.2. The Swatch Configuration File](#)

alias back door : [11.1.2. Back Doors and Trap Doors](#)

aliases : (see [aliases](#))

copyrights on : [26.4.2. Copyright Infringement](#)

Electronic Communications Privacy Act (ECPA) : [26.2.3. Federal Computer Crime Laws](#)

firewalls : [21.4.2. Electronic Mail](#)

forwarding (UUCP) : [15.6.1. Mail Forwarding for UUCP](#)

harassment via : [26.4.7. Harassment, Threatening Communication, and Defamation](#)

logging : [10.4.2. Mail](#)

message flooding : [25.3.2. Message Flooding](#)

phantom, monitoring : [17.3.4.2. Using sendmail to receive email](#)

receiving by sendmail : [17.3.4.2. Using sendmail to receive email](#)

sending via CGI scripts : [18.2.3.3. Sending mail](#)

sent directly to file : [15.7. Early Security Problems with UUCP](#)

startup file attacks : [11.5.2.5. .forward, .procmailrc](#)

mail command : [15.1.3. mail Command](#)

Mail_Aliases table (NIS+) : [19.5.3. NIS+ Tables](#)

mailing lists

[E.1. Mailing Lists](#)

[E.1.3.10. WWW-security](#)

maintenance mode : [C.5.1. Process #1: /etc/init](#)

maintenance personnel : [13.3. Outsiders](#)

makedbm program : [19.4.4.1. Setting up netgroups](#)

malware : [11.1. Programmed Threats: Definitions](#)

man pages : [2.5. The Problem with Security Through Obscurity](#)

management, role of

[2.3.4. Convincing Management](#)

[2.5. The Problem with Security Through Obscurity](#)

MANs (Metropolitan Networks) : [16.1. Networking](#)

manual logging

[10.7. Handwritten Logs](#)

[10.7.2.2. Informational material](#)

manual pages : [23.2. Tips on Avoiding Security-related Bugs](#)

maps, NIS : (see [NIS](#))

Massey, James L. : [6.4.1. Summary of Private Key Systems](#)

Master mode (uucico) : [15.1.4. How the UUCP Commands Work](#)

master server

[19.4. Sun's Network Information Service \(NIS\)](#)

(see also [NIS](#))

MCERT : [F.3.4.21. Motorola, Inc. and subsidiaries](#)

MCI Corporation : [F.3.4.19. MCI Corporation](#)

MD2 algorithm : [6.5.4.1. MD2, MD4, and MD5](#)

MD4 algorithm : [6.5.4.1. MD2, MD4, and MD5](#)

MD5 algorithm

[6.5.2. Using Message Digests](#)

[6.5.4.1. MD2, MD4, and MD5](#)

[23.5.1. Use Message Digests for Storing Passwords](#)

[23.9. A Good Random Seed Generator](#)

digital signatures versus : [6.6.3.6. PGP detached signatures](#)

in POP : [17.3.10. Post Office Protocol \(POP\) \(TCP Ports 109 and 110\)](#)

media : [12.3.3. Other Media](#)

damaged by smoke : [12.2.1.2. Smoke](#)

destroying : [12.3.2.3. Sanitize your media before disposal](#)

failure of : [7.1.4. Guarding Against Media Failure](#)

hard/soft disk quotas : [25.2.2.5. Using quotas](#)

print through process : [12.3.2.1. Verify your backups](#)
rotating for backups : [7.1.3. Types of Backups](#)
rotation of : [7.2.1.2. Media rotation](#)
sanitizing : [12.3.2.3. Sanitize your media before disposal](#)
viruses from : [11.1.5. Viruses](#)
meet-in-the-middle attacks : [6.4.5.1. Double DES](#)
memory
 [25.2.2. Disk Attacks](#)
 [25.2.2.8. Tree-structure attacks](#)
 hidden space : [25.2.2.7. Hidden space](#)
 reserved space : [25.2.2.6. Reserved space](#)
 swap space : [25.2.3. Swap Space Problems](#)
 /tmp directory and : [25.2.4. /tmp Problems](#)
 tree-structure attacks : [25.2.2.8. Tree-structure attacks](#)
Merkle, Ralph : [6.4.5.1. Double DES](#)
Message Authentication Code (MAC) : [6.5.5.2. Message authentication codes](#)
message digests
 [6.5. Message Digests and Digital Signatures](#)
 [6.5.2. Using Message Digests](#)
 [9.2.3. Checksums and Signatures](#)
 [23.5.1. Use Message Digests for Storing Passwords](#)
Tripwire package
 [9.2.4. Tripwire](#)
 [9.2.4.2. Running Tripwire](#)
message flooding : [25.3.2. Message Flooding](#)
messages log file : [10.2.3. messages Log File](#)
meta characters : [23.2. Tips on Avoiding Security-related Bugs](#)
metadata
 [9.2.2. Checklists and Metadata](#)
 [9.2.2.2. Ancestor directories](#)
Metropolitan Networks (MANs) : [16.1. Networking](#)
MH (mail handler) : [11.5.2.5. .forward, .procmailrc](#)
Micro-BIT Virus Center : [F.3.4.16. Germany: Southern area](#)
Miller, Barton : [23.1.2. An Empirical Study of the Reliability of UNIX Utilities](#)
MILNET : [F.3.4.20. MILNET](#)
MIME : [11.1.5. Viruses](#)
MIT-KERBEROS-5 authentication : [17.3.21.3. The xhost facility](#)
Mitnick, Kevin : [27.2.6. Network Providers that Network Too Well](#)
mkpasswd program : [8.8.4. Password Generators](#)

mktemp function : [23.2. Tips on Avoiding Security-related Bugs](#)
MLS (Multilevel Security) environment : ["Secure" Versions of UNIX](#)
mobile network computing : [8.7. One-Time Passwords](#)

modems

[14. Telephone Security](#)

[14.6. Additional Security for Modems](#)

callback setups

[14.4.2.](#)

[14.6. Additional Security for Modems](#)

clogging : [25.3.4. Clogging](#)

encrypting : [14.6. Additional Security for Modems](#)

hanging up : (see [signals](#))

physical security of

[14.5.4. Physical Protection of Modems](#)

[14.6. Additional Security for Modems](#)

recording call information : [10.3.1. aculog File](#)

tracing connections

[24.2.4. Tracing a Connection](#)

[24.2.4.2. How to contact the system administrator of a computer you don't know](#)

UNIX and

[14.5. Modems and UNIX](#)

[14.5.3.3. Privilege testing](#)

modification times

[5.1.2. Inodes](#)

[5.1.5. File Times](#)

[7.4.7. inode Modification Times](#)

[9.2.2. Checklists and Metadata](#)

monitoring

hardware for : (see [detectors](#))

intruders : [24.2.3. Monitoring the Intruder](#)

performance : [13.2.3. Performance Reviews and Monitoring](#)

security : (see [logging](#))

users : [26.2.6. Other Tips](#)

monitors and screen savers : [12.3.5.2. X screen savers](#)

Morris, Robert T.

[1. Introduction](#)

[8.6. The UNIX Encrypted Password System](#)

[17.4. Security Implications of Network Services](#)

motd file : [26.2.6. Other Tips](#)
Motorola, Inc. : [F.3.4.20. MILNET](#)
Motorola, Inc. and subsidiaries : [F.3.4.21. Motorola, Inc. and subsidiaries](#)
mount command : [20.3. Client-Side NFS Security](#)
 -nODEV option : [5.5.5. Turning Off SUID and SGID in Mounted Filesystems](#)
 -nosuid option : [5.5.5. Turning Off SUID and SGID in Mounted Filesystems](#)
mounted filesystems : [5.5.5. Turning Off SUID and SGID in Mounted Filesystems](#)
mounting filesystem : (see [directories](#))
mrand48 function : [23.7.3. drand48 \(\), lrand48 \(\), and mrand48 \(\)](#)
mtime
 [5.1.2. Inodes](#)
 [5.1.5. File Times](#)
 [9.2.2. Checklists and Metadata](#)
 [24.4.1.6. Changes to startup files](#)
MUDs (Multiuser Dungeons) : [17.3.23. Other TCP Ports: MUDs and Internet Relay Chat \(IRC\)](#)
Muffet, Alec : [10.5.3.1. Beware false log entries](#)
multicast groups : [16.2.1.2. Classical network addresses](#)
MULTICS (Multiplexed Information and Computing Service) : [1.3. History of UNIX](#)
multilevel security
 [1.3. History of UNIX](#)
 [2.4.4.7. Defend in depth](#)
 [2.5.3. Final Words: Risk Management Means Common Sense](#)
 [17.2. Controlling Access to Servers](#)
multitasking
 [1.4. Security and UNIX](#)
 [C.1.3.3. Process priority and niceness](#)
multiuser operating systems : [1.4. Security and UNIX](#)
multiuser workstations : [17.3.21.1. /etc/fstab and /etc/logindevperm](#)
munitions export : [26.4.1. Munitions Export](#)
MX record type : [17.3.6. Domain Name System \(DNS\) \(TCP and UDP Port 53\)](#)
MYNAME= command : [15.5.2. Permissions Commands](#)

[Copyright](#) © 1999 [O'Reilly & Associates, Inc.](#) All Rights Reserved.

[[Library Home](#) | [DNS & BIND](#) | [TCP/IP](#) | [sendmail](#) | [sendmail Reference](#) | [Firewalls](#) | [Practical Security](#)]



Practical UNIX & Internet Security

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

Index: N

name service

[16.2.6. Name Service](#)

[16.2.6.2. Other naming services](#)

security and : [16.3.2. Security and Nameservice](#)

name-value pairs in BNU UUCP : [15.5.1.2. Name-value pairs](#)

named daemon : [16.2.6.1. DNS under UNIX](#)

named nameserver : [17.3.6.2. DNS nameserver attacks](#)

named-xfer program : [16.2.6.1. DNS under UNIX](#)

named.boot file

[17.3.6.1. DNS zone transfers](#)

[17.3.6.2. DNS nameserver attacks](#)

names

choosing UUCP : [15.5.2. Permissions Commands](#)

computer

[16.2.3. Hostnames](#)

[16.2.3.1. The /etc/hosts file](#)

user : (see [usernames](#))

nameserver attacks, DNS : [17.3.6.2. DNS nameserver attacks](#)

nameserver cache loading : [16.3.2. Security and Nameservice](#)

NASA

Ames Research Center : [F.3.4.22. NASA: Ames Research Center](#)

NASA: Goddard Space Flight Center : [F.3.4.23. NASA: Goddard Space Flight Center](#)

National Aeronautical Space Agency : (see [NASA](#))

National Computer Security Center (NCSC) : [F.2.1. National Institute of Standards and Technology \(NIST\)](#)

National Institute of Standards and Technology : (see [NIST](#))

National Science Foundation Network : (see [networks, NFSNET](#))

national security : [26.2.2. Federal Jurisdiction](#)

natural disasters

[1.1. What Is Computer Security?](#)

[7.1.1.1. A taxonomy of computer failures](#)

[7.1.6.1. Physical security for backups](#)

[12.2.1.1. Fire](#)

(see also [physical security](#))
accidents : [12.2.2. Preventing Accidents](#)
earthquakes : [12.2.1.4. Earthquake](#)
fires
 [12.2.1.1. Fire](#)
 [12.2.1.2. Smoke](#)
lightning
 [12.2. Protecting Computer Hardware](#)
 [12.2.1.9. Lightning](#)
natural gas : [12.2.1.5. Explosion](#)
Naval Computer Incident Response Team (NAVCIRT) : [F.3.4.44. U.S. Department of the Navy](#)
ncheck command : [5.5.4.1. The ncheck command](#)
 -s option
 [5.5.4.1. The ncheck command](#)
 [5.6. Device Files](#)
NCSA HTTPD server : [10.3.5. access_log Log File](#)
NCSA server : (see [Web servers](#))
NCSC (National Computer Security Center) : [F.2.1. National Institute of Standards and Technology \(NIST\)](#)
needxpnhelo (sendmail) : [17.3.4.3. Improving the security of Berkeley sendmail V8](#)
needmailhelo (sendmail) : [17.3.4.3. Improving the security of Berkeley sendmail V8](#)
needvrfyhelo (sendmail) : [17.3.4.3. Improving the security of Berkeley sendmail V8](#)
nested directories : [25.2.2.8. Tree-structure attacks](#)
Netgroup table (NIS+) : [19.5.3. NIS+ Tables](#)
netgroups, NIS
 [19.4.4. NIS Netgroups](#)
 [19.4.4.6. NIS is confused about "+"](#)
 limiting imported accounts : [19.4.4.2. Using netgroups to limit the importing of accounts](#)
NetInfo
 [3.2.2. The /etc/passwd File and Network Databases](#)
 [16.2.6.2. Other naming services](#)
Netmasks table (NIS+) : [19.5.3. NIS+ Tables](#)
netnews~firewalls : [21.4.3. Netnews](#)
.netrc file : [10.4.3. Network Setup](#)

Netscape Navigator

encryption system of : [18.4.1. Eavesdropping Over the Wire](#)

random number generator : [23.8. Picking a Random Seed](#)

netstat command

[17.5. Monitoring Your Network with netstat](#)

[24.2.1. Catching One in the Act](#)

[24.2.4. Tracing a Connection](#)

-a option : [17.5. Monitoring Your Network with netstat](#)

-n option : [17.5. Monitoring Your Network with netstat](#)

network connections : [17.3.3. TELNET \(TCP Port 23\)](#)

network databases : [3.2.2. The /etc/passwd File and Network Databases](#)

Network Filesystem : (see [NFS](#))

network filesystems : [5.5.5. Turning Off SUID and SGID in Mounted Filesystems](#)

Network Information Center (NIC) : [24.2.4.2. How to contact the system administrator of a computer you don't know](#)

Network Information System : (see [NIS](#))

Network News Transport Protocol : (see [NNTP](#))

network providers : [27.2.6. Network Providers that Network Too Well](#)

network services

[17. TCP/IP Services](#)

[17.7. Summary](#)

[23.3. Tips on Writing Network Programs](#)

DNS : (see [DNS](#))

encryption with : [17.4. Security Implications of Network Services](#)

finger : (see [finger command](#))

FTP : (see [FTP](#))

NNTP : (see [NNTP](#))

NTP : (see [NTP](#))

passwords for : [17.4. Security Implications of Network Services](#)

POP : (see [POP](#))

root account with : [17.4. Security Implications of Network Services](#)

securing : [19.1. Securing Network Services](#)

SMTP : (see [SMTP](#))

SNMP : (see [SNMP](#))

spoofing : [17.5. Monitoring Your Network with netstat](#)

systat : [17.3.1. systat \(TCP Port 11\)](#)

table of : [G. Table of IP Services](#)

Telnet : (see [Telnet utility](#))

TFTP : (see [TFTP](#))
UUCP over TCP : [17.3.20. UUCP over TCP \(TCP Port 540\)](#)
Network Time Protocol : (see [NTP](#))
network weaving : [16.1.1.1. Who is on the Internet?](#)
networks
 10Base-T : [12.3.1.2. Eavesdropping by Ethernet and 10Base-T](#)
 allowing threats from : [11.4. Entry](#)
 ARPANET : [16.1.1. The Internet](#)
 backing up
 [7.2.2. Small Network of Workstations and a Server](#)
 [7.2.4. Large Service-Based Networks with Large Budgets](#)
 backups across : [7.4.5. Backups Across the Net](#)
 cables for : [12.2.4.2. Network cables](#)
 checklist for
 [A.1.1.15. Chapter 16: TCP/IP Networks](#)
 [A.1.1.16. Chapter 17: TCP/IP Services](#)
 configuration files : [10.4.3. Network Setup](#)
 connectors for : [12.2.4.3. Network connectors](#)
 cutting cables : [25.1. Destructive Attacks](#)
 denial of service on
 [25.3. Network Denial of Service Attacks](#)
 [25.3.4. Clogging](#)
 disabling physically : [25.3.3. Signal Grounding](#)
 Internet : [16.1.1. The Internet](#)
 LANs : (see [LANs](#))
 logging across : [10.5.2.2. Logging across the network](#)
 logging services of : [10.3.6. Logging Network Services](#)
 MANs : [16.1. Networking](#)
 mobile computing : [8.7. One-Time Passwords](#)
 monitoring with netstat : [17.5. Monitoring Your Network with netstat](#)
 NFSNET : [16.1.1. The Internet](#)
 packet-switching : [16.2. IPv4: The Internet Protocol Version 4](#)
 scanning : [17.6. Network Scanning](#)
 security references : [D.1.8. Network Technology and Security](#)
 services for : [11.1.2. Back Doors and Trap Doors](#)
 sniffers : [16.3. IP Security](#)
 spoofed connection : [8.5.3.1. Trusted path](#)
 TCP/IP : (see [TCP/IP, networks](#))
 UNIX and : [16.1.2. Networking and UNIX](#)

