Chapter 3 Unix Overview

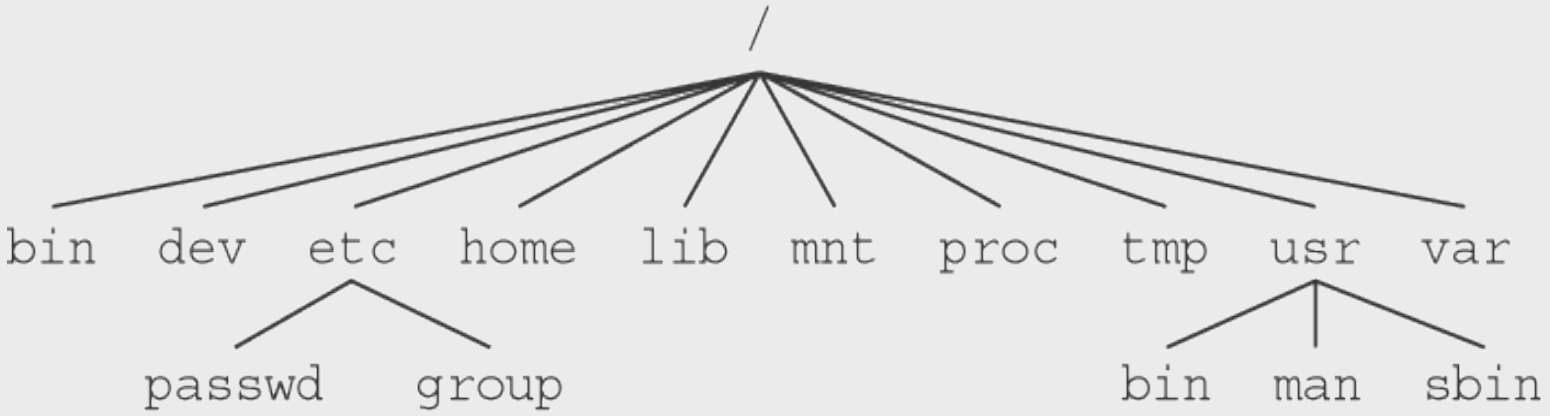


Figure 3.1 Unix file system

Directory	Purpose
/	The root directory
/bin or /sbin	Critical executables needed to boot the system
/dev	Device drivers
/etc	System configuration files such as passwords, network addresses and names,system startup scripts
/home	User home directories
/lib	Shared libraries used by programs
/mnt	Temporary mount point for file systems
/proc	Images of currently executing processes on the system
/tmp	Temporary files
/usr	A variety of critical system files, including system utilities (/usr/bin), and administration executables (/usr/sbin)
/var	Stores varying files such as /var/log, /var/mail