UUCP over : [15.8. UUCP Over Networks](#)
WANs : [16.1. Networking](#)
Networks table (NIS+) : [19.5.3. NIS+ Tables](#)
networks, computer : [1.4.3. Add-On Functionality Breeds Problems](#)
Neumann, Peter : [1.3. History of UNIX](#)
newgrp command : [4.1.3.2. Groups and older AT&T UNIX](#)
newkey -u command
 [19.3.2.1. Creating passwords for users](#)
 [19.5.4.2. When a user's passwords don't match](#)
news : (see [Usenet](#))
news (user) : [4.1. Users and Groups](#)
newsgroups, defamation/harassment via : [26.4.7. Harassment, Threatening Communication, and Defamation](#)
NEXTSTEP Window Server (NSWS) : [17.3.16. NEXTSTEP Window Server \(NSWS\) \(TCP Port 178\)](#)
NFS (Network Filesystem) : [19. RPC, NIS, NIS+, and Kerberos authentication and](#)
 [19.2.2. RPC Authentication](#)
 [19.2.2.4. AUTH_KERB](#)
checklist for : [A.1.1.19. Chapter 20: NFS](#)
file permissions : [5.1.7. File Permissions in Detail](#)
find command on : [5.5.4. Finding All of the SUID and SGID Files](#)
-local option : [11.6.1.2. Writable system files and directories](#)
MOUNT : [20.1.1. NFS History](#)
Secure NFS : (see [Secure NFS](#))
server, and UUCP : [15.3. UUCP and Security](#)
technical description of : [20.1.1. NFS History](#)
and trusted hosts : [17.3.18.2. The problem with trusted hosts](#)
-xdev option : [11.6.1.2. Writable system files and directories](#)
NIC (Network Information Center) : [24.2.4.2. How to contact the system administrator of a computer you don't know](#)
nice command : [25.2.1.2. System overload attacks](#)
nice numbers : [C.1.3.3. Process priority and niceness](#)
NIS (Network Information Service)
 + in
 [19.4. Sun's Network Information Service \(NIS\)](#)
 [19.4.4.6. NIS is confused about "+"](#)
clients : [19.4. Sun's Network Information Service \(NIS\)](#)
domains : [19.4.3. NIS Domains](#)

maps : [19.4. Sun's Network Information Service \(NIS\)](#)

netgroups

[19.4.4. NIS Netgroups](#)

[19.4.4.6. NIS is confused about "+"](#)

limiting imported accounts : [19.4.4.2. Using netgroups to limit the importing of accounts](#)

Secure RPC with

[19.3.2. Setting Up Secure RPC with NIS](#)

[19.3.4. Limitations of Secure RPC](#)

spoofing : [19.4.4.5. Spoofing NIS](#)

UDP : [16.2.4.3. UDP](#)

Yellow Pages : [16.2.6.2. Other naming services](#)

NIS (Network Information System)

[3.2.2. The /etc/passwd File and Network Databases](#)

[3.4. Changing Your Password](#)

[19. RPC, NIS, NIS+, and Kerberos](#)

[19.4. Sun's Network Information Service \(NIS\)](#)

[19.4.5. Unintended Disclosure of Site Information with NIS](#)

NIS+

[3.2.2. The /etc/passwd File and Network Databases](#)

[3.4. Changing Your Password](#)

[16.2.6.2. Other naming services](#)

[19.5. Sun's NIS+](#)

[19.5.5. NIS+ Limitations](#)

integrity-checking software for : [19.5.5. NIS+ Limitations](#)

principals : [19.5.1. What NIS+ Does](#)

Secure RPC with

[19.3.2. Setting Up Secure RPC with NIS](#)

[19.3.4. Limitations of Secure RPC](#)

nisaddcred command : [19.3.1.1. Proving your identity](#)

niscat command : [3.2.2. The /etc/passwd File and Network Databases](#)

nischown command : [19.5.4. Using NIS+](#)

nispasswd command

[3.4. Changing Your Password](#)

[19.5.4. Using NIS+](#)

[19.5.4.2. When a user's passwords don't match](#)

NIST (National Institute of Standards and Technology)

[F.2.1. National Institute of Standards and Technology \(NIST\)](#)

[F.3.4.26. NIST \(National Institute of Standards and Technology\)](#)

NNTP (Network News Transport Protocol) : [17.3.13. Network News Transport Protocol \(NNTP\) \(TCP Port 119\)](#)

nobody (user)

[4.1. Users and Groups](#)

[19.3.2.1. Creating passwords for users](#)

noexpn (sendmail) : [17.3.4.3. Improving the security of Berkeley sendmail V8](#)

noise, electrical : [12.2.1.8. Electrical noise](#)

nonadaptive modems : (see [modems](#))

nonblocking systems : [19.2. Sun's Remote Procedure Call \(RPC\)](#)

nonce : [23.3. Tips on Writing Network Programs](#)

nonrepudiation : [6.5. Message Digests and Digital Signatures](#)

NORDUNET : [F.3.4.27. NORDUNET: Denmark, Sweden, Norway, Finland, Iceland](#)

NOREAD= command : [15.5.2. Permissions Commands](#)

Northwestern University : [F.3.4.28. Northwestern University](#)

nosuid : [11.1.2. Back Doors and Trap Doors](#)

Novell : [1.3. History of UNIX](#)

novrify (sendmail) : [17.3.4.3. Improving the security of Berkeley sendmail V8](#)

Nowitz, David : [15.2. Versions of UUCP](#)

NOWRITE= command : [15.5.2. Permissions Commands](#)

npasswd package : [8.8.2. Constraining Passwords](#)

NPROC variable : [25.2.1.1. Too many processes](#)

NSA (National Security Agency) : [F.2.2. National Security Agency \(NSA\)](#)

NSWS (NextStep Window Server) : [17.3.16. NEXTSTEP Window Server \(NSWS\) \(TCP Port 178\)](#)

NTP (Network Time Protocol) : [17.3.14. Network Time Protocol \(NTP\) \(UDP Port 123\)](#)

Secure RPC and : [19.3.1.3. Setting the window](#)

NU-CERT : [F.3.4.28. Northwestern University](#)

null device : [5.6. Device Files](#)

nuucp account

[15.1.4. How the UUCP Commands Work](#)

[15.3.1. Assigning Additional UUCP Logins](#)

[15.4.1.3. Format of USERFILE entry without system name](#)

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

[Copyright](#) © 1999 [O'Reilly & Associates, Inc.](#) All Rights Reserved.

[[Library Home](#) | [DNS & BIND](#) | [TCP/IP](#) | [sendmail](#) | [sendmail Reference](#) | [Firewalls](#) | [Practical Security](#)]



Practical UNIX & Internet Security

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

Index: O

obscurity : (see [security, through obscurity](#))

octal file permissions

[5.2.3. Calculating Octal File Permissions](#)

[5.2.4. Using Octal File Permissions](#)

octets : [16.2.1. Internet Addresses](#)

Odlyzko, Andrew : [19.3.4. Limitations of Secure RPC](#)

OFB (output feedback) : [6.4.4.2. DES modes](#)

on-the-job security

[13.2. On the Job](#)

[13.2.6. Departure](#)

one : [9.2.1. Comparison Copies](#)

one-command accounts : [8.1.3. Accounts That Run a Single Command](#)

one-time pad encryption

[6.4.7. An Unbreakable Encryption Algorithm](#)

[8.7.3. Code Books](#)

one-time passwords

[3.7. One-Time Passwords](#)

[8.7. One-Time Passwords](#)

[8.7.3. Code Books](#)

[17.4. Security Implications of Network Services](#)

[23.3. Tips on Writing Network Programs](#)

one-way phone lines : [14.4.1. One-Way Phone Lines](#)

open access, tradition of : [1.4.1. Expectations](#)

open accounts

[8.1.4. Open Accounts](#)

[8.1.4.6. Potential problems with rsh](#)

[8.8.7. Algorithm and Library Changes](#)

open command : [23.2. Tips on Avoiding Security-related Bugs](#)

O_CREAT and O_EXCL flags : [23.2. Tips on Avoiding Security-related Bugs](#)

Open Software Distribution (OSD) : [Preface](#)

Open Software Foundation (OSF) : [1.3. History of UNIX](#)

open system call : [5.1.7. File Permissions in Detail](#)

Open System Interconnection (OSI) : [16.4.4. OSI](#)

opendir library call : [5.4. Using Directory Permissions](#)

operating systems

[1.2. What Is an Operating System?](#)

[12.3.3. Other Media](#)

keeping secret : [2.5. The Problem with Security Through Obscurity](#)

operating systems

[Which UNIX System?](#)

(see also under specific name)

optic cables : (see [cables, network](#))

optical vampire taps : [12.3.1.5. Fiber optic cable](#)

Options command : [18.3.2. Commands Within the <Directory> Block](#)

Orange Book : [2.3.3. Adding Up the Numbers](#)

originate mode : [14.3.1. Originate and Answer](#)

originate testing : [14.5.3.1. Originate testing](#)

OSF (Open Software Foundation) : [1.3. History of UNIX](#)

OSF/1 operating system : [1.3. History of UNIX](#)

OSI (Open System Interconnection) : [16.4.4. OSI](#)

Outcome table (NIS+) : [19.5.3. NIS+ Tables](#)

outgoing calls : [14.5. Modems and UNIX](#)

outgoing mail, logging : [10.4.2. Mail](#)

output feedback (OFB) : [6.4.4.2. DES modes](#)

outsiders : [13.3. Outsiders](#)

overload attacks

[25.2. Overload Attacks](#)

[25.2.5. Soft Process Limits: Preventing Accidental Denial of Service](#)

overtime : [13.2.3. Performance Reviews and Monitoring](#)

overwriting media : [12.3.2.3. Sanitize your media before disposal](#)

OW- (sendmail.cf) : [17.3.4.2. Using sendmail to receive email](#)

owners of information : [2.4.4.1. Assign an owner](#)

owners, changing : [5.7. chown: Changing a File's Owner](#)

ownership notices : [26.2.6. Other Tips](#)

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

[Copyright](#) © 1999 [O'Reilly & Associates, Inc.](#) All Rights Reserved.

[[Library Home](#) | [DNS & BIND](#) | [TCP/IP](#) | [sendmail](#) | [sendmail Reference](#) | [Firewalls](#) | [Practical Security](#)]



Practical UNIX & Internet Security

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

Index: P

pacct file : [10.2. The acct/pacct Process Accounting File](#)

pack program : [6.6.1.2. Ways of improving the security of crypt](#)

packet sniffing : [16.3.1. Link-level Security](#)

packet-switching networks : [16.2. IPv4: The Internet Protocol Version 4](#)

packets : (see [IP packets](#))

paper

backups on : [24.5.1. Never Trust Anything Except Hardcopy](#)

copies : [7.3.2. Building an Automatic Backup System](#)

logging on : [10.7. Handwritten Logs](#)

shredders for : [12.3.3. Other Media](#)

throwing out : [12.3.3. Other Media](#)

parent processes : [C.2. Creating Processes](#)

partitions : [25.2.2.4. Using partitions to protect your users](#)

backup by : [7.1.3. Types of Backups](#)

root : (see [root directory](#))

pass phrases : (see [passwords](#))

pass phrases for PGP

[6.6.3.1. Encrypting files with IDEA](#)

(see also [passwords](#))

passive FTP

[17.3.2.2. Passive vs. active FTP](#)

[17.3.2.3. FTP passive mode](#)

passwd command

[3.4. Changing Your Password](#)

[8.6.2. What Is Salt?](#)

as SUID program : [5.5. SUID](#)

-l option

[8.4.1. Changing an Account's Password](#)

[8.8.8. Disabling an Account by Changing Its Password](#)

-n option : [8.8.6. Password Aging and Expiration](#)

-x option : [8.8.6. Password Aging and Expiration](#)

-f nomemory option : [3.5. Verifying Your New Password](#)

using as superuser : [3.5. Verifying Your New Password](#)

passwd file

[1.2. What Is an Operating System?](#)

[3.2.1. The /etc/passwd File](#)

[3.2.2. The /etc/passwd File and Network Databases](#)

[4.2.3. Impact of the /etc/passwd and /etc/group Files on Security](#)

[7.1.2. What Should You Back Up?](#)

[8.1.1. Accounts Without Passwords](#)

[8.6. The UNIX Encrypted Password System](#)

[15.1.4. How the UUCP Commands Work](#)

[24.4.1. New Accounts](#)

[C.5.1. Process #1: /etc/init](#)

(see [/etc/passwd file](#))

Passwd table (NIS+) : [19.5.3. NIS+ Tables](#)

passwd+ package

[8.8.2. Constraining Passwords](#)

[8.8.4. Password Generators](#)

password coach : [8.8.4. Password Generators](#)

password file : [19.4.4.6. NIS is confused about "+"](#)

password modems : [14.6. Additional Security for Modems](#)

password.adjunct file : [8.8.5. Shadow Password Files](#)

passwords

[3.2. Passwords](#)

[3.6.1. Bad Passwords: Open Doors](#)

[3.8. Summary](#)

[23.5. Tips on Using Passwords](#)

accounts without : [8.1.1. Accounts Without Passwords](#)

assigning to users : [8.8.1. Assigning Passwords to Users](#)

avoiding conventional

[8.8. Administrative Techniques for Conventional Passwords](#)

[8.8.9. Account Names Revisited: Using Aliases for Increased Security](#)

bad choices for

[3.6.1. Bad Passwords: Open Doors](#)

[3.6.4. Passwords on Multiple Machines](#)

changing

[3.4. Changing Your Password](#)

[3.5. Verifying Your New Password](#)

[8.4.1. Changing an Account's Password](#)

[8.8.8. Disabling an Account by Changing Its Password](#)

checklist for : [A.1.1.2. Chapter 3: Users and Passwords](#)

constraining : [8.8.2. Constraining Passwords](#)

conventional : [3.2.6. Conventional UNIX Passwords](#)
cracking

[8.6.1. The crypt\(\) Algorithm](#)

[8.8.3. Cracking Your Own Passwords](#)

[8.8.3.2. The dilemma of password crackers](#)

[17.3.3. TELNET \(TCP Port 23\)](#)

encrypting

[8.6. The UNIX Encrypted Password System](#)

[8.6.4. Crypt16\(\) and Other Algorithms](#)

expiring : [8.8.6. Password Aging and Expiration](#)

federal jurisdiction over : [26.2.2. Federal Jurisdiction](#)

FTP and : [17.3.2. \(FTP\) File Transfer Protocol \(TCP Ports 20 and 21\)](#)

generators of : [8.8.4. Password Generators](#)

hit lists of : [3.6.1. Bad Passwords: Open Doors](#)

Kerberos : [19.6.5. Kerberos Limitations](#)

logging changes to : [10.7.2.1. Exception and activity reports](#)

logging failed attempts at : [10.5.3. syslog Messages](#)

for MUDs : [17.3.23. Other TCP Ports: MUDs and Internet Relay Chat \(IRC\)](#)

on multiple machines

[3.6.4. Passwords on Multiple Machines](#)

[3.6.5. Writing Down Passwords](#)

over network connections : [23.3. Tips on Writing Network Programs](#)

with network services : [17.4. Security Implications of Network Services](#)

NIS, with Secure RPC : [19.3.2.1. Creating passwords for users](#)

NIS+, changing : [19.5.4.1. Changing your password](#)

one-time

[3.7. One-Time Passwords](#)

[8.7. One-Time Passwords](#)

[8.7.3. Code Books](#)

[17.4. Security Implications of Network Services](#)

with POP : [17.3.10. Post Office Protocol \(POP\) \(TCP Ports 109 and 110\)](#)

required for Web use

[18.3.2. Commands Within the <Directory> Block](#)

[18.3.3. Setting Up Web Users and Passwords](#)

shadow

[8.4.1. Changing an Account's Password](#)

[8.8.5. Shadow Password Files](#)

sniffing

[1.4.3. Add-On Functionality Breeds Problems](#)

[3. Users and Passwords](#)

[8.7. One-Time Passwords](#)

system clock and : [17.3.14. Network Time Protocol \(NTP\) \(UDP Port 123\)](#)

token cards with : [8.7.2. Token Cards](#)

unique, number of : [3.6.3. Good Passwords: Locked Doors](#)

usernames as : [8.8.3.1. Joetest: a simple password cracker](#)

UUCP accounts : [15.3.2. Establishing UUCP Passwords](#)

verifying new : [3.5. Verifying Your New Password](#)

wizard's (sendmail) : [17.3.4.1. sendmail and security](#)

writing down : [3.6.5. Writing Down Passwords](#)

patches, logging : [10.7.2.2. Informational material](#)

patents : [26.4.4. Patent Concerns](#)

and cryptography : [6.7.1. Cryptography and the U.S. Patent System](#)

PATH variable

[8.1.4.1. Restricted shells under System V UNIX](#)

[8.1.4.6. Potential problems with rsh](#)

[23.4. Tips on Writing SUID/SGID Programs](#)

attacks via : [11.5.1.1. PATH attacks](#)

pathnames : [23.2. Tips on Avoiding Security-related Bugs](#)

paths : [5.1.3. Current Directory and Paths](#)

trusted : [8.5.3.1. Trusted path](#)

pax program : [7.4.2. Simple Archives](#)

PCERT (Purdue University) : [F.3.4.30. Purdue University](#)

PCs

viruses on : [11.1.5. Viruses](#)

web server on : [18.2. Running a Secure Server](#)

PDP-11 processors

[1.3. History of UNIX](#)

[8.6.1. The crypt\(\) Algorithm](#)

Penn State response team : [F.3.4.29. Pennsylvania State University](#)

per-machine logs : [10.7.2. Per-Machine Logs](#)

per-site logs : [10.7.1. Per-Site Logs](#)

performance

compromised

[25.2.1. Process-Overload Problems](#)

[25.2.1.2. System overload attacks](#)

reviews : [13.2.3. Performance Reviews and Monitoring](#)

with Secure RPC : [19.3.4. Limitations of Secure RPC](#)

using FFS : [25.2.2.6. Reserved space](#)
perimeter, security : [12.1.1. The Physical Security Plan](#)
perl command
-T option
 [18.2.3.4. Tainting with Perl](#)
 [23.4. Tips on Writing SUID/SGID Programs](#)
Perl programming language
 [5.5.3. SUID Shell Scripts](#)
 [11.1.4. Trojan Horses](#)
 [11.5.1.2. IFS attacks](#)
random seed generator : [23.9. A Good Random Seed Generator](#)
script for reading lastlog file : [10.1.1. lastlog File](#)
Swatch program
 [10.6. Swatch: A Log File Tool](#)
 [10.6.2. The Swatch Configuration File](#)
 [E.4.9. Swatch](#)
tainting facility : [18.2.3.4. Tainting with Perl](#)
permissions
 [1.1. What Is Computer Security?](#)
 [5.1.6. Understanding File Permissions](#)
 [5.2.4. Using Octal File Permissions](#)
 [11.1.5. Viruses](#)
 [11.6.1. File Protections](#)
 [11.6.1.3. World-readable backup devices](#)
access control lists (ACLs)
 [5.2.5. Access Control Lists](#)
 [5.2.5.2. HP-UX access control lists](#)
changing
 [5.2.1. chmod: Changing a File's Permissions](#)
 [5.2.4. Using Octal File Permissions](#)
directory : [5.4. Using Directory Permissions](#)
/etc/utmp file : [10.1.2. utmp and wtmp Files](#)
intruder's modifications to : [24.4.1.2. Changes in file and directory protections](#)
modem devices : [14.5.2. Setting Up the UNIX Device](#)
modem files : [14.5.1. Hooking Up a Modem to Your Computer](#)
of NIS+ objects : [19.5.5. NIS+ Limitations](#)
octal
 [5.2.3. Calculating Octal File Permissions](#)

[5.2.4. Using Octal File Permissions](#)
of .rhosts file : [17.3.18.4. The ~/.rhosts file](#)
SUID programs
[5.5. SUID](#)
[5.5.7. SGID Bit on Files \(System V UNIX Only\): Mandatory Record Locking](#)
symbolic links and : [5.1.7. File Permissions in Detail](#)
umasks
[5.3. The umask](#)
[5.3.2. Common umask Values](#)
UUCP : [15.4.1.4. Special permissions](#)
Permissions file
[15.5. Security in BNU UUCP](#)
[15.5.1. Permissions File](#)
[15.5.3. uucheck: Checking Your Permissions File](#)
checking with uucheck : [15.5.3. uucheck: Checking Your Permissions File](#)
personnel : (see [employees](#))
PGP (Pretty Good Privacy)
[6.6.3. PGP: Pretty Good Privacy](#)
[6.6.3.6. PGP detached signatures](#)
-eat and -seat options : [6.6.3.3. Encrypting a message](#)
encrypting message with : [6.6.3.3. Encrypting a message](#)
encrypting Web documents : [18.4.1. Eavesdropping Over the Wire](#)
-ka option : [6.6.3.2. Creating your PGP public key](#)
-kg option : [6.6.3.2. Creating your PGP public key](#)
-kvc option : [6.6.3.6. PGP detached signatures](#)
-kxaf option : [6.6.3.2. Creating your PGP public key](#)
-o option : [6.6.3.6. PGP detached signatures](#)
-sat option : [6.6.3.4. Adding a digital signature to an announcement](#)
-sb option : [6.6.3.6. PGP detached signatures](#)
software signature : [E.4. Software Resources](#)
ph (phonebook) server : [17.3.8.3. Replacing finger](#)
phantom mail : [17.3.4.2. Using sendmail to receive email](#)
physical security
[12. Physical Security](#)
[12.4.2. "Nothing to Lose?"](#)
access control : [12.2.3. Physical Access](#)
of backups
[7.1.6. Security for Backups](#)

[7.1.6.3. Data security for backups](#)

checklist for : [A.1.1.11. Chapter 12: Physical Security](#)
modems

[14.5.4. Physical Protection of Modems](#)

[14.6. Additional Security for Modems](#)

read-only filesystems : [9.1.2. Read-only Filesystems](#)

signal grounding : [25.3.3. Signal Grounding](#)

PIDs (process IDs)

[C.1.3.1. Process identification numbers \(PID\)](#)

[C.1.3.4. Process groups and sessions](#)

Pieprzyk, Josef : [6.5.4.3. HAVAL](#)

PingWare program : [17.6.3. PingWare](#)

pipe (in Swatch program) : [10.6.2. The Swatch Configuration File](#)

pipes

[18.2.3.2. Testing is not enough!](#)

[18.2.3.3. Sending mail](#)

pipes (for smoking) : [12.2.1.2. Smoke](#)

piracy of software

[26.4.2.1. Software piracy and the SPA](#)

(see also [software](#))

pirated software : (see [software](#))

plaintext attacks : [6.2.3. Cryptographic Strength](#)

.plan file : [17.3.8.1. The .plan and .project files](#)

platforms : (see [operating systems](#))

play accounts : (see [open accounts](#))

playback attacks : [19.6.1.2. Using the ticket granting ticket](#)

plus sign (+)

in hosts.equiv file : [17.3.18.5. Searching for .rhosts files](#)

in NIS

[19.4. Sun's Network Information Service \(NIS\)](#)

[19.4.4.6. NIS is confused about "+"](#)

Point-to-Point Protocol (PPP) : [14.5. Modems and UNIX](#)

policy, security

[1.2. What Is an Operating System?](#)

[2. Policies and Guidelines](#)

[2.5.3. Final Words: Risk Management Means Common Sense](#)

[A.1.1.1. Chapter 2: Policies and Guidelines](#)

cost-benefit analysis

[2.3. Cost-Benefit Analysis](#)

[2.3.4. Convincing Management](#)

risk assessment

[2.2. Risk Assessment](#)

[2.2.2. Review Your Risks](#)

[2.5.3. Final Words: Risk Management Means Common Sense](#)

role of

[2.4.1. The Role of Policy](#)

[2.4.4. Some Key Ideas in Developing a Workable Policy](#)

[2.4.4.7. Defend in depth](#)

politics : [11.3. Authors](#)

polyalphabetic ciphers : [6.3. The Enigma Encryption System](#)

polygraph tests : [13.1. Background Checks](#)

POP (Post Office Protocol) : [17.3.10. Post Office Protocol \(POP\) \(TCP Ports 109 and 110\)](#)

popen function

[18.2.3.2. Testing is not enough!](#)

[23.2. Tips on Avoiding Security-related Bugs](#)

pornography : [26.4.5. Pornography and Indecent Material](#)

port numbers

[23.3. Tips on Writing Network Programs](#)

[G. Table of IP Services](#)

portable computers : [12.2.6.3. Portables](#)

portable I/O library : [1.3. History of UNIX](#)

portmap service

[19.2.1. Sun's portmap/rpcbind](#)

[19.4.4.4. Spoofing RPC](#)

[E.4.6. portmap](#)

portmapper program

[17.3.11. Sun RPC's portmapper \(UDP and TCP Ports 111\)](#)

[19.2.1. Sun's portmap/rpcbind](#)

[19.4.5. Unintended Disclosure of Site Information with NIS](#)

ports

[16.2.4.2. TCP](#)

[17.1.1. The /etc/services File](#)

[G. Table of IP Services](#)

trusted : (see [trusted](#), [ports](#))

positivity : [2.4.4.2. Be positive](#)

POSIX

[1.3. History of UNIX](#)

[1.4.2. Software Quality](#)
[C.1.3.4. Process groups and sessions](#)
chown command and : [5.7. chown: Changing a File's Owner](#)
Post Office Protocol : (see [POP](#))
postmaster, contacting : [24.2.4.2. How to contact the system administrator of a computer you don't know](#)
PostScript files : [11.1.5. Viruses](#)
power outages, logging : [10.7.1.1. Exception and activity reports](#)
power surges
[12.2. Protecting Computer Hardware](#)
[12.2.1.8. Electrical noise](#)
(see also [lightning](#))
PPP (Point-to-Point Protocol)
[14.5. Modems and UNIX](#)
[16.2. IPv4: The Internet Protocol Version 4](#)
preserve program : [5.5.3.2. Another SUID example: IFS and the /usr/lib/preserve hole](#)
Pretty Good Privacy : (see [PGP](#))
prevention, cost of
[2.3. Cost-Benefit Analysis](#)
[2.3.4. Convincing Management](#)
primary group : [4.1.3. Groups and Group Identifiers \(GIDs\)](#)
principals, NIS+ : [19.5.1. What NIS+ Does](#)
print through process : [12.3.2.1. Verify your backups](#)
printers
 buffers : [12.3.4.1. Printer buffers](#)
 /etc/hosts.lpd file : [17.3.18.6. /etc/hosts.lpd file](#)
 logging to : [10.5.2.1. Logging to a printer](#)
 output from : [12.3.4.2. Printer output](#)
 ports for : [12.3.1.4. Auxiliary ports on terminals](#)
priority of processes : [C.1.3.3. Process priority and niceness](#)
privacy
 [2.1. Planning Your Security Needs](#)
 [2.5.2. Confidential Information](#)
 [9. Integrity Management](#)
 [12.3. Protecting Data](#)
 [12.3.6. Key Switches](#)
 (see also [encryption](#); [integrity](#))
 Electronic Communications Privacy Act (ECPA) : [26.2.3. Federal](#)

[Computer Crime Laws](#)

Secure RPC : [19.3.4. Limitations of Secure RPC](#)

private-key cryptography

[6.4. Common Cryptographic Algorithms](#)

[6.4.1. Summary of Private Key Systems](#)

privilege testing (modem) : [14.5.3.3. Privilege testing](#)

privileges, file : (see [permissions](#))

privileges, SUID : (see [SUID/SGID programs](#))

processes

[C.1. About Processes](#)

[C.5.3. Running the User's Shell](#)

accounting

[10.2. The acct/pacct Process Accounting File](#)

[10.2.3. messages Log File](#)

group IDs

[4.3.3. Other IDs](#)

[C.1.3.4. Process groups and sessions](#)

overload attacks

[25.2.1. Process-Overload Problems](#)

[25.2.1.2. System overload attacks](#)

priority of : [C.1.3.3. Process priority and niceness](#)

scheduler : [C.1.3.3. Process priority and niceness](#)

procmail system : [11.5.2.5. .forward, .procmailrc](#)

.procmailrc file : [11.5.2.5. .forward, .procmailrc](#)

.profile file

[8.1.4.1. Restricted shells under System V UNIX](#)

[8.1.4.6. Potential problems with rsh](#)

[11.5.2.1. .login, .profile, /etc/profile](#)

[24.4.1.6. Changes to startup files](#)

programmed threats

[11. Protecting Against Programmed Threats](#)

[11.6.2. Shared Libraries](#)

authors of : [11.3. Authors](#)

checklist for : [A.1.1.10. Chapter 11: Protecting Against Programmed Threats](#)

protection from : [11.5. Protecting Yourself](#)

references on : [D.1.4. Computer Viruses and Programmed Threats](#)

programming : [23. Writing Secure SUID and Network Programs](#)

references for : [D.1.11. UNIX Programming and System Administration](#)

programs

CGI : (see [CGI, scripts](#))

integrity of : (see [integrity, data](#))

for network services : [23.3. Tips on Writing Network Programs](#)

rabbit

[11.1. Programmed Threats: Definitions](#)

[11.1.7. Bacteria and Rabbits](#)

running simultaneously : [23.2. Tips on Avoiding Security-related Bugs](#)

secure : [23. Writing Secure SUID and Network Programs](#)

worms : [11.1.6. Worms](#)

Project Athena : (see [Kerberos system](#))

.project file : [17.3.8.1. The .plan and .project files](#)

proprietary ownership notices : [26.2.6. Other Tips](#)

prosecution, criminal

[26.2. Criminal Prosecution](#)

[26.2.7. A Final Note on Criminal Actions](#)

protocols

[16.2.4. Packets and Protocols](#)

(see also under specific protocol)

IP : (see [IP protocols](#))

Protocols table (NIS+) : [19.5.3. NIS+ Tables](#)

proxies, checklist for : [A.1.1.21. Chapter 22: Wrappers and Proxies](#)

pruning the wtmp file : [10.1.3.1. Pruning the wtmp file](#)

ps command

[6.6.2. des: The Data Encryption Standard](#)

[10.1.2. utmp and wtmp Files](#)

[19.3.2.3. Making sure Secure RPC programs are running on every workstation](#)

[24.2.1. Catching One in the Act](#)

[C.1.2. The ps Command](#)

[C.1.2.2. Listing processes with Berkeley-derived versions of UNIX](#)

with kill command : [24.2.5. Getting Rid of the Intruder](#)

to stop process overload

[25.2.1.1. Too many processes](#)

[25.2.1.2. System overload attacks](#)

pseudo-devices : [5.6. Device Files](#)

pseudorandom functions : [23.6. Tips on Generating Random Numbers](#)

PUBDIR= command : [15.5.2. Permissions Commands](#)

public-key cryptography

[6.4. Common Cryptographic Algorithms](#)
[6.4.2. Summary of Public Key Systems](#)
[6.4.6. RSA and Public Key Cryptography](#)
[6.4.6.3. Strength of RSA](#)
[6.5.3. Digital Signatures](#)
[18.3. Controlling Access to Files on Your Server](#)
[18.6. Dependence on Third Parties](#)
breaking : [19.3.4. Limitations of Secure RPC](#)
PGP : [6.6.3.2. Creating your PGP public key](#)
proving identity with : [19.3.1.1. Proving your identity](#)
publicity hounds : [11.3. Authors](#)
publicizing security holes : [2.5.1. Going Public](#)
publickey file : [19.3.2.1. Creating passwords for users](#)
Purdue University (PCERT) : [F.3.4.30. Purdue University](#)
Purify : [23.2. Tips on Avoiding Security-related Bugs](#)
pwck command : [8.2. Monitoring File Format](#)

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

[Copyright](#) © 1999 [O'Reilly & Associates, Inc.](#) All Rights Reserved.

[[Library Home](#) | [DNS & BIND](#) | [TCP/IP](#) | [sendmail](#) | [sendmail Reference](#) | [Firewalls](#) | [Practical Security](#)]



Practical UNIX & Internet Security

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

Index: Q

quality of software

[1.4.2. Software Quality](#)

[1.4.3. Add-On Functionality Breeds Problems](#)

quantifying threats : [2.2.1.3. Quantifying the threats](#)

quot command : [25.2.2.2. quot command](#)

quotacheck -a command : [25.2.2.5. Using quotas](#)

quotas : [25.2.2.5. Using quotas](#)

on /tmp directory : [25.2.4. /tmp Problems](#)

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

[Copyright](#) © 1999 [O'Reilly & Associates, Inc.](#) All Rights Reserved.

[[Library Home](#) | [DNS & BIND](#) | [TCP/IP](#) | [sendmail](#) | [sendmail Reference](#) | [Firewalls](#) | [Practical Security](#)]



Practical UNIX & Internet Security

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

Index: R

rabbit programs

[11.1. Programmed Threats: Definitions](#)

[11.1.7. Bacteria and Rabbits](#)

race conditions : [23.2. Tips on Avoiding Security-related Bugs](#)

radio

eavesdropping : [12.3.1.3. Eavesdropping by radio and using TEMPEST](#)

transmissions : [14.4.4.1. Kinds of eavesdropping](#)

transmitters : [12.2.1.8. Electrical noise](#)

rain : (see [water](#))

RAM theft : [12.2.6. Preventing Theft](#)

rand function : [23.7.1. rand \(\)](#)

random device : [23.7.4. Other random number generators](#)

random function : [23.7.2. random \(\)](#)

random numbers : [23.6. Tips on Generating Random Numbers](#)

raw devices : [5.6. Device Files](#)

rc directory : [C.5.1. Process #1: /etc/init](#)

RC2, RC4, and RC5 algorithms

[6.4.1. Summary of Private Key Systems](#)

[6.4.8. Proprietary Encryption Systems](#)

RC4 and RC5 algorithms : [6.4.1. Summary of Private Key Systems](#)

rcp command

[1.4.3. Add-On Functionality Breeds Problems](#)

[7.4.5. Backups Across the Net](#)

RCS (Revision Control System)

[7.3.2. Building an Automatic Backup System](#)

[17.3. Primary UNIX Network Services](#)

rdist program

[7.4.5. Backups Across the Net](#)

[9.2.1.3. rdist](#)

rdump/rrestore program : [7.4.5. Backups Across the Net](#)

read permission

[5.1.7. File Permissions in Detail](#)

[5.4. Using Directory Permissions](#)

read system call : [5.1.7. File Permissions in Detail](#)

time-outs on : [23.3. Tips on Writing Network Programs](#)
read-only exporting filesystems : [11.6.1.2. Writable system files and directories](#)
read-only filesystems : [9.1.2. Read-only Filesystems](#)
READ= command : [15.5.2. Permissions Commands](#)
readdir library call : [5.4. Using Directory Permissions](#)
real UIDs/GIDs
 [4.3.1. Real and Effective UIDs](#)
 [C.1.3.2. Process real and effective UID](#)
realpath function : [23.2. Tips on Avoiding Security-related Bugs](#)
reauthentication
 Kerberos : [19.6.4. Using Kerberos](#)
 Secure RPC : [19.3.1.3. Setting the window](#)
Receive Data (RD) : [14.3. The RS-232 Serial Protocol](#)
Redman, Brian E. : [15.2. Versions of UUCP](#)
refer_log file : [18.4.2. Eavesdropping Through Log Files](#)
reflectors (in Enigma system) : [6.3. The Enigma Encryption System](#)
reformatting attack : [25.1. Destructive Attacks](#)
relative humidity : [12.2.1.11. Humidity](#)
relative pathnames : [5.1.3. Current Directory and Paths](#)
remote
 command execution
 [15.1.2. uux Command](#)
 [15.4.3. L.cmds: Providing Remote Command Execution](#)
 [17.3.17. rexec \(TCP Port 512\)](#)
 comparison copies : [9.2.1.2. Remote copies](#)
 computers
 transferring files to : [15.1.1. uucp Command](#)
 file access (UUCP)
 [15.4.1. USERFILE: Providing Remote File Access](#)
 [15.4.2.1. Some bad examples](#)
 network filesystems : [5.5.5. Turning Off SUID and SGID in Mounted Filesystems](#)
 procedure calls : (see [RPCs](#))
remote file
 [10.3.1. aculog File](#)
 [14.5.1. Hooking Up a Modem to Your Computer](#)
remote.unknown file : [15.5. Security in BNU UUCP](#)
renice command
 [25.2.1.2. System overload attacks](#)