Table 3.1 Important Directories in the Unix file system

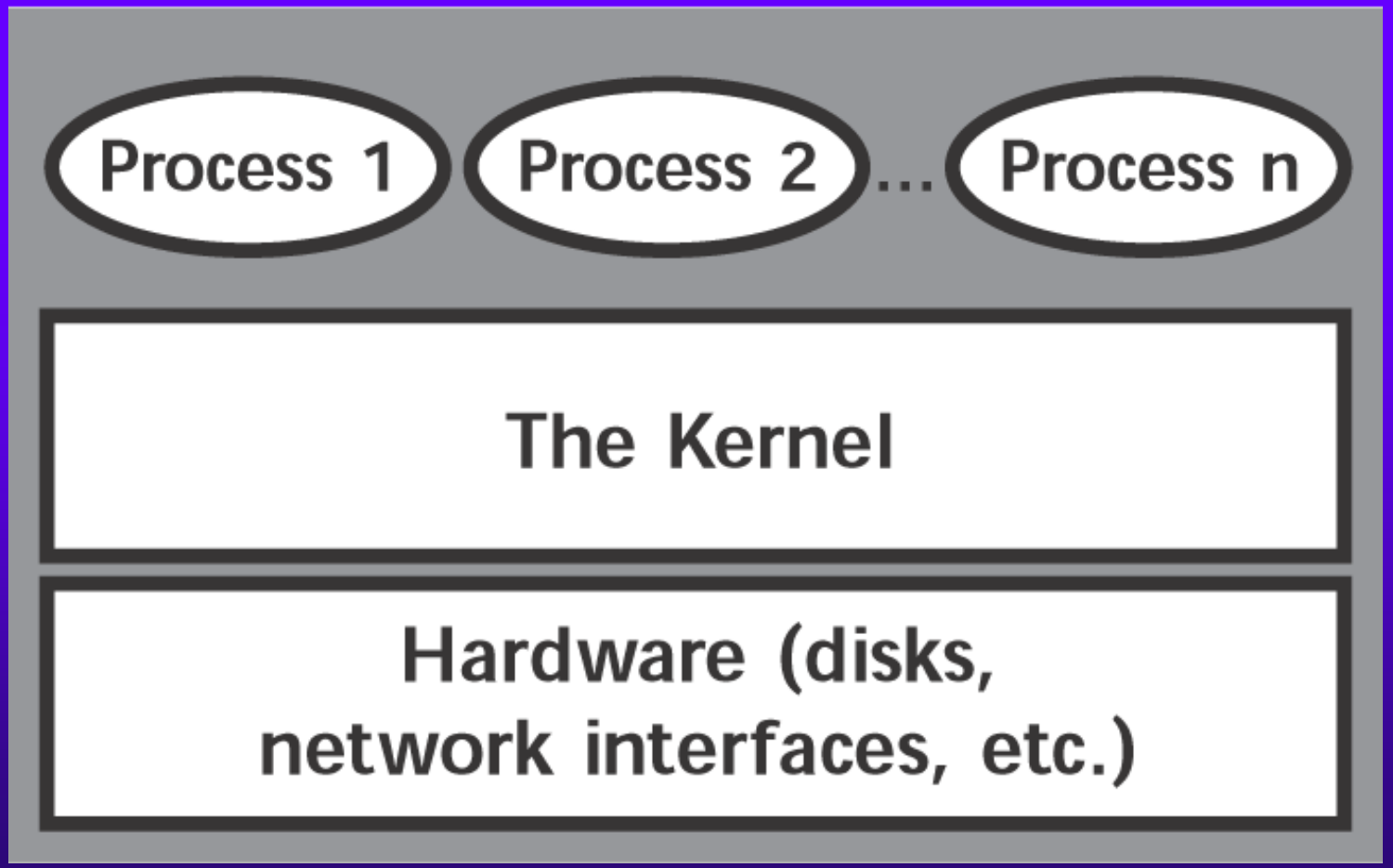


Figure 3.2 Unix Architecture

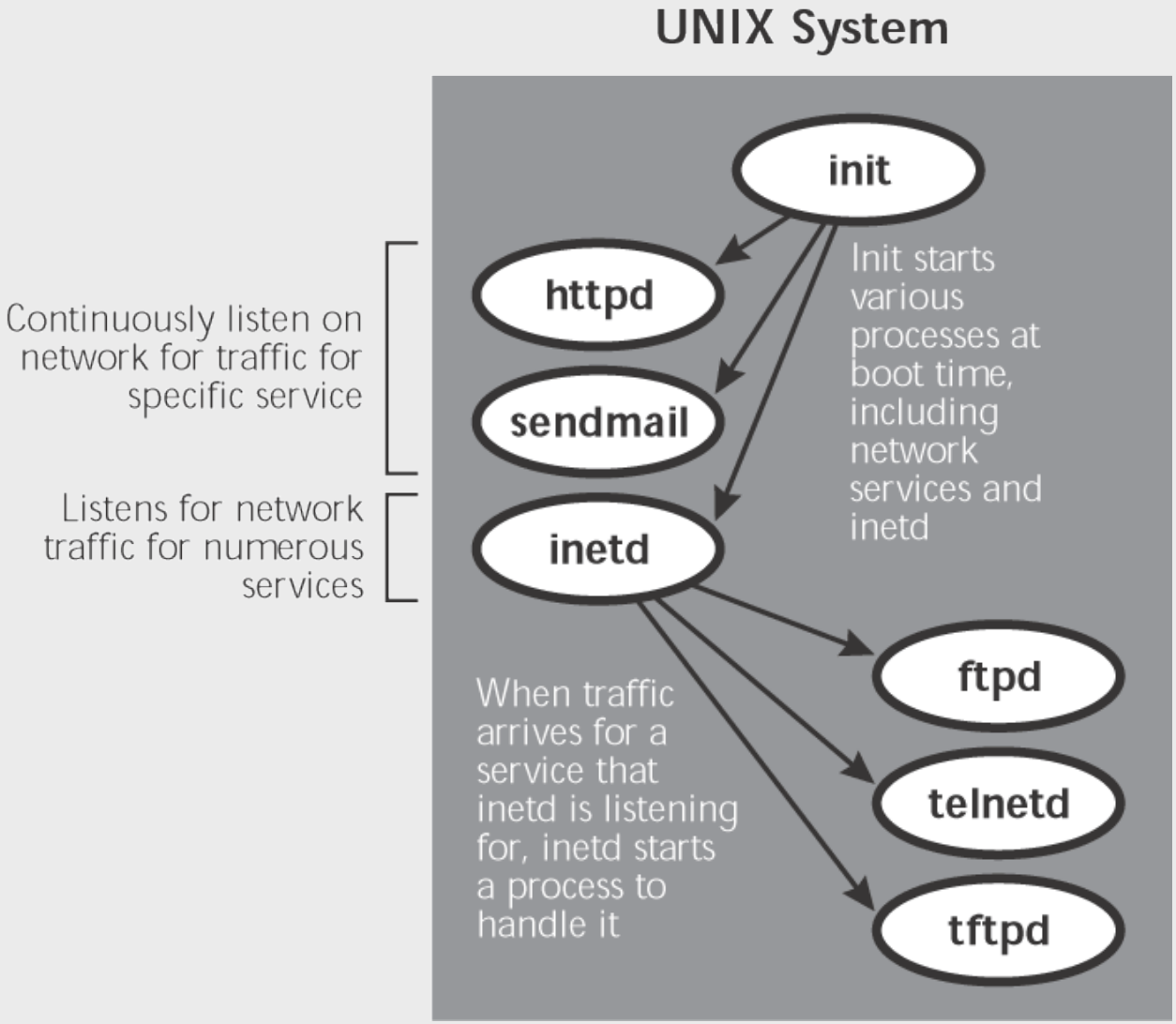


Figure 3.3 Relationship between init, inetd, and various network services

Sample `/etc/inetd.conf` file containing services spawned by `inetd`

```
# These are standard services.
#
ftp       stream tcp   nowait root   /usr/sbin/in.ftpd       in.ftpd
telnet    stream tcp   nowait root   /usr/sbin/in.telnetd    in.telnetd
#
shell     stream tcp   nowait root   /usr/sbin/in.rshd       in.rshd
login     stream tcp   nowait root   /usr/sbin/in.rlogind    in.rlogind
#exec     stream tcp   nowait root   /usr/sbin/in.rexecd     in.rexecd
```

Note that this line is commented out with a #, so the exec service will not be activated by `inetd`

/etc/inetd.conf file format

- Service name (port # defined in /etc/services)
- Socket type (stream or dgram)
- Protocol (tcp, udp, rpc/tcp, or rpc/udp)
- Wait status (wait or nowait)
- Username (service run as)
- Server program
- Server program arguments

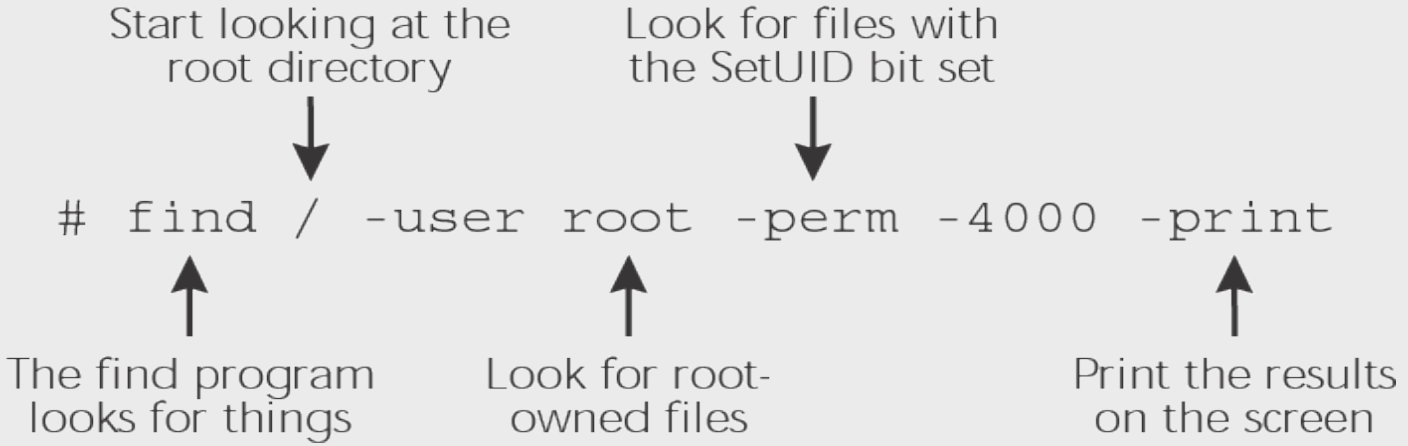
Use of inetd.conf to create backdoor listeners and attack relays

Common Unix Administration Tasks

- Vulnerability of using “.” in your search path
  $PATH
- Showing all running processes
  `ps -aux`
  `ps -aef`