[C.1.3.3. Process priority and niceness](#)

replay attacks

[17.3.14. Network Time Protocol \(NTP\) \(UDP Port 123\)](#)

[19.6.1.2. Using the ticket granting ticket](#)

reporting security holes : [2.5.1. Going Public](#)

Request to Send (RTS) : [14.3. The RS-232 Serial Protocol](#)

REQUEST= command

[15.5.1.3. A Sample Permissions file](#)

[15.5.2. Permissions Commands](#)

reserved memory space : [25.2.2.6. Reserved space](#)

resolution, time : [23.8. Picking a Random Seed](#)

resolver library (bind) : [16.2.6.1. DNS under UNIX](#)

resolving (DNS) : [17.3.6. Domain Name System \(DNS\) \(TCP and UDP Port 53\)](#)

response teams

[27.3.5. Response Personnel?](#)

[F.3. Emergency Response Organizations](#)

[F.3.4.46. Westinghouse Electric Corporation](#)

mailing lists for : [E.1.1. Response Teams and Vendors](#)

restore : (see [dump/restore program](#))

restricted

filesystems

[8.1.5. Restricted Filesystem](#)

[8.1.5.2. Checking new software](#)

FTP : [17.3.2.5. Restricting FTP with the standard UNIX FTP server](#)

logins : [8.3. Restricting Logins](#)

shells

[8.1.4.1. Restricted shells under System V UNIX](#)

[8.1.4.6. Potential problems with rsh](#)

su use : [4.3.6. Restricting su](#)

restrictmailq (sendmail) : [17.3.4.3. Improving the security of Berkeley sendmail V8](#)

retention of backups

[7.1.5. How Long Should You Keep a Backup?](#)

[7.2.2.2. Retention schedule](#)

(see also [networks, backing up](#))

return calls : [23.2. Tips on Avoiding Security-related Bugs](#)

reverse lookup

[16.3.2. Security and Nameservice](#)

[23.3. Tips on Writing Network Programs](#)

Revision Control System (RCS)

[7.3.2. Building an Automatic Backup System](#)

[17.3. Primary UNIX Network Services](#)

revocation certificate : [6.6.3.2. Creating your PGP public key](#)

rexed service : [19.2.2.4. AUTH KERB](#)

rexec service : [17.3.17. rexec \(TCP Port 512\)](#)

RFC 1750 : [23.8. Picking a Random Seed](#)

.rhosts file

[10.4.3. Network Setup](#)

[17.3.18.4. The ~/.rhosts file](#)

[17.3.18.5. Searching for .rhosts files](#)

back door in : [11.1.2. Back Doors and Trap Doors](#)

intruder's changes to : [24.4.1.4. Changes in .rhosts files](#)

searching for : [17.3.18.5. Searching for .rhosts files](#)

Ring Indicator (RI) : [14.3. The RS-232 Serial Protocol](#)

RIP (Routing Internet Protocol) : [17.3.19. Routing Internet Protocol \(RIP routed\) \(UDP Port 520\)](#)

risk assessment

[2.2. Risk Assessment](#)

[2.2.2. Review Your Risks](#)

[2.5.3. Final Words: Risk Management Means Common Sense](#)

risks : (see [threats](#))

Ritchie, Dennis : [1.3. History of UNIX](#)

Rivest, Ronald L.

[6.1.3. Modern Controversy](#)

[6.4.1. Summary of Private Key Systems](#)

[6.4.2. Summary of Public Key Systems](#)

[6.4.6. RSA and Public Key Cryptography](#)

[6.5.4.1. MD2, MD4, and MD5](#)

RJE (Remote Job Entry) : [3.2.1. The /etc/passwd File](#)

rlogin command

[1.4.3. Add-On Functionality Breeds Problems](#)

[3.5. Verifying Your New Password](#)

[16.3.2. Security and Nameservice](#)

[17.3.18. rlogin and rsh \(TCP Ports 513 and 514\)](#)

[17.3.18.6. /etc/hosts.lpd file](#)

versus Telnet : [17.3.18. rlogin and rsh \(TCP Ports 513 and 514\)](#)

rlogind command : [17.3.18. rlogin and rsh \(TCP Ports 513 and 514\)](#)

rm command

[5.4. Using Directory Permissions](#)
[15.4.3. L.cmds: Providing Remote Command Execution](#)
and deep tree structures : [25.2.2.8. Tree-structure attacks](#)
rmail program : [15.4.3. L.cmds: Providing Remote Command Execution](#)
root account
[4. Users, Groups, and the Superuser](#)
[4.1. Users and Groups](#)
[4.2.1. The Superuser](#)
[4.2.1.5. The problem with the superuser](#)
[5.5.2. Problems with SUID](#)
(see also [superuser](#))
abilities of : [27.1.3. What the Superuser Can and Cannot Do](#)
chroot
[8.1.5. Restricted Filesystem](#)
[8.1.5.2. Checking new software](#)
immutable files and : [9.1.1. Immutable and Append-Only Files](#)
network services with : [17.4. Security Implications of Network Services](#)
protecting
[8.5. Protecting the root Account](#)
[8.5.3.2. Trusted computing base](#)
on remote machine, fingering : [24.2.4.2. How to contact the system administrator of a computer you don't know](#)
single-command accounts and : [8.1.3. Accounts That Run a Single Command](#)
web server as : [18.2.1. The Server's UID](#)
root directory : [5.1.1. Directories](#)
backups of : [7.1.3. Types of Backups](#)
UUCP access from : [15.4.2.1. Some bad examples](#)
root option for /etc/exports : [20.2.1.1. /etc/exports](#)
ROT13 algorithm
[6.4.1. Summary of Private Key Systems](#)
[6.4.3. ROT13: Great for Encoding Offensive Jokes](#)
rotating backup media
[7.1.3. Types of Backups](#)
[7.2.1.2. Media rotation](#)
routed daemon : [17.3.19. Routing Internet Protocol \(RIP routed\) \(UDP Port 520\)](#)
routers, intelligent : [21.2.3. Setting Up the Choke](#)
routing : [16.2.2. Routing](#)
Routing Internet Protocol : (see [RIP](#))

RPC table (NIS+) : [19.5.3. NIS+ Tables](#)
rpc.rexdserver : [17.3.22. RPC rpc.rexd \(TCP Port 512\)](#)
rpcbind : (see [portmapper program](#))
RPCs (remote procedure calls)
 [17.3.22. RPC rpc.rexd \(TCP Port 512\)](#)
 [19. RPC, NIS, NIS+, and Kerberos](#)
 [19.7.2. SESAME](#)
 authentication of
 [19.2.2. RPC Authentication](#)
 [19.2.2.4. AUTH_KERB](#)
 portmapper program : [17.3.11. Sun RPC's portmapper \(UDP and TCP Ports 111\)](#)
 Secure : (see [Secure RPC](#))
 spoofing : [19.4.4.4. Spoofing RPC](#)
RS-232 serial protocol : [14.3. The RS-232 Serial Protocol](#)
RSA algorithm
 [6.4.2. Summary of Public Key Systems](#)
 [6.4.6. RSA and Public Key Cryptography](#)
 [6.4.6.3. Strength of RSA](#)
 [6.5.3. Digital Signatures](#)
rsh (restricted shell)
 [8.1.4.1. Restricted shells under System V UNIX](#)
 [8.1.4.6. Potential problems with rsh](#)
 [17.3.18. rlogin and rsh \(TCP Ports 513 and 514\)](#)
 [17.3.18.6. /etc/hosts.lpd file](#)
rsh command : [16.3.2. Security and Nameservice](#)
rshd program : [11.1.2. Back Doors and Trap Doors](#)
RUID : (see [real UIDs/GIDs](#))
runacct command : [10.2. The acct/pacct Process Accounting File](#)
ruusend command : [15.4.3. L.cmds: Providing Remote Command Execution](#)
rw option for /etc/exports : [20.2.1.1. /etc/exports](#)

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

[Copyright](#) © 1999 [O'Reilly & Associates, Inc.](#) All Rights Reserved.

[[Library Home](#) | [DNS & BIND](#) | [TCP/IP](#) | [sendmail](#) | [sendmail Reference](#) | [Firewalls](#) | [Practical Security](#)]



Practical UNIX & Internet Security

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

Index: S

S/Key codebook scheme : [8.7.3. Code Books](#)

sa command : [10.2. The acct/pacct Process Accounting File](#)

sabotage : (see [terrorism](#); [vandalism](#))

salt

[8.6.2. What Is Salt?](#)

[8.6.3. What the Salt Doesn't Do](#)

sanitizing media : [12.3.2.3. Sanitize your media before disposal](#)

SATAN package

[17.6.1. SATAN](#)

[E.4.7. SATAN](#)

savacct file : [10.2. The acct/pacct Process Accounting File](#)

saved UID : [4.3.2. Saved IDs](#)

saving backup media

[7.1.5. How Long Should You Keep a Backup?](#)

(see also [archiving information](#); [backups](#))

sbrk command : [23.2. Tips on Avoiding Security-related Bugs](#)

scanf function : [23.2. Tips on Avoiding Security-related Bugs](#)

scanning networks : [17.6. Network Scanning](#)

SCCS (Source Code Control System)

[7.3.2. Building an Automatic Backup System](#)

[17.3. Primary UNIX Network Services](#)

Scherbius, Arthur : [6.3. The Enigma Encryption System](#)

screen savers : [12.3.5.2. X screen savers](#)

screens, multiple : [12.3.4.3. Multiple screens](#)

script command : [24.1.2. Rule #2: DOCUMENT](#)

scripts, CGI : (see [CGI, scripts](#))

scytales : [6.1. A Brief History of Cryptography](#)

search warrants

[26.2.4. Hazards of Criminal Prosecution](#)

[26.2.5. If You or One of Your Employees Is a Target of an Investigation...](#)

searching for .rhosts file : [17.3.18.5. Searching for .rhosts files](#)

Seberry, Jennifer : [6.5.4.3. HAVAL](#)

secrecy, Kerberos : [19.6.1.3. Authentication, data integrity, and secrecy](#)

secret keys : [6.4.6. RSA and Public Key Cryptography](#)

Secret Service, U.S.

[26.2.2. Federal Jurisdiction](#)

[F.3.3. U.S. Secret Service \(USSS\)](#)

Secure Hash Algorithm (SHA)

[6.5.3. Digital Signatures](#)

[6.5.4.2. SHA](#)

Secure HTTP : [18.4.1. Eavesdropping Over the Wire](#)

Secure NFS : [19.3.2.4. Using Secure NFS](#)

-secure option

[19.3.2.4. Using Secure NFS](#)

[19.4.4.5. Spoofing NIS](#)

secure option for /etc/exports : [20.2.1.1. /etc/exports](#)

Secure RPC

[19.3. Secure RPC \(AUTH_DES\)](#)

[19.3.4. Limitations of Secure RPC](#)

with NIS/NIS+

[19.3.2. Setting Up Secure RPC with NIS](#)

[19.3.4. Limitations of Secure RPC](#)

NTP and : [19.3.1.3. Setting the window](#)

reauthentication : [19.3.1.3. Setting the window](#)

versus Kerberos : [19.6.2. Kerberos vs. Secure RPC](#)

Secure Socket Layer : (see [SSL](#))

secure terminals : [8.5.1. Secure Terminals](#)

SecureID : [8.7.2. Token Cards](#)

SecureNet key : [8.7.2. Token Cards](#)

security

[2.1. Planning Your Security Needs](#)

[9.1.2. Read-only Filesystems](#)

[12.1.1. The Physical Security Plan](#)

(see also [integrity](#); [physical security](#); [system administration](#); [threats](#))
of CGI scripts

[18.2.3. Writing Secure CGI Scripts and Programs](#)

[18.2.4.1. Beware mixing HTTP with anonymous FTP](#)

changed detection

[9.2. Detecting Change](#)

[9.3. A Final Note](#)

checking arguments : [23.2. Tips on Avoiding Security-related Bugs](#)

critical messages to log

[10.5.3. syslog Messages](#)

[10.5.3.1. Beware false log entries](#)
cryptography
 [6. Cryptography](#)
 [6.7.2. Cryptography and Export Controls](#)
definition of : [1.1. What Is Computer Security?](#)
digital signatures : (see [digital signatures](#))
disabling finger : [17.3.8.2. Disabling finger](#)
disk quotas : [25.2.2.5. Using quotas](#)
dormant accounts, finding : [8.4.3. Finding Dormant Accounts](#)
drills : [24.1.3. Rule #3: PLAN AHEAD](#)
/etc/passwd : (see [/etc/group file](#); [/etc/passwd file](#))
firewalls : (see [firewalls](#))
four steps toward : [2.4.4.7. Defend in depth](#)
guessable passwords
 [3.6.1. Bad Passwords: Open Doors](#)
 [3.6.4. Passwords on Multiple Machines](#)
identification protocol : [17.3.12. Identification Protocol \(auth\) \(TCP Port 113\)](#)
improving DES algorithm
 [6.4.5. Improving the Security of DES](#)
 [6.4.5.2. Triple DES](#)
IP
 [16.3. IP Security](#)
 [16.3.3. Authentication](#)
laws and : (see [laws](#))
legal liability
 [26.4. Other Liability](#)
 [26.4.7. Harassment, Threatening Communication, and Defamation](#)
levels of NIS+ servers : [19.5.5. NIS+ Limitations](#)
link-level : [16.3.1. Link-level Security](#)
message digests : (see [message digests](#))
modems and
 [14.4. Modems and Security](#)
 [14.4.4.2. Protection against eavesdropping](#)
monitoring : (see [logging](#))
multilevel (defense in depth)
 [1.3. History of UNIX](#)
 [2.4.4.7. Defend in depth](#)
 [2.5.3. Final Words: Risk Management Means Common Sense](#)

[17.2. Controlling Access to Servers](#)
name service and : [16.3.2. Security and Nameservice](#)
national : [26.2.2. Federal Jurisdiction](#)
network services
[17.4. Security Implications of Network Services](#)
[19.1. Securing Network Services](#)
passwords
[3.2. Passwords](#)
[3.8. Summary](#)
personnel
[13. Personnel Security](#)
[13.3. Outsiders](#)
[A.1.1.12. Chapter 13: Personnel Security](#)
policy of
[1.2. What Is an Operating System?](#)
[2. Policies and Guidelines](#)
[2.5.3. Final Words: Risk Management Means Common Sense](#)
protecting backups
[7.1.6. Security for Backups](#)
[7.1.6.3. Data security for backups](#)
published resources on
[D. Paper Sources](#)
[D.2. Security Periodicals](#)
responding to breakins
[24. Discovering a Break-in](#)
[24.7. Damage Control](#)
restricting login : [8.3. Restricting Logins](#)
.rhosts : (see [.rhosts file](#))
sendmail problems : [17.3.4.1. sendmail and security](#)
Skipjack algorithm : [6.4.1. Summary of Private Key Systems](#)
SNMP and : [17.3.15. Simple Network Management Protocol \(SNMP\)](#)
[\(UDP Ports 161 and 162\)](#)
software piracy : [26.4.2.1. Software piracy and the SPA](#)
standards of : [2.4.2. Standards](#)
superuser problems : [4.2.1.5. The problem with the superuser](#)
through obscurity
[2.5. The Problem with Security Through Obscurity](#)
[2.5.3. Final Words: Risk Management Means Common Sense](#)
[8.8.9. Account Names Revisited: Using Aliases for Increased Security](#)

[18.2.4. Keep Your Scripts Secret!](#)

tools for : [11.1. Programmed Threats: Definitions](#)

Tripwire package

[9.2.4. Tripwire](#)

[9.2.4.2. Running Tripwire](#)

UNIX and

[1. Introduction](#)

[1.4. Security and UNIX](#)

[1.4.3. Add-On Functionality Breeds Problems](#)

user awareness of

[1.4.1. Expectations](#)

[2. Policies and Guidelines](#)

[2.4.4.4. Concentrate on education](#)

[13.2.2. Ongoing Training and Awareness](#)

UUCP : (see [UUCP](#))

weakness-finding tools : [11.1.1. Security Tools](#)

World Wide Web

[18. WWW Security](#)

[18.7. Summary](#)

X Window System

[17.3.21.2. X security](#)

[17.3.21.3. The xhost facility](#)

Security Emergency Response Team (SERT) : [F.3.4.4. Australia: Internet .au domain](#)

security file (UUCP) : [10.3.4. uucp Log Files](#)

security holes

[2.5. The Problem with Security Through Obscurity](#)

(see also [back doors](#); [threats](#))

ftpd program : [6.5.2. Using Message Digests](#)

mailing list for : [E.1.3.3. Bugtraq](#)

reporting : [2.5.1. Going Public](#)

ruusend in L.cmds file : [15.4.3. L.cmds: Providing Remote Command Execution](#)

SUID/SGID programs : [5.5.3.1. write: Example of a possible SUID/SGID security hole](#)

/usr/lib/preserve : [5.5.3.2. Another SUID example: IFS and the /usr/lib/preserve hole](#)

UUCP : [15.7. Early Security Problems with UUCP](#)

sed scripts : [11.1.4. Trojan Horses](#)

seeds, random number

[23.6. Tips on Generating Random Numbers](#)

[23.8. Picking a Random Seed](#)

select system call : [17.1.3. The /etc/inetd Program](#)

selection lists : [18.2.3.1. Do not trust the user's browser!](#)

self-destruct sequences : [27.2.1. Hardware Bugs](#)

SENDFILES= command

[15.5.1.3. A Sample Permissions file](#)

[15.5.2. Permissions Commands](#)

sendmail

[11.1.2. Back Doors and Trap Doors](#)

[11.5.2.5. .forward, .procmailrc](#)

[11.5.3.3. /usr/lib/aliases, /etc/aliases, /etc/sendmail/aliases, aliases.dir, or aliases.pag](#)

[17.3.4. Simple Mail Transfer Protocol \(SMTP\) \(TCP Port 25\)](#)

[17.3.4.3. Improving the security of Berkeley sendmail V8](#)

[24.2.4.2. How to contact the system administrator of a computer you don't know](#)

(see also [mail](#))

aliases : [11.5.3.3. /usr/lib/aliases, /etc/aliases, /etc/sendmail/aliases, aliases.dir, or aliases.pag](#)

determining version of : [17.3.4.1. sendmail and security](#)

.forward file : [24.4.1.6. Changes to startup files](#)

improving Version 8 : [17.3.4.3. Improving the security of Berkeley sendmail V8](#)

logging to syslog : [17.3.4.3. Improving the security of Berkeley sendmail V8](#)

same Internet/NIS domain : [19.4.3. NIS Domains](#)

security problems with : [17.3.4.1. sendmail and security](#)

sendmail.cf file : [17.3.4. Simple Mail Transfer Protocol \(SMTP\) \(TCP Port 25\)](#)

sensors : (see [detectors](#))

separation of duties : [13.2.5. Least Privilege and Separation of Duties](#)

sequence of commands : [23.2. Tips on Avoiding Security-related Bugs](#)

serial interfaces : [14.2. Serial Interfaces](#)

Serial Line Internet Protocol (SLIP) : [14.5. Modems and UNIX](#)

serial numbers, logging : [10.7.1.2. Informational material](#)

SERT (Security Emergency Response Team) : [F.3.4.4. Australia: Internet .au domain](#)

server-side includes

[18.2.2.2. Additional configuration issues](#)

[18.3.2. Commands Within the <Directory> Block](#)

servers

[16.2.5. Clients and Servers](#)

[17.1. Understanding UNIX Internet Servers](#)

[17.1.3. The /etc/inetd Program](#)

backing up : [7.2.2. Small Network of Workstations and a Server](#)

checklist for bringing up : [17.4. Security Implications of Network Services](#)

controlling access to : [17.2. Controlling Access to Servers](#)

ftp : (see [FTP](#))

http : (see [http server](#))

load shedding : [23.3. Tips on Writing Network Programs](#)

master/slave : (see [NIS](#))

NIS+, security levels of : [19.5.5. NIS+ Limitations](#)

overloading with requests : [25.3.1. Service Overloading](#)

setting up for FTP

[17.3.2.4. Setting up an FTP server](#)

[17.3.2.6. Setting up anonymous FTP with the standard UNIX FTP server](#)

web : (see [web servers](#))

WN : [18.3. Controlling Access to Files on Your Server](#)

Xauthority : [17.3.21.4. Using Xauthority magic cookies](#)

service overloading : [25.3.1. Service Overloading](#)

services file : [17.1.1. The /etc/services File](#)

Services table (NIS+) : [19.5.3. NIS+ Tables](#)

SESAME (Secure European System for Applications in a Multivendor Environment) : [19.7.2. SESAME](#)

session

hijacking : [17.3.3. TELNET \(TCP Port 23\)](#)

IDs

[4.3.3. Other IDs](#)

[C.1.3.4. Process groups and sessions](#)

keys

[6.4. Common Cryptographic Algorithms](#)

[19.3.1.1. Proving your identity](#)

setgid function

[4.3.3. Other IDs](#)

[23.4. Tips on Writing SUID/SGID Programs](#)

setpgrp function : [C.1.3.4. Process groups and sessions](#)

setrlimit function : [23.2. Tips on Avoiding Security-related Bugs](#)

setsid function : [C.1.3.4. Process groups and sessions](#)

setuid file : [4.3.1. Real and Effective UIDs](#)

setuid function : [23.4. Tips on Writing SUID/SGID Programs](#)

setuid/setgid : (see [SUID/SGID programs](#))

SGID bit

[5.5.1. SUID, SGID, and Sticky Bits](#)

[5.5.7. SGID Bit on Files \(System V UNIX Only\): Mandatory Record Locking](#)

(see also [SUID/SGID programs](#))

clearing with chown : [5.7. chown: Changing a File's Owner](#)

on directories : [5.5.6. SGID and Sticky Bits on Directories](#)

on files : [5.5.7. SGID Bit on Files \(System V UNIX Only\): Mandatory Record Locking](#)

SGID files : [B.3.2.2. SGID files](#)

sh (Bourne shell)

[11.5.1. Shell Features](#)

[C.5.3. Running the User's Shell](#)

(see also [shells](#))

sh program : [5.5.3.2. Another SUID example: IFS and the /usr/lib/preserve hole](#)
SUID and : [5.5.2. Problems with SUID](#)

SHA (Secure Hash Algorithm)

[6.5.3. Digital Signatures](#)

[6.5.4.2. SHA](#)

shadow file

[8.1.1. Accounts Without Passwords](#)

[8.8.5. Shadow Password Files](#)

shadow passwords

[3.2.1. The /etc/passwd File](#)

[8.4.1. Changing an Account's Password](#)

[8.8.5. Shadow Password Files](#)

Shamir, Adi

[6.4.2. Summary of Public Key Systems](#)

[6.4.6. RSA and Public Key Cryptography](#)

shar format file : [11.1.4. Trojan Horses](#)

shareware : [27.2.2. Viruses on the Distribution Disk](#)

shell escapes

[8.1.3. Accounts That Run a Single Command](#)

[8.1.4.6. Potential problems with rsh](#)

in L.cmds list : [15.4.3. L.cmds: Providing Remote Command Execution](#)
shell scripts, SUID

[5.5.3. SUID Shell Scripts](#)

[5.5.3.2. Another SUID example: IFS and the /usr/lib/preserve hole](#)

shells

[1.2. What Is an Operating System?](#)

[3.2.1. The /etc/passwd File](#)

[11.1.4. Trojan Horses](#)

[11.5.1. Shell Features](#)

[11.5.1.4. Filename attacks](#)

[C.2. Creating Processes](#)

[C.5.3. Running the User's Shell](#)

changing

[8.4.2. Changing the Account's Login Shell](#)

[8.7.1. Integrating One-time Passwords with UNIX](#)

history files : [10.4.1. Shell History](#)

one-command accounts : [8.1.3. Accounts That Run a Single Command](#)

restricted (rsh, ksh)

[8.1.4.1. Restricted shells under System V UNIX](#)

[8.1.4.6. Potential problems with rsh](#)

UUCP : (see [uucico program](#))

shells file : [8.4.2. Changing the Account's Login Shell](#)

Shimomura, Tsutomu : [23.3. Tips on Writing Network Programs](#)

shoulder surfing

[3.2.4. Passwords Are a Shared Secret](#)

[5.5.2. Problems with SUID](#)

shredders : [12.3.3. Other Media](#)

SHTTP : (see [Secure HTTP](#))

shutdowns and wtmp file : [10.1.3. last Program](#)

SIGHUP signal : [C.4. The kill Command](#)

SIGKILL signal : [C.4. The kill Command](#)

Signal Ground (SG) : [14.3. The RS-232 Serial Protocol](#)

signal grounding : [25.3.3. Signal Grounding](#)

signals : [C.3. Signals](#)

signature : [9.2. Detecting Change](#)

signatures : (see [digital signatures](#))

SIGSTOP signal : [C.4. The kill Command](#)

SIGTERM signal : [25.2.1.1. Too many processes](#)

Simple Mail Transfer Protocol (SMTP)

[17.3.4. Simple Mail Transfer Protocol \(SMTP\) \(TCP Port 25\)](#)
[17.3.4.3. Improving the security of Berkeley sendmail V8](#)
Simple Network Management Protocol : (see [SNMP](#))
single-user mode : [C.5.1. Process #1: /etc/init](#)
Skipjack algorithm : [6.4.1. Summary of Private Key Systems](#)
slash (/)
IFS separator : [11.5.1.2. IFS attacks](#)
root directory
[5.1.1. Directories](#)
(see also [root directory](#))
Slave mode (uucico) : [15.1.4. How the UUCP Commands Work](#)
slave server
[19.4. Sun's Network Information Service \(NIS\)](#)
(see also [NIS](#))
SLIP (Serial Line Internet Protocol)
[14.5. Modems and UNIX](#)
[16.2. IPv4: The Internet Protocol Version 4](#)
Small Business Community Nationwide (SBA CERT) : [F.3.4.31. Small Business Association \(SBA\): small business community nationwide](#)
smap program : [17.3.4.1. sendmail and security](#)
smart cards, firewalls : [21.5. Special Considerations](#)
smit tool : [8.8.2. Constraining Passwords](#)
smoke and smoking : [12.2.1.2. Smoke](#)
SMTP (Simple Mail Transfer Protocol)
[17.3.4. Simple Mail Transfer Protocol \(SMTP\) \(TCP Port 25\)](#)
[17.3.4.3. Improving the security of Berkeley sendmail V8](#)
SNA (System Network Architecture) : [16.4.2. SNA](#)
SNEFRU algorithm : [6.5.4.4. SNEFRU](#)
sniffers
[1.4.3. Add-On Functionality Breeds Problems](#)
[3. Users and Passwords](#)
[8.7. One-Time Passwords](#)
[17.3.3. TELNET \(TCP Port 23\)](#)
(see also [eavesdropping](#))
network : [16.3. IP Security](#)
packet : [16.3.1. Link-level Security](#)
SNMP (Simple Network Management Protocol) : [17.3.15. Simple Network Management Protocol \(SNMP\) \(UDP Ports 161 and 162\)](#)
snoop program : [24.2.3. Monitoring the Intruder](#)

SOCKS : [E.4.8. SOCKS](#)

soft disk quotas : [25.2.2.5. Using quotas](#)

software

for backups

[7.4. Software for Backups](#)

[7.4.7. inode Modification Times](#)

bugs in : (see [bugs](#))

for checking integrity : [19.5.5. NIS+ Limitations](#)

checking new

[8.1.5.2. Checking new software](#)

[11.1.2. Back Doors and Trap Doors](#)

consistency of : [2.1. Planning Your Security Needs](#)

distributing : (see [FTP](#))

exporting : [26.4.1. Munitions Export](#)

failure of : [7.1.1.1. A taxonomy of computer failures](#)

hacker challenges : [27.2.4. Hacker Challenges](#)

logic bombs : [11.1.3. Logic Bombs](#)

operating system : (see [operating systems](#))

patches for, logging : [10.7.2.2. Informational material](#)

quality of

[1.4.2. Software Quality](#)

[1.4.3. Add-On Functionality Breeds Problems](#)

stolen (pirated)

[17.3.2.6. Setting up anonymous FTP with the standard UNIX FTP server](#)

[26.4.2.1. Software piracy and the SPA](#)

stored via FTP : [17.3.2.6. Setting up anonymous FTP with the standard UNIX FTP server](#)

testing : [1.4.2. Software Quality](#)

vendor license agreements : [18.5.2. Trusting Your Software Vendor](#)

viruses : [11.1.5. Viruses](#)

worms : [11.1.6. Worms](#)

software patents : [6.7.1. Cryptography and the U.S. Patent System](#)

Software Publishers Association (SPA) : [26.4.2.1. Software piracy and the SPA](#)

Software Security Response Team (SSRT) : [F.3.4.9. Digital Equipment Corporation and customers](#)

Solaris

[1.3. History of UNIX](#)

[8.7.1. Integrating One-time Passwords with UNIX](#)

[/etc/logindevperm : 17.3.21.1. /etc/fstab and /etc/logindevperm](#)
process limit : [25.2.1.1. Too many processes](#)
Secure RPC time window : [19.3.1.3. Setting the window](#)
[/var/adm/loginlog file : 10.1.4. loginlog File](#)
wtmpt file : [10.1.2. utmp and wtmp Files](#)
Source Code Control System (SCCS) : [7.3.2. Building an Automatic Backup System](#)
source code, keeping secret : [2.5. The Problem with Security Through Obscurity](#)
SPA (Software Publishers Association) : [26.4.2.1. Software piracy and the SPA](#)
Spaf's first principle : [2.4.4.5. Have authority commensurate with responsibility](#)
spies
 [11.3. Authors](#)
 [14.4.4.1. Kinds of eavesdropping](#)
spoofing : [16.3. IP Security](#)
 network connection : [8.5.3.1. Trusted path](#)
 network services : [17.5. Monitoring Your Network with netstat](#)
NIS : [19.4.4.5. Spoofing NIS](#)
RPCs : [19.4.4.4. Spoofing RPC](#)
spool file : [15.1.4. How the UUCP Commands Work](#)
spoolers, printer : [12.3.4.1. Printer buffers](#)
sprinkler systems
 [12.2.1.1. Fire](#)
 (see also [water](#))
Sprint response team : [F.3.4.32. Sprint](#)
sprintf function
 [23.1.1. The Lesson of the Internet Worm](#)
 [23.2. Tips on Avoiding Security-related Bugs](#)
sscanf function : [23.2. Tips on Avoiding Security-related Bugs](#)
SSL (Secure Socket Layer) : [18.4.1. Eavesdropping Over the Wire](#)
SSRT (Software Security Response Team) : [F.3.4.9. Digital Equipment Corporation and customers](#)
Stallman, Richard : [1. Introduction](#)
start bit
 [14.1. Modems: Theory of Operation](#)
 [14.2. Serial Interfaces](#)
startup command : [10.2.1. Accounting with System V](#)
startup files
 attacks via
 [11.5.2. Start-up File Attacks](#)

[11.5.2.7. Other initializations](#)

intruder's changes to : [24.4.1.6. Changes to startup files](#)
stat function : [5.4. Using Directory Permissions](#)
state law enforcement : [26.2.1. The Local Option](#)
stateless : [20.1.4.3. Connectionless and stateless](#)
static electricity : [12.2.1.8. Electrical noise](#)
static links : [23.4. Tips on Writing SUID/SGID Programs](#)
stdio : (see [portable I/O library](#))
Steele, Guy L. : [1. Introduction](#)
sticky bits : [5.5.1. SUID, SGID, and Sticky Bits](#)
on directories : [5.5.6. SGID and Sticky Bits on Directories](#)
stolen property : (see [theft](#))
stop bit
[14.1. Modems: Theory of Operation](#)
[14.2. Serial Interfaces](#)
storage
[12.3.4. Protecting Local Storage](#)
[12.3.4.5. Function keys](#)
strcpy routine : [23.1.1. The Lesson of the Internet Worm](#)
streadd function : [23.2. Tips on Avoiding Security-related Bugs](#)
strecpy function : [23.2. Tips on Avoiding Security-related Bugs](#)
strength, cryptographic : [6.2.3. Cryptographic Strength](#)
of DES algorithm
[6.4.4.3. DES strength](#)
[6.4.5.2. Triple DES](#)
of RSA algorithm : [6.4.6.3. Strength of RSA](#)
string command : [12.3.5.2. X screen savers](#)
strtrns function : [23.2. Tips on Avoiding Security-related Bugs](#)
su command
[4.2.1.2. Superuser is not for casual use](#)
[4.3. su: Changing Who You Claim to Be](#)
[4.3.8. Other Uses of su](#)
becoming superuser : [4.3.4. Becoming the Superuser](#)
log of failed attempts : [4.3.7. The Bad su Log](#)
sulog file
[10.1. The Basic Log Files](#)
[10.3.2. sulog Log File](#)
utmp and wtmp files and : [10.1.2.1. su command and /etc/utmp and /var/adm/wtmp files](#)

subnetting : [16.2.1.2. Classical network addresses](#)
substitution (in encryption) : [6.1.2. Cryptography and Digital Computers](#)
SUID/SGID programs
 [4.3.1. Real and Effective UIDs](#)
 [5.5. SUID](#)
 [5.5.7. SGID Bit on Files \(System V UNIX Only\): Mandatory Record Locking](#)
 [B.3. SUID and SGID Files](#)
back door via : [11.1.2. Back Doors and Trap Doors](#)
chown command and : [5.7. chown: Changing a File's Owner](#)
chroot call and : [8.1.5.2. Checking new software](#)
created by intruders : [24.4.1.3. New SUID and SGID files](#)
on directories : [5.5.6. SGID and Sticky Bits on Directories](#)
disabling (turning off) : [5.5.5. Turning Off SUID and SGID in Mounted Filesystems](#)
finding all files
 [5.5.4. Finding All of the SUID and SGID Files](#)
 [5.5.4.1. The ncheck command](#)
shell scripts
 [5.5.3. SUID Shell Scripts](#)
 [5.5.3.2. Another SUID example: IFS and the /usr/lib/preserve hole](#)
uucp access : [15.3. UUCP and Security](#)
writing : [23.4. Tips on Writing SUID/SGID Programs](#)
SUID/SGID programs:writing:programming:writing:zzz] : [23. Writing Secure SUID and Network Programs](#)
suing : (see [civil actions](#))
sulog file
 [4.3.7. The Bad su Log](#)
 [10.3.2. sulog Log File](#)
sum command
 [6.5.5.1. Checksums](#)
 [9.2.3. Checksums and Signatures](#)
Sun Microsystem's NIS : (see [NIS](#))
Sun Microsystems : [E.3.4.34. Sun Microsystems customers](#)
SUN-DES-1 authentication : [17.3.21.3. The xhost facility](#)
SunOS operating system : [1.3. History of UNIX](#)
 authdes_win variable : [19.3.1.3. Setting the window](#)
 /etc/fstab file : [17.3.21.1. /etc/fstab and /etc/logindevperm](#)
TFTP sand : [17.3.7. Trivial File Transfer Protocol \(TFTP\) \(UDP Port 69\)](#)

trusted hosts and : [17.3.18.5. Searching for .rhosts files](#)
superencryption : [6.4.5. Improving the Security of DES](#)
superuser