- Killing/restarting processes
  `kill -HUP` pid
  `killall -HUP` inetd
- /etc/passwd file
- Unix permissions rwxrwxrwx
  `chmod` command

Common Unix Administration Tasks (cont.)

- SetUID programs
  - Executes with permissions of its owner, not of its user
  - /etc/passwd setUID root r-s--x--x
  - Creating setUID files
    - #chmod 4741 foo
- Finding setUID files



- Vulnerability of setUID programs

Unix Trust

Alice's name is in
Bob's `/etc/hosts.equiv`
or `~/.rhosts` file

- Authenticating users on behalf of another machine
- R-commands
  - rlogin
  - rsh
  - rcp
- Weakness of r-commands
  - Actions based on IP address of trusted machine
  - Undermining r-commands via IP address spoofing

Logs and Auditing

- Syslog daemon
  - Syslogd
- /etc/syslog.conf
- /var/log
  - /var/log/messages
  - /var/log/http
- Accounting files
  - Utmp
    - Records who is currently logged into a system
    - used by who command
  - Wtmp
    - records all logins and logouts
    - used by last command
  - lastlog
    - Records time and location of each user's last login to system

Network File System (NFS)

- mountd
- Nfsd
- Share only folders that require sharing
- Export files only to hosts requiring access
- Carefully assign permissions to shared files
- Avoid NFS sharing across the Internet
- Alternatives
  - Secure ftp
  - IPSec-based VPN