[4. Users, Groups, and the Superuser](#)

[4.2.1. The Superuser](#)

[4.2.1.5. The problem with the superuser](#)

(see also [root account](#))

abilities of : [27.1.3. What the Superuser Can and Cannot Do](#)

becoming with su : [4.3.4. Becoming the Superuser](#)

changing passwords

[8.4.1. Changing an Account's Password](#)

[8.8.8. Disabling an Account by Changing Its Password](#)

encryption and : [6.2.4. Why Use Encryption with UNIX?](#)

logging attempts to become : (see [sulog file](#))

problems with : [4.2.1.5. The problem with the superuser](#)

restrictions on : [4.2.1.4. What the superuser can't do](#)

TCB files : [8.5.3.2. Trusted computing base](#)

using passwd command : [3.5. Verifying Your New Password](#)

web server as : [18.2.1. The Server's UID](#)

SURFnet : [F.3.4.25. Netherlands: SURFnet-connected sites](#)

surges : (see [power surges](#))

SVR4 (System V Release 4) : [1.3. History of UNIX](#)

swap partition : [5.5.1. SUID, SGID, and Sticky Bits](#)

swap space : [25.2.3. Swap Space Problems](#)

Swatch program

[10.6. Swatch: A Log File Tool](#)

[10.6.2. The Swatch Configuration File](#)

[E.4.9. Swatch](#)

SWITCH : [F.3.4.35. SWITCH-connected sites](#)

symbolic links and permissions : [5.1.7. File Permissions in Detail](#)

symbolic-link following

[18.2.2.2. Additional configuration issues](#)

[18.3.2. Commands Within the <Directory> Block](#)

SymLinksIfOwnerMatch option : [18.3.2. Commands Within the <Directory> Block](#)

symmetric key : (see [private-key cryptography](#))

SYN bit : [16.2.4.2. TCP](#)

sync system call

[5.6. Device Files](#)

[8.1.3. Accounts That Run a Single Command](#)
sys (user) : [4.1. Users and Groups](#)
syslog facility
 [4.3.7. The Bad su Log](#)
 [10.5. The UNIX System Log \(syslog\) Facility](#)
 [10.5.3.1. Beware false log entries](#)
 [23.1.1. The Lesson of the Internet Worm](#)
 false log entries : [10.5.3.1. Beware false log entries](#)
 where to log
 [10.5.2. Where to Log](#)
 [10.5.2.3. Logging everything everywhere](#)
syslog file : [17.3.4.3. Improving the security of Berkeley sendmail V8](#)
syslog.conf file : [10.5.1. The syslog.conf Configuration File](#)
systat service : [17.3.1. systat \(TCP Port 11\)](#)
system
 auditing activity on : [2.1. Planning Your Security Needs](#)
 backing up critical files
 [7.3. Backing Up System Files](#)
 [7.3.2. Building an Automatic Backup System](#)
 control over : (see [access control](#))
 database files : [1.2. What Is an Operating System?](#)
 overload attacks : [25.2.1.2. System overload attacks](#)
 performance : (see [performance](#))
 remote, commands on : [15.1.2. uux Command](#)
 summarizing usage per user : [25.2.2.2. quot command](#)
 transferring files to other : [15.1.1. uucp Command](#)
system (in swatch program) : [10.6.2. The Swatch Configuration File](#)
system administration : [2.4.4.5. Have authority commensurate with responsibility](#)
 avoiding conventional passwords
 [8.8. Administrative Techniques for Conventional Passwords](#)
 [8.8.9. Account Names Revisited: Using Aliases for Increased Security](#)
 change monitoring : [9.3. A Final Note](#)
 changing passwords
 [8.4.1. Changing an Account's Password](#)
 [8.8.8. Disabling an Account by Changing Its Password](#)
 cleaning up /tmp directory : [25.2.4. /tmp Problems](#)
 contacting administrator : [24.2.4.2. How to contact the system administrator of a computer you don't know](#)

controlling UUCP security : [15.3. UUCP and Security](#)
detached signatures (PGP) : [6.6.3.6. PGP detached signatures](#)
disabling finger system : [17.3.8.2. Disabling finger](#)
discovering intruders
 [24.2. Discovering an Intruder](#)
 [24.2.6. Anatomy of a Break-in](#)
dual universes and : [5.9.1. Dual Universes](#)
errors by : [7.1.1.1. A taxonomy of computer failures](#)
finding largest files : [25.2.2.1. Disk-full attacks](#)
immutable files and : [9.1.1. Immutable and Append-Only Files](#)
locked accounts : [3.3. Entering Your Password](#)
message authentication : [6.5.2. Using Message Digests](#)
monitoring phantom mail : [17.3.4.2. Using sendmail to receive email](#)
new passwords : [3.4. Changing Your Password](#)
read-only filesystems and : [9.1.2. Read-only Filesystems](#)
references on : [D.1.11. UNIX Programming and System Administration](#)
removing automatic backups : [18.2.3.5. Beware stray CGI scripts](#)
sanitizing media : [12.3.2.3. Sanitize your media before disposal](#)
trusting : [27.3.2. Your System Administrator?](#)
weakness-finding tools : [11.1.1. Security Tools](#)
system call : [5.1.7. File Permissions in Detail](#)
system clock
 changing
 [5.1.5. File Times](#)
 [9.2.3. Checksums and Signatures](#)
 [17.3.14. Network Time Protocol \(NTP\) \(UDP Port 123\)](#)
 for random seeds : [23.8. Picking a Random Seed](#)
 Secure RPC timestamp : [19.3.1.3. Setting the window](#)
system files : [11.6.1.2. Writable system files and directories](#)
 initialization files : [11.5.3.5. System initialization files](#)
system function
 [5.5.3.2. Another SUID example: IFS and the /usr/lib/preserve hole](#)
 [18.2.3.2. Testing is not enough!](#)
 [18.2.3.3. Sending mail](#)
 [23.2. Tips on Avoiding Security-related Bugs](#)
system functions, checking arguments to : [23.2. Tips on Avoiding Security-related Bugs](#)
System Network Architecture (SNA) : [16.4.2. SNA](#)
System V UNIX

[Which UNIX System?](#)

[1.3. History of UNIX](#)

accounting with : [10.2.1. Accounting with System V](#)

chroot in : [8.1.5. Restricted Filesystem](#)

default umask value : [5.3. The umask](#)

groups and : [4.1.3.2. Groups and older AT&T UNIX](#)

inittab program : [C.5.1. Process #1: /etc/init](#)

modems and : [14.5.1. Hooking Up a Modem to Your Computer](#)

passwords : [8.1.1. Accounts Without Passwords](#)

ps command with : [C.1.2.1. Listing processes with systems derived from System V](#)

random number generators : [23.7.3. drand48 \(\), lrand48 \(\), and mrand48 \(\)](#)

recent login times : [10.1.1. lastlog File](#)

Release 4 (SVR4) : [1.3. History of UNIX](#)

restricted shells : [8.1.4.1. Restricted shells under System V UNIX](#)

SGI bit on files : [5.5.7. SGID Bit on Files \(System V UNIX Only\): Mandatory Record Locking](#)

su command and : [4.3.6. Restricting su](#)

SUID files, list of : [B.3. SUID and SGID Files](#)

utmp and wtmp files : [10.1.2. utmp and wtmp Files](#)

UUCP : [15.4.1.3. Format of USERFILE entry without system name](#)

/var/adm/loginlog file : [10.1.4. loginlog File](#)

wtmpx file : [10.1.2. utmp and wtmp Files](#)

Systems file : [15.3.3. Security of L.sys and Systems Files](#)

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

[Copyright](#) © 1999 [O'Reilly & Associates, Inc.](#) All Rights Reserved.

[[Library Home](#) | [DNS & BIND](#) | [TCP/IP](#) | [sendmail](#) | [sendmail Reference](#) | [Firewalls](#) | [Practical Security](#)]



Practical UNIX & Internet Security

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

Index: T

table objects (NIS+) : [19.5.3. NIS+ Tables](#)

TACACS : [17.3.5. TACACS \(UDP Port 49\)](#)

tainting

[18.2.3.4. Tainting with Perl](#)

[23.4. Tips on Writing SUID/SGID Programs](#)

taintperl

[5.5.3. SUID Shell Scripts](#)

[18.2.3.4. Tainting with Perl](#)

[23.4. Tips on Writing SUID/SGID Programs](#)

talk program : [11.1.4. Trojan Horses](#)

tandem backup : [7.1.4. Guarding Against Media Failure](#)

tar program

[6.6.1.2. Ways of improving the security of crypt](#)

[7.3.2. Building an Automatic Backup System](#)

[7.4.2. Simple Archives](#)

[7.4.4. Encrypting Your Backups](#)

[24.2.6. Anatomy of a Break-in](#)

Taylor UUCP : [15.2. Versions of UUCP](#)

TCB (trusted computing base) : [8.5.3.2. Trusted computing base](#)

/tcg directory : [8.1.1. Accounts Without Passwords](#)

tcov tester : [23.2. Tips on Avoiding Security-related Bugs](#)

TCP (Transmission Control Protocol)

[16.2.4.2. TCP](#)

[17.1.3. The /etc/inetd Program](#)

(see also [network services](#))

connections, clogging : [25.3.4. Clogging](#)

TCP/IP

[1.4.3. Add-On Functionality Breeds Problems](#)

[10.5.2.2. Logging across the network](#)

(see also [networks](#))

checklist for

[A.1.1.15. Chapter 16: TCP/IP Networks](#)

[A.1.1.16. Chapter 17: TCP/IP Services](#)

network services : (see [network services](#))

- networks
 - [16. TCP/IP Networks](#)
 - [16.5. Summary](#)
- tcpwrapper program
 - [17.2. Controlling Access to Servers](#)
 - [E.4.10. tcpwrapper](#)
- tcsh
 - [11.5.1. Shell Features](#)
 - (see also [shells](#))
 - history file : [10.4.1. Shell History](#)
- telecommunications : [26.2.2. Federal Jurisdiction](#)
- telephone
 - [14.3.1. Originate and Answer](#)
 - (see also [modems](#))
 - calls, recording outgoing : [10.3.1. aculog File](#)
 - cellular : [12.2.1.8. Electrical noise](#)
 - checklist for : [A.1.1.13. Chapter 14: Telephone Security](#)
 - hang-up signal : (see [signals](#))
 - lines : [14.5.4. Physical Protection of Modems](#)
 - leasing : [14.5.4. Physical Protection of Modems](#)
 - one-way : [14.4.1. One-Way Phone Lines](#)
 - physical security of : [14.5.4. Physical Protection of Modems](#)
 - Telnet versus : [17.3.3. TELNET \(TCP Port 23\)](#)
- Telnet utility
 - [3.5. Verifying Your New Password](#)
 - [16.2.5. Clients and Servers](#)
 - [17.3.3. TELNET \(TCP Port 23\)](#)
 - versus rlogin : [17.3.18. rlogin and rsh \(TCP Ports 513 and 514\)](#)
- telnetd program : [11.1.2. Back Doors and Trap Doors](#)
- temperature : [12.2.1.6. Temperature extremes](#)
- TEMPEST system : [12.3.1.3. Eavesdropping by radio and using TEMPEST](#)
- terminal name and last command : [10.1.3. last Program](#)
- terrorism : [12.2.5. Defending Against Acts of War and Terrorism](#)
- testing
 - CGI scripts : [18.2.3.2. Testing is not enough!](#)
 - core files and : [23.2. Tips on Avoiding Security-related Bugs](#)
 - programs : [23.2. Tips on Avoiding Security-related Bugs](#)
 - software : [1.4.2. Software Quality](#)
- TFTP (Trivial File Transfer Protocol) : [17.3.7. Trivial File Transfer Protocol](#)

[\(TFTP\) \(UDP Port 69\)](#)

tftpd server : [17.3.7. Trivial File Transfer Protocol \(TFTP\) \(UDP Port 69\)](#)
theft

[7.1.1.1. A taxonomy of computer failures](#)

[12.2.6. Preventing Theft](#)

[12.2.6.4. Minimizing downtime](#)

[12.4.1.2. Potential for eavesdropping and data theft](#)

of backups

[12.3.2. Protecting Backups](#)

[12.3.2.4. Backup encryption](#)

of RAM chips : [12.2.6. Preventing Theft](#)

thieves : [11.3. Authors](#)

third-party billing : [14.5.4. Physical Protection of Modems](#)

Thompson, Ken

[1.3. History of UNIX](#)

[8.6. The UNIX Encrypted Password System](#)

threats

assessing cost of : [2.3.3. Adding Up the Numbers](#)

back doors : (see [back doors](#))

to backups

[7.1.6. Security for Backups](#)

[7.1.6.3. Data security for backups](#)

bacteria programs : [11.1.7. Bacteria and Rabbits](#)

biological : [12.2.1.7. Bugs \(biological\)](#)

broadcast storms : [25.3.2. Message Flooding](#)

via CGI scripts : [18.2.3.2. Testing is not enough!](#)

changing file owners : [5.7. chown: Changing a File's Owner](#)

changing system clock : [5.1.5. File Times](#)

code breaking

[6.1.1. Code Making and Code Breaking](#)

(see also [cryptography](#))

commonly attacked accounts : [8.1.2. Default Accounts](#)

computer failures : [7.1.1.1. A taxonomy of computer failures](#)

decode aliases : [17.3.4.2. Using sendmail to receive email](#)

deep tree structures : [25.2.2.8. Tree-structure attacks](#)

denial of service

[17.1.3. The /etc/inetd Program](#)

[17.3.21.5. Denial of service attacks under X](#)

[25. Denial of Service Attacks and Solutions](#)

[25.3.4. Clogging](#)
accidental : [25.2.5. Soft Process Limits: Preventing Accidental Denial of Service](#)
checklist for : [A.1.1.24. Chapter 25: Denial of Service Attacks and Solutions](#)
destructive attacks : [25.1. Destructive Attacks](#)
disk attacks
 [25.2.2. Disk Attacks](#)
 [25.2.2.8. Tree-structure attacks](#)
overload attacks
 [25.2. Overload Attacks](#)
 [25.2.5. Soft Process Limits: Preventing Accidental Denial of Service](#)
 system overload attacks : [25.2.1.2. System overload attacks](#)
disposed materials : [12.3.3. Other Media](#)
DNS client flooding : [16.3.2. Security and Nameservice](#)
DNS nameserver attacks : [17.3.6.2. DNS nameserver attacks](#)
DNS zone transfers : [17.3.6.1. DNS zone transfers](#)
dormant accounts
 [8.4. Managing Dormant Accounts](#)
 [8.4.3. Finding Dormant Accounts](#)
false syslog entries : [10.5.3.1. Beware false log entries](#)
filename attacks : [11.5.1.4. Filename attacks](#)
hidden space : [25.2.2.7. Hidden space](#)
HOME variable attacks : [11.5.1.3. \\$HOME attacks](#)
identifying and quantifying
 [2.2.1.2. Identifying threats](#)
 [2.2.2. Review Your Risks](#)
IFS variable attacks : [11.5.1.2. IFS attacks](#)
intruders : (see [intruders](#))
letting in accidentally : [11.4. Entry](#)
logic bombs
 [11.1.3. Logic Bombs](#)
 [27.2.2. Viruses on the Distribution Disk](#)
mailing list for : [E.1.3.9. RISKS](#)
media failure : [7.1.4. Guarding Against Media Failure](#)
meet-in-the-middle attacks : [6.4.5.1. Double DES](#)
MUD/IRC client programs : [17.3.23. Other TCP Ports: MUDs and Internet Relay Chat \(IRC\)](#)

newly created accounts : [24.4.1. New Accounts](#)
NIS, unintended disclosure : [19.4.5. Unintended Disclosure of Site Information with NIS](#)
with NNTP : [17.3.13. Network News Transport Protocol \(NNTP\) \(TCP Port 119\)](#)
open (guest) accounts
 [8.1.4. Open Accounts](#)
 [8.1.4.6. Potential problems with rsh](#)
PATH variable attacks : [11.5.1.1. PATH attacks](#)
plaintext attacks : [6.2.3. Cryptographic Strength](#)
playback (replay) attacks : [19.6.1.2. Using the ticket granting ticket programmed](#)
 [11. Protecting Against Programmed Threats](#)
 [11.6.2. Shared Libraries](#)
 [A.1.1.10. Chapter 11: Protecting Against Programmed Threats](#)
 [D.1.4. Computer Viruses and Programmed Threats](#)
 authors of : [11.3. Authors](#)
 damage from : [11.2. Damage](#)
replay attacks : [17.3.14. Network Time Protocol \(NTP\) \(UDP Port 123\)](#)
rsh, problems with : [8.1.4.6. Potential problems with rsh](#)
sendmail problems : [17.3.4.1. sendmail and security](#)
spoofed network connection : [8.5.3.1. Trusted path](#)
start-up file attacks
 [11.5.2. Start-up File Attacks](#)
 [11.5.2.7. Other initializations](#)
system clock : (see [system clock](#))
theft : (see [theft](#))
/tmp directory attacks : [25.2.4. /tmp Problems](#)
toll fraud : [14.4.1. One-Way Phone Lines](#)
traffic analysis : [18.4. Avoiding the Risks of Eavesdropping](#)
tree-structure attacks : [25.2.2.8. Tree-structure attacks](#)
Trojan horses
 [4.3.5. Using su with Caution](#)
 [11.1.4. Trojan Horses](#)
 [11.5. Protecting Yourself](#)
 [17.3.21.2. X security](#)
 [19.6.5. Kerberos Limitations](#)
 [27.2.2. Viruses on the Distribution Disk](#)
trusted hosts : (see [trusted, hosts](#))

unattended terminals

[12.3.5. Unattended Terminals](#)

[12.3.5.2. X screen savers](#)

unowned files : [24.4.1.8. Unowned files](#)

vandalism

[12.2.4. Vandalism](#)

[12.2.4.3. Network connectors](#)

viruses

[11.1.5. Viruses](#)

(see [viruses](#))

war and terrorism : [12.2.5. Defending Against Acts of War and Terrorism](#)

weakness-finding tools : [11.1.1. Security Tools](#)

by web browsers

[18.5. Risks of Web Browsers](#)

[18.5.2. Trusting Your Software Vendor](#)

worms : [11.1.6. Worms](#)

three-way handshake (TCP) : [16.2.4.2. TCP](#)

ticket-granting service

[19.6.1.1. Initial login](#)

[19.6.1.2. Using the ticket granting ticket](#)

[19.6.1.3. Authentication, data integrity, and secrecy](#)

tickets : (see [Kerberos system](#))

Tiger : [E.4.11. Tiger](#)

tilde (~)

in automatic backups : [18.2.3.5. Beware stray CGI scripts](#)

as home directory : [11.5.1.3. \\$HOME attacks](#)

~! in mail messages : [8.1.3. Accounts That Run a Single Command](#)

time

[19.3.1.3. Setting the window](#)

(see also [NTP](#); [system clock](#))

CPU, accounting

[10.2. The acct/pacct Process Accounting File](#)

[10.2.3. messages Log File](#)

defining random seed by : [23.8. Picking a Random Seed](#)

modification

[5.1.2. Inodes](#)

[5.1.5. File Times](#)

[7.4.7. inode Modification Times](#)

[9.2.2. Checklists and Metadata](#)

[24.5.1. Never Trust Anything Except Hardcopy](#)
most recent login : [10.1.1. lastlog File](#)
Secure RPC window of : [19.3.1.3. Setting the window](#)
timeouts
[11.1.3. Logic Bombs](#)
[23.3. Tips on Writing Network Programs](#)
timesharing
[19.6.5. Kerberos Limitations](#)
[23.2. Tips on Avoiding Security-related Bugs](#)
Timezone table (NIS+) : [19.5.3. NIS+ Tables](#)
tip command
[10.3.1. aculog File](#)
[14.5. Modems and UNIX](#)
[14.5.3.1. Originate testing](#)
[14.5.3.3. Privilege testing](#)
-l option : [14.5.3.1. Originate testing](#)
TIS Internet Firewall Toolkit (FWTK) : [E.4.12. TIS Internet Firewall Toolkit](#)
TMOUT variable : [12.3.5.1. Built-in shell autologout](#)
/tmp directory
[14.5.3.3. Privilege testing](#)
[25.2.4. /tmp Problems](#)
tmpfile function : [23.2. Tips on Avoiding Security-related Bugs](#)
token cards : [8.7.2. Token Cards](#)
token ring : [16.1. Networking](#)
toll fraud : [14.4.1. One-Way Phone Lines](#)
tools : [1.3. History of UNIX](#)
to find weaknesses : [11.1.1. Security Tools](#)
quality of
[1.4.2. Software Quality](#)
[1.4.3. Add-On Functionality Breeds Problems](#)
Totient Function : [6.4.6.1. How RSA works](#)
tracing connections
[24.2.4. Tracing a Connection](#)
[24.2.4.2. How to contact the system administrator of a computer you don't know](#)
trademarks : [26.4.3. Trademark Violations](#)
traffic analysis : [18.4. Avoiding the Risks of Eavesdropping](#)
training : [13.2.1. Initial Training](#)
transfer zones : [16.2.6.1. DNS under UNIX](#)

transferring files : [15.1.1. uucp Command](#)

Transmission Control Protocol (TCP) : [16.2.4.2. TCP](#)

Transmit Data (TD) : [14.3. The RS-232 Serial Protocol](#)

transmitters, radio : [12.2.1.8. Electrical noise](#)

transposition (in encryption) : [6.1.2. Cryptography and Digital Computers](#)

trap doors : (see [back doors](#))

trashing : [12.3.3. Other Media](#)

tree structures : [25.2.2.8. Tree-structure attacks](#)

trimlog : [E.4.13. trimlog](#)

Triple DES

[6.4.5. Improving the Security of DES](#)

[6.4.5.2. Triple DES](#)

Tripwire package

[9.2.4. Tripwire](#)

[9.2.4.2. Running Tripwire](#)

[19.5.5. NIS+ Limitations](#)

[E.4.14. Tripwire](#)

Trivial File Transfer Protocol (TFTP) : [17.3.7. Trivial File Transfer Protocol \(TFTP\) \(UDP Port 69\)](#)

Trojan horses

[4.3.5. Using su with Caution](#)

[11.1.4. Trojan Horses](#)

[11.5. Protecting Yourself](#)

[27.2.2. Viruses on the Distribution Disk](#)

Kerberos and : [19.6.5. Kerberos Limitations](#)

X clients : [17.3.21.2. X security](#)

truncate system call : [5.1.7. File Permissions in Detail](#)

trust

[1.1. What Is Computer Security?](#)

[2.1.1. Trust](#)

[27. Who Do You Trust?](#)

[27.4. What All This Means](#)

of log files : [10.8. Managing Log Files](#)

trusted

[8.5.3.2. Trusted computing base](#)

[17.1.1. The /etc/services File](#)

hosts

[17.3.18.1. Trusted hosts and users](#)

[17.3.18.4. The ~/.rhosts file](#)

NFS and : [17.3.18.2. The problem with trusted hosts](#)
path : [8.5.3.1. Trusted path](#)
ports : [1.4.3. Add-On Functionality Breeds Problems](#)
users
 [17.3.4.1. sendmail and security](#)
 [17.3.18.1. Trusted hosts and users](#)
TRW Network Area and System Administrators : [E.3.4.36. TRW network area and system administrators](#)
tty file : [7.1.2. What Should You Back Up?](#)
ttypmon program : [C.5.2. Logging In](#)
ttys file
 [8.5.1. Secure Terminals](#)
 [14.5.1. Hooking Up a Modem to Your Computer](#)
ttytab file : [C.5.1. Process #1: /etc/init](#)
ttypwatch program : [24.2.3. Monitoring the Intruder](#)
tunefs command : [25.2.2.6. Reserved space](#)
tunneling : [16.4.1. IPX](#)
twisted pair : [16.1. Networking](#)
TZ variable : [23.2. Tips on Avoiding Security-related Bugs](#)

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

[Copyright](#) © 1999 [O'Reilly & Associates, Inc.](#) All Rights Reserved.

[[Library Home](#) | [DNS & BIND](#) | [TCP/IP](#) | [sendmail](#) | [sendmail Reference](#) | [Firewalls](#) | [Practical Security](#)]



Practical UNIX & Internet Security

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

Index: U

U.S. Department of Energy : [F.3.4.12. France: universities, Ministry of Research and Education in France, CNRS, CEA, INRIA, CNES, INRA, IFREMER, and EDF](#)

U.S. Department of the Navy : [F.3.4.44. U.S. Department of the Navy](#)

U.S. law : (see [laws](#))

U.S. Secret Service

[26.2.2. Federal Jurisdiction](#)

[F.3.3. U.S. Secret Service \(USSS\)](#)

UDP (User Datagram Protocol)

[16.2.4.3. UDP](#)

[17.1.3. The /etc/inetd Program](#)

(see also [network services](#))

packet relay : [E.4.15. UDP Packet Relay](#)

ufsdump : (see [dump/restore program](#))

UIDs (user identifiers)

[4.1. Users and Groups](#)

[4.1.2. Multiple Accounts with the Same UID](#)

real versus effective

[4.3.1. Real and Effective UIDs](#)

[C.1.3.2. Process real and effective UID](#)

RPC requests and : [19.2.2.2. AUTH_UNIX](#)

su command and : [10.1.2.1. su command and /etc/utmp and /var/adm/wtmp files](#)

of web servers : [18.2.1. The Server's UID](#)

zero : (see [root account](#); [superuser](#))

UK Defense Research Agency : [F.3.4.37. UK: Defense Research Agency](#)

ulimit command : [25.2.5. Soft Process Limits: Preventing Accidental Denial of Service](#)

Ultrix : [1.3. History of UNIX](#)

trusted path : [8.5.3.1. Trusted path](#)

UUCP : [15.4.1.3. Format of USERFILE entry without system name](#)

umask

[5.3. The umask](#)

[5.3.2. Common umask Values](#)

[8.4.3. Finding Dormant Accounts](#)

unattended terminals

[12.3.5. Unattended Terminals](#)

[12.3.5.2. X screen savers](#)

uninterruptable power supply (UPS)

[2.2. Risk Assessment](#)

[12.2.1.1. Fire](#)

Unisys : [F.3.4.39. UK: other government departments and agencies](#)

universes : [5.9.1. Dual Universes](#)

UNIX : [1. Introduction](#)

add-on functionality of : [1.4.3. Add-On Functionality Breeds Problems](#)

conventional passwords : [3.2.6. Conventional UNIX Passwords](#)

DAC (Discretionary Access Controls) : [4.1.3. Groups and Group Identifiers \(GIDs\)](#)

DNS under : [16.2.6.1. DNS under UNIX](#)

encryption programs for

[6.6. Encryption Programs Available for UNIX](#)

[6.6.3.6. PGP detached signatures](#)

filesystem

[5. The UNIX Filesystem](#)

[5.10. Summary](#)

history of : [1.3. History of UNIX](#)

modems and

[14.5. Modems and UNIX](#)

[14.5.3.3. Privilege testing](#)

networking and : [16.1.2. Networking and UNIX](#)

operating systems : (see [operating systems](#))

primary network services

[17.3. Primary UNIX Network Services](#)

[17.3.23. Other TCP Ports: MUDs and Internet Relay Chat \(IRC\)](#)

process scheduler : [C.1.3.3. Process priority and niceness](#)

processes : (see [processes](#))

programming references : [D.1.11. UNIX Programming and System Administration](#)

published resources for : [D.1. UNIX Security References](#)

security and

[1.4. Security and UNIX](#)

[1.4.3. Add-On Functionality Breeds Problems](#)

signals : [C.3. Signals](#)

starting up

[C.5. Starting Up UNIX and Logging In](#)

[C.5.3. Running the User's Shell](#)

Version 6 : [1.3. History of UNIX](#)

viruses : (see [viruses](#))

web server on : [18.2. Running a Secure Server](#)

unlinked files : [25.2.2.7. Hidden space](#)

unowned files : [24.4.1.8. Unowned files](#)

unplugging connections : [24.2.5. Getting Rid of the Intruder](#)

unpredictability of randomness : [23.6. Tips on Generating Random Numbers](#)

upgrades, logging : [10.7.2.1. Exception and activity reports](#)

uploading stored information : [12.3.4. Protecting Local Storage](#)

UPS (uninterruptable power supply)

[2.2. Risk Assessment](#)

[12.2.1.1. Fire](#)

uptime command : [8.1.3. Accounts That Run a Single Command](#)

urandom device : [23.7.4. Other random number generators](#)

Usenet

[17.3.13. Network News Transport Protocol \(NNTP\) \(TCP Port 119\)](#)

[E.2. Usenet Groups](#)

(see also [NNTP](#))

cleanup scripts : [11.5.3. Abusing Automatic Mechanisms](#)

encryption for : (see [ROT13 algorithm](#))

posting breakins to : [24.6. Resuming Operation](#)

reporting security holes on : [2.5.1. Going Public](#)

User Datagram Protocol (UDP) : [16.2.4.3. UDP](#)

user error : [7.1.1.1. A taxonomy of computer failures](#)

user IDs : (see [UIDs](#))

USERFILE file (UUCP)

[15.4.1. USERFILE: Providing Remote File Access](#)

[15.4.2.1. Some bad examples](#)

usermod command

-e option : [8.4.3. Finding Dormant Accounts](#)

-f option : [8.4.3. Finding Dormant Accounts](#)

-s option : [8.3. Restricting Logins](#)

usernames : [3.1. Usernames](#)

aliases for : [8.8.9. Account Names Revisited: Using Aliases for Increased Security](#)

doubling as passwords (Joes) : [3.6.2. Smoking Joes](#)

last command and : [10.1.3. last Program](#)

as passwords : [8.8.3.1. Joetest: a simple password cracker](#)

special

[4.2. Special Usernames](#)

[4.2.3. Impact of the /etc/passwd and /etc/group Files on Security](#)

using someone else's

[4.3. su: Changing Who You Claim to Be](#)

[4.3.8. Other Uses of su](#)

users

[4. Users, Groups, and the Superuser](#)

[4.1. Users and Groups](#)

[4.1.2. Multiple Accounts with the Same UID](#)

(see also [groups](#); [su command](#))

assigning passwords to : [8.8.1. Assigning Passwords to Users](#)

auditing who is logged in

[10.1.2. utmp and wtmp Files](#)

[10.1.2.1. su command and /etc/utmp and /var/adm/wtmp files](#)

authentication for Web : [18.3.3. Setting Up Web Users and Passwords](#)

becoming other

[4.3. su: Changing Who You Claim to Be](#)

[4.3.8. Other Uses of su](#)

checklist for : [A.1.1.2. Chapter 3: Users and Passwords](#)

dormant accounts and

[8.4. Managing Dormant Accounts](#)

[8.4.3. Finding Dormant Accounts](#)

identifiers for : (see [UIDs](#))

importing to NIS server

[19.4.1. Including or excluding specific accounts:](#)

[19.4.4.2. Using netgroups to limit the importing of accounts](#)

letting in threats : [11.4. Entry](#)

limited : [8.1.5.1. Limited users](#)

logging

[10.4. Per-User Trails in the Filesystem](#)

[10.4.3. Network Setup](#)

NIS passwords for : [19.3.2.1. Creating passwords for users](#)

nobody (Secure RPC) : [19.3.2.1. Creating passwords for users](#)

notifying about monitoring : [26.2.6. Other Tips](#)

proving identity of : [19.3.1.1. Proving your identity](#)

recognizing as intruders

[24.2. Discovering an Intruder](#)

[24.2.6. Anatomy of a Break-in](#)

restricting certain : [18.3. Controlling Access to Files on Your Server](#)

root : (see [root account](#); [superuser](#))

sending messages to : [10.5.1. The syslog.conf Configuration File](#)

summarizing system usage by : [25.2.2.2. quot command](#)

tainting : [18.2.3.4. Tainting with Perl](#)

training : [13.2.1. Initial Training](#)

UIDs : (see [UIDs](#))

unattended terminals

[12.3.5. Unattended Terminals](#)

[12.3.5.2. X screen savers](#)

USERFILE entries for : [15.4.1.2. USERFILE entries for local users](#)

www : [18.2.2. Understand Your Server's Directory Structure](#)

users command

[10.1.2. utmp and wtmp Files](#)

[24.2.1. Catching One in the Act](#)

USG (UNIX Support Group) : [1.3. History of UNIX](#)

/usr directory

[4.3.7. The Bad su Log](#)

(see also [/var directory](#))

backing up /usr/bin : [7.1.2. What Should You Back Up?](#)

/usr/adm directory : [11.5.3.6. Other files](#)

/usr/adm/lastlog file : [10.1.1. lastlog File](#)

/usr/adm/messages file : [10.2.3. messages Log File](#)

/usr/bin directory

[11.1.5. Viruses](#)

[11.5.1.1. PATH attacks](#)

/usr/bin/uudecode : (see [uudecode program](#))

/usr/etc/yp/makedbm program : [19.4.4.1. Setting up netgroups](#)

/usr/lib/aliases file : [11.5.3.3. /usr/lib/aliases, /etc/aliases,](#)

[/etc/sendmail/aliases, aliases.dir, or aliases.pag](#)

/usr/lib directory : [11.5.3.6. Other files](#)

in restricted filesystems : [8.1.5. Restricted Filesystem](#)

/usr/lib/preserve program : [5.5.3.2. Another SUID example: IFS and the](#)

[/usr/lib/preserve hole](#)

/usr/lib/sendmail : (see [sendmail](#))

/usr/lib/uucp/Devices file : [14.5.1. Hooking Up a Modem to Your Computer](#)

/usr/lib/uucp directory

[15.4.2.1. Some bad examples](#)

[15.5.2. Permissions Commands](#)

/usr/lib/uucp/L-devices file : [14.5.1. Hooking Up a Modem to Your Computer](#)

/usr/lib/uucp/L.cmds file : (see [L.cmds file](#))

/usr/lib/uucp/L.sys file : [15.3.3. Security of L.sys and Systems Files](#)

/usr/lib/uucp/Permissions file : (see [Permissions file](#))

/usr/lib/uucp/Systems file : [15.3.3. Security of L.sys and Systems Files](#)

/usr/lib/uucp/USERFILE file

[15.4.1. USERFILE: Providing Remote File Access](#)

[15.4.2.1. Some bad examples](#)

/usr/local/bin : [1.1. What Is Computer Security?](#)

/usr/local/bin directory : [11.5.1.1. PATH attacks](#)

/usr/local/etc/http/logs directory : [10.3.5. access_log Log File](#)

/usr/local/lib directory : [11.5.3.6. Other files](#)

/usr/sbin/rexecd : (see [rexec service](#))

/usr/spool/cron/crontabs directory : [15.6.2. Automatic Execution of Cleanup Scripts](#)

/usr/spool/uucp directory : [15.1.4. How the UUCP Commands Work](#)

/usr/spool/uucppublic : (see [uucppublic directory](#))

/usr/ucb directory : [11.1.5. Viruses](#)

utility programs : [1.2. What Is an Operating System?](#)

utimes commandn : [24.5.1. Never Trust Anything Except Hardcopy](#)

utmp file

[10.1.2. utmp and wtmp Files](#)

[10.1.2.1. su command and /etc/utmp and /var/adm/wtmp files](#)

[24.2.1. Catching One in the Act](#)

[24.2.4. Tracing a Connection](#)

uucheck program : [15.5.3. uucheck: Checking Your Permissions File](#)

uucico program

[15.1.4. How the UUCP Commands Work](#)

[15.3. UUCP and Security](#)

[15.5.1.1. Starting up](#)

uucp (user)

[4.1. Users and Groups](#)

[4.2.2. Other Special Users](#)

uucp command : [15.1.1. uucp Command](#)

UUCP system

[4.1.2. Multiple Accounts with the Same UID](#)

[14.5. Modems and UNIX](#)

[15. UUCP](#)

[15.9. Summary](#)

additional logins : [15.3.1. Assigning Additional UUCP Logins](#)
BNU

[15.2. Versions of UUCP](#)

[15.5. Security in BNU UUCP](#)

[15.5.3. uucheck: Checking Your Permissions File](#)

checklist for : [A.1.1.14. Chapter 15: UUCP](#)

cleanup scripts

[11.5.3. Abusing Automatic Mechanisms](#)

[15.6.2. Automatic Execution of Cleanup Scripts](#)

early security problems : [15.7. Early Security Problems with UUCP](#)

HoneyDanBer (HDB) : [15.2. Versions of UUCP](#)

logging : [10.3.4. uucp Log Files](#)

mail forwarding : [15.6.1. Mail Forwarding for UUCP](#)

naming computer : [15.5.2. Permissions Commands](#)

over networks : [15.8. UUCP Over Networks](#)

NFS server and : [15.3. UUCP and Security](#)

passwords for : [15.3.2. Establishing UUCP Passwords](#)

Taylor : [15.2. Versions of UUCP](#)

over TCP : [17.3.20. UUCP over TCP \(TCP Port 540\)](#)

Version 2

[15.2. Versions of UUCP](#)

[15.4. Security in Version 2 UUCP](#)

[15.4.3. L.cmds: Providing Remote Command Execution](#)

uucpa account : [15.3.1. Assigning Additional UUCP Logins](#)

uucpd program : [15.8. UUCP Over Networks](#)

uucppublic directory

[15.1.1. uucp Command](#)

[15.4.1.3. Format of USERFILE entry without system name](#)

[15.5.2. Permissions Commands](#)

uudecode program : [17.3.4.2. Using sendmail to receive email](#)

uuencode program : [6.6.1.2. Ways of improving the security of crypt](#)

uux command : [15.1.2. uux Command](#)

- (hyphen) option : [15.1.2. uux Command](#)

-r option : [15.1.4. How the UUCP Commands Work](#)

uuxqt program : [15.4.1.3. Format of USERFILE entry without system name](#)

uuxqtcmds files : [15.4.3. L.cmds: Providing Remote Command Execution](#)

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

[Copyright](#) © 1999 [O'Reilly & Associates, Inc.](#) All Rights Reserved.

[[Library Home](#) | [DNS & BIND](#) | [TCP/IP](#) | [sendmail](#) | [sendmail Reference](#) | [Firewalls](#) | [Practical Security](#)]



Practical UNIX & Internet Security

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

Index: V

vacuums, computer : [12.2.1.3. Dust](#)

VALIDATE= command : [15.5.2. Permissions Commands](#)

vampire taps : [12.3.1.5. Fiber optic cable](#)

vandalism

[7.1.1.1. A taxonomy of computer failures](#)

[12.2.4. Vandalism](#)

[12.2.4.3. Network connectors](#)

/var directory

[4.3.7. The Bad su Log](#)

[9.1.2. Read-only Filesystems](#)

(see also [/usr directory](#))

/var/adm/acct : [10.2. The acct/pacct Process Accounting File](#)

/var/adm directory : [11.5.3.6. Other files](#)

/var/adm/lastlog file : [10.1.1. lastlog File](#)

/var/adm/loginlog file : [10.1.4. loginlog File](#)

/var/adm/messages : [10.2.3. messages Log File](#)

/var/adm/messages file : [4.3.7. The Bad su Log](#)

/var/adm/savacct : [10.2. The acct/pacct Process Accounting File](#)

/var/adm/sulog file : [4.3.7. The Bad su Log](#)

/var/adm/wtmp file

[10.1.2. utmp and wtmp Files](#)

[10.1.3.1. Pruning the wtmp file](#)

/var/adm/xferlog : [10.3.3. xferlog Log File](#)

/var/log directory : [11.5.3.6. Other files](#)

/var/spool/uucp/.Admin directory : [10.3.4. uucp Log Files](#)

variables

bounds checking : [23.2. Tips on Avoiding Security-related Bugs](#)

to CGI scripts : [18.2.3.1. Do not trust the user's browser!](#)

vendor liability : [18.5.2. Trusting Your Software Vendor](#)

vendors : [27.3.3. Your Vendor?](#)

ventilation

[12.2.1.10. Vibration](#)

(see also [dust](#); [smoke and smoking](#))

air ducts : [12.2.3.2. Entrance through air ducts](#)

holes (in hardware) : [12.2.4.1. Ventilation holes](#)
VERB command (sendmail) : [17.3.4.3. Improving the security of Berkeley sendmail V8](#)
verifying
backups : [12.3.2.1. Verify your backups](#)
new passwords : [3.5. Verifying Your New Password](#)
signatures with PGP : [6.6.3.5. Decrypting messages and verifying signatures](#)
Verisign Inc. : [18.6. Dependence on Third Parties](#)
Version 2 UUCP
[15.2. Versions of UUCP](#)
[15.4. Security in Version 2 UUCP](#)
[15.4.3. L.cmds: Providing Remote Command Execution](#)
callback feature : [15.4.1.5. Requiring callback](#)
Veteran's Health Administration : [F.3.4.45. U.S. Veteran's Health Administration](#)
vi editor
[5.5.3.2. Another SUID example: IFS and the /usr/lib/preserve hole](#)
[11.5.2.4. .exrc](#)
[11.5.2.7. Other initializations](#)
vibration : [12.2.1.10. Vibration](#)
video tape : [7.1.4. Guarding Against Media Failure](#)
vipw command : [8.4.1. Changing an Account's Password](#)
virtual terminals : (see [Telnet utility](#))
Virtual Private Network : [21.1.2. Uses of Firewalls](#)
viruses
[11.1. Programmed Threats: Definitions](#)
[11.1.5. Viruses](#)
[27.2.2. Viruses on the Distribution Disk](#)
bacteria programs : [11.1.7. Bacteria and Rabbits](#)
references on : [D.1.4. Computer Viruses and Programmed Threats](#)
voltage spikes : [12.2.1.8. Electrical noise](#)
VPN : [21.1.2. Uses of Firewalls](#)
VRFY option (sendmail) : [17.3.4.3. Improving the security of Berkeley sendmail V8](#)
vsprintf function : [23.2. Tips on Avoiding Security-related Bugs](#)
VT100 terminal : [27.2.1. Hardware Bugs](#)

[Copyright](#) © 1999 [O'Reilly & Associates, Inc.](#) All Rights Reserved.

[[Library Home](#) | [DNS & BIND](#) | [TCP/IP](#) | [sendmail](#) | [sendmail Reference](#) | [Firewalls](#) | [Practical Security](#)]



Practical UNIX & Internet Security

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

Index: W

w command

[10.1.2. utmp and wtmp Files](#)

[17.3.1. systat \(TCP Port 11\)](#)

[24.2.1. Catching One in the Act](#)

-Wall option (in C) : [23.2. Tips on Avoiding Security-related Bugs](#)

WANs (Wide Area Networks) : [16.1. Networking](#)

war : [12.2.5. Defending Against Acts of War and Terrorism](#)

warrants

[26.2.4. Hazards of Criminal Prosecution](#)

[26.2.5. If You or One of Your Employees Is a Target of an Investigation...](#)

water : [12.2.1.12. Water](#)

humidity : [12.2.1.11. Humidity](#)

sprinkler systems : [12.2.1.1. Fire](#)

stopping fires with : [12.2.1.1. Fire](#)

web browsers

[18.5. Risks of Web Browsers](#)

[18.5.2. Trusting Your Software Vendor](#)

Netscape Navigator : [18.4.1. Eavesdropping Over the Wire](#)

Web documents : (see [HTML documents](#))

Web servers

access to files on

[18.3. Controlling Access to Files on Your Server](#)

[18.3.3. Setting Up Web Users and Passwords](#)

log files : [18.4.2. Eavesdropping Through Log Files](#)

on Macintosh : [18.2. Running a Secure Server](#)

web servers

[18.2. Running a Secure Server](#)

[18.2.5. Other Issues](#)

authentication users : [18.3.3. Setting Up Web Users and Passwords](#)

.htaccess file bug : [18.3.1. The access.conf and .htaccess Files](#)

multiple suppliers of : [18.6. Dependence on Third Parties](#)

as superuser : [18.2.1. The Server's UID](#)

symbolic-link following : [18.2.2.2. Additional configuration issues](#)

Weiner, Michael : [6.4.4.3. DES strength](#)

Westinghouse : [F.3.4.46. Westinghouse Electric Corporation](#)

wheel group

[4.1.3.1. The /etc/group file](#)

[4.3.6. Restricting su](#)

[8.5.2. The wheel Group](#)

who command

[8.1.3. Accounts That Run a Single Command](#)

[10.1.2. utmp and wtmp Files](#)

[17.3.1. systat \(TCP Port 11\)](#)

[24.2.1. Catching One in the Act](#)

[24.2.4. Tracing a Connection](#)

whodo command

[10.1.2. utmp and wtmp Files](#)

[24.2.1. Catching One in the Act](#)

whois command : [24.2.4.2. How to contact the system administrator of a computer you don't know](#)

Wide Area Networks (WANs) : [16.1. Networking](#)

window, time : (see [time](#))

windows (glass) : [12.2.3.3. Glass walls](#)

windows servers : (see [NSWS](#); [X Window System](#))

wireless transmission : (see [radio, transmissions](#))

wiretaps : (see [eavesdropping](#))

wiz command : [17.3.4.2. Using sendmail to receive email](#)

wizard's password (sendmail) : [17.3.4.1. sendmail and security](#)

WN server : [18.3. Controlling Access to Files on Your Server](#)

workstations, backing up : [7.2.1. Individual Workstation](#)

World Wide Web (WWW)

[18. WWW Security](#)

[18.7. Summary](#)

browsers : (see [web browsers](#))

checklist for : [A.1.1.17. Chapter 18: WWW Security](#)

documents on : (see [HTML documents](#))

eavesdropping on

[18.4. Avoiding the Risks of Eavesdropping](#)

[18.4.2. Eavesdropping Through Log Files](#)

encrypting information on : [18.4.1. Eavesdropping Over the Wire](#)

HTTP : (see [HTTP](#))

logging downloaded files : [10.3.5. access_log Log File](#)

posting breakins on : [24.6. Resuming Operation](#)

references on : [E.3. WWW Pages](#)
security mailing list : [E.1.3.10. WWW-security](#)
servers : (see [Web servers](#))
trademarks and copyrights
 [26.4.2. Copyright Infringement](#)
 [26.4.3. Trademark Violations](#)
viruses through : [11.1.5. Viruses](#)
world-writable files/directories : [11.6.1.1. World-writable user files and directories](#)
Worm program : [1. Introduction](#)
worms
 [11.1. Programmed Threats: Definitions](#)
 [11.1.6. Worms](#)
wrappers, checklist for : [A.1.1.21. Chapter 22: Wrappers and Proxies](#)
write command
 [5.5.3.1. write: Example of a possible SUID/SGID security hole](#)
 [23.2. Tips on Avoiding Security-related Bugs](#)
in Swatch program : [10.6.2. The Swatch Configuration File](#)
time-outs on : [23.3. Tips on Writing Network Programs](#)
write permission
 [5.1.7. File Permissions in Detail](#)
 [5.4. Using Directory Permissions](#)
write-protecting backups : [7.1.6.2. Write-protect your backups](#)
write-protecting filesystems : [9.1.2. Read-only Filesystems](#)
WRITE= command : [15.5.2. Permissions Commands](#)
writing
 passwords (on paper) : [3.6.5. Writing Down Passwords](#)
 programmed threats : [11.3. Authors](#)
wtmp file
 [10.1.2. utmp and wtmp Files](#)
 [10.1.3.1. Pruning the wtmp file](#)
wtmpx file : [10.1.2. utmp and wtmp Files](#)
wuftpd server : [17.3.2.4. Setting up an FTP server](#)
www user/group : [18.2.2. Understand Your Server's Directory Structure](#)

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

[Copyright](#) © 1999 [O'Reilly & Associates, Inc.](#) All Rights Reserved.

[[Library Home](#) | [DNS & BIND](#) | [TCP/IP](#) | [sendmail](#) | [sendmail Reference](#) | [Firewalls](#) | [Practical Security](#)]



Practical UNIX & Internet Security

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

Index: X

X Window System

[12.3.4.4. X terminals](#)

[17.3.21. The X Window System \(TCP Ports 6000-6063\)](#)

[17.3.21.5. Denial of service attacks under X](#)

denial of service under : [17.3.21.5. Denial of service attacks under X](#)

screen savers : [12.3.5.2. X screen savers](#)

X-rated material : [26.4.5. Pornography and Indecent Material](#)

X.500 directory service : [16.4.4. OSI](#)

X/Open Consortium : [1.3. History of UNIX](#)

xargs command

[5.2.5.1. AIX Access Control Lists](#)

[11.5.1.4. Filename attacks](#)

Xauthority facility, magic cookies : [17.3.21.4. Using Xauthority magic cookies](#)

xdm system : [17.3.21.4. Using Xauthority magic cookies](#)

XDR (external data representation) : [19.2. Sun's Remote Procedure Call \(RPC\)](#)

Xerox Network Systems (XNS) : [16.4.5. XNS](#)

xferlog file : [10.3.3. xferlog Log File](#)

xfrnets directive : [17.3.6.1. DNS zone transfers](#)

xhost command : [17.3.21.3. The xhost facility](#)

XOR (exclusive OR) : [6.4.7. An Unbreakable Encryption Algorithm](#)

XScreensaver program : [12.3.5.2. X screen savers](#)

XTACACS : (see [TACACS](#))

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

[Copyright](#) © 1999 [O'Reilly & Associates, Inc.](#) All Rights Reserved.

[[Library Home](#) | [DNS & BIND](#) | [TCP/IP](#) | [sendmail](#) | [sendmail Reference](#) | [Firewalls](#) | [Practical Security](#)]



Practical UNIX & Internet Security

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

Index: Y

Yellow Pages, NIS : [16.2.6.2. Other naming services](#)

ypbind daemon

[19.3.2.3. Making sure Secure RPC programs are running on every workstation](#)

[19.4.4.5. Spoofing NIS](#)

ypcat publickey command : [19.3.2.3. Making sure Secure RPC programs are running on every workstation](#)

yppasswd command

[3.4. Changing Your Password](#)

[8.2. Monitoring File Format](#)

ypserv daemon : [19.4.4.5. Spoofing NIS](#)

ypset command : [19.4.5. Unintended Disclosure of Site Information with NIS](#)

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

[Copyright](#) © 1999 [O'Reilly & Associates, Inc.](#) All Rights Reserved.

[[Library Home](#) | [DNS & BIND](#) | [TCP/IP](#) | [sendmail](#) | [sendmail Reference](#) | [Firewalls](#) | [Practical Security](#)]



Practical UNIX & Internet Security

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

Index: Z

Zheng, Yliang : [6.5.4.3. HAVAL](#)

Zimmermann, Phil : [6.6.3. PGP: Pretty Good Privacy](#)

zone transfers

[17.3.6. Domain Name System \(DNS\) \(TCP and UDP Port 53\)](#)

[17.3.6.1. DNS zone transfers](#)

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

[Copyright](#) © 1999 [O'Reilly & Associates, Inc.](#) All Rights Reserved.

[[Library Home](#) | [DNS & BIND](#) | [TCP/IP](#) | [sendmail](#) | [sendmail Reference](#) | [Firewalls](#) | [Practical Security](#)]



Practical UNIX & Internet Security

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

Index: Symbols and Numbers

10BaseT networks

[12.3.1.2. Eavesdropping by Ethernet and 10Base-T](#)

[16.1. Networking](#)

8mm video tape : [7.1.4. Guarding Against Media Failure](#)

@ (at sign)

with chacl command : [5.2.5.2. HP-UX access control lists](#)

in xhost list : [17.3.21.3. The xhost facility](#)

! and mail command : [15.1.3. mail Command](#)

. (dot) directory : [5.1.1. Directories](#)

.. (dot-dot) directory : [5.1.1. Directories](#)

(hash mark), disabling services with : [17.3. Primary UNIX Network Services](#)

+ (plus sign)

in hosts.equiv file : [17.3.18.5. Searching for .rhosts files](#)

in NIS

[19.4. Sun's Network Information Service \(NIS\)](#)

[19.4.4.6. NIS is confused about "+"](#)

/ (slash)

IFS separator : [11.5.1.2. IFS attacks](#)

root directory

[5.1.1. Directories](#)

(see also [root directory](#))

~ (tilde)

in automatic backups : [18.2.3.5. Beware stray CGI scripts](#)

for home directory : [11.5.1.3. \\$HOME attacks](#)

[Search](#) | [Symbols](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

[Copyright](#) © 1999 [O'Reilly & Associates, Inc.](#) All Rights Reserved.

[[Library Home](#) | [DNS & BIND](#) | [TCP/IP](#) | [sendmail](#) | [sendmail Reference](#) | [Firewalls](#) | [Practical Security](#)]