Linux Overview

Amir Hossein Payberah
payberah@gmail.com

1

Agenda

- ➲ Linux Overview
- ➲ Linux Distributions
- ➲ Linux vs Windows
- ➲ Linux Architecture
- ➲ Linux Security

What is Linux?
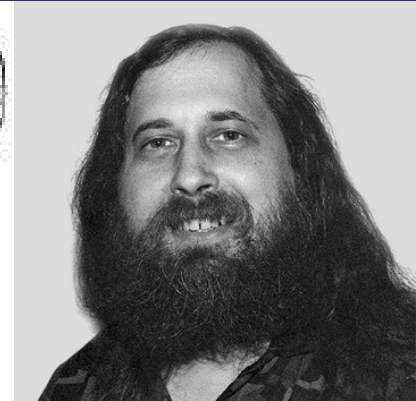
- Similar Operating System To Microsoft Windows, Sun Solaris, Mac OS But It Is Very Unique.
- Linux Source Code Is Completely Free!
- Many Distributions Built For All PC Architectures And Designs.
- Reliable, Efficient, Gaining Popularity.

Linux History

➲ History and People
- Richard M. Stallman
- No Free Unix
- Linus Travolds
- Alan Cox

Why Linux?

- ➲ It's free!
- ➲ Open Source (modifiability, extensibil-ity, ...)
- ➲ Works on several platforms
- ➲ Robustness
- ➲ Widespread Usage
- ➲ Tons Of Applications (Free).

Linux Features

- ⮑ Monolithic kernel (but well-defined inter-faces)
- ⮑ Multi-tasking
- ⮑ Multi-user capability
- ⮑ Architecture Independence (PCs, Alpha, Sparc,…)
- ⮑ Support for Posix standard
- ⮑ Several Executables formats
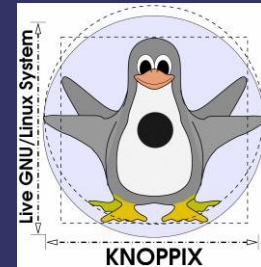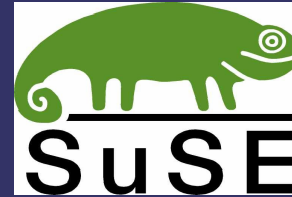- ⮑ Several File Systems
- ⮑ Several network protocols

Agenda

- ➲ Linux Overview
- ➲ Linux Distributions
- ➲ Linux vs Windows
- ➲ Linux Architecture
- ➲ Linux Security

Linux Distributions

Rank of Distributions

Distribution	Rank from Google
Debian	1
Red Hat	2
Mandrake	3
Caldera/SCO	4
Slackware	5
SuSE	6
TurboLinux	7
Gentoo	8

Debian

- ➲ Advantages:
  - Stable server system
  - Suitable for learning and engineering pur-
    poses

- ➲ Disadvantages:
  - Non-friendly
  - Detailed administration and installation

Mandrake

➲ Advantages:
- Excellent installer GUI
- Ease of administration
- Proper distribution for Desktop clients

➲ Disadvantages:
- Drawback in terms of software as a server

RedHat

⤷ Advantages:
- Best known Linux distribution in corporate market
- Supported by the majority of software vendors
- Service level and support agreement
- Suitable for both desktop clients and serv-ers
- Easy installation and administration

Suse

⮕ Advantages:
- ● Widely used Linux distribution in corporate market
- ● Supported by the majority of software vendors
- ● Service level and support agreement
- ● Suitable for both desktop clients and serv-ers
- ● Easy installation and administration
- ● Excellent graphical management tool both for administrators and end-users.

Which Distribution?

- ➲ **SuSE** is advised for new Linux users. Desktop users will like it.

- ➲ **RedHat Server Edition** is the best solution for servers.

Agenda

- Linux Overview
- Linux Distributions
- Linux vs Windows
- Linux Architecture
- Linux Security

Fundamental Difference between Linux & Windows

➲ One fundamental difference between the two systems is the fact that Linux is "open source".

➲ This means that unlike Windows where you only get access to the compiled programs that you run on your machine, with Linux you also get the original computer code to examine and tweak (modify) at your leisure.

➲ This also goes to show that Linux users are more advanced

Comparing Applications

- ⮑ Linux falls short in the number of different applications available for it.
- ⮑ There are much more various applications available for Microsoft since the population of Window's users is greater than Linux's.

Comparing Applications (Cont.)

- ➲ Linux programs are distributes freely since they are not developed by commercial software companies, but instead are created under the GNU Public License, which makes the software free

- ➲ Linux software lacks the GUI and is therefore not "liked" by many users

- ➲ Windows has its own share of problems – the fact that some software is not compliant for different versions of windows (i.e. Windows 95/98) and that many times the GUI concept is overused such that command arguments cannot be passed to the program

Cost Comparison *(in 1999)*

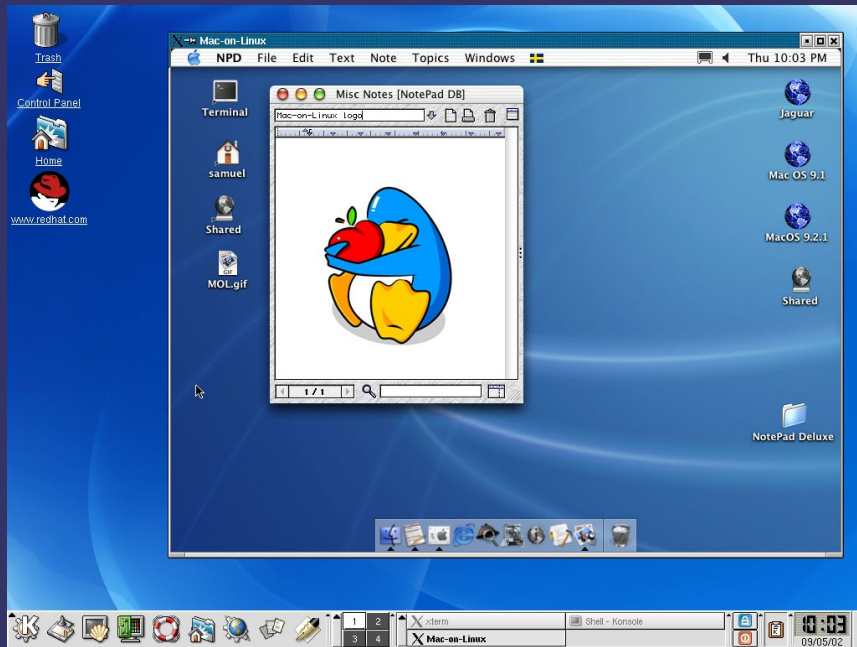| Item	Linux	NT
Server OS	$30	$700
10 Client access	0	$2700
10 Workstations OS	0	$370
Office Suite	$1690	$4080
Total	$1720	$9730

Comparing GUI

- ➲ Linux contains X-Windows with many interfaces
  - GDK
  - KDE
- ➲ Linux offers a choice of many desktops thus allowing the user to work in different windows on different desktop for convenience
- ➲ Windows, on the other hand, is limited to the way the application windows are laid out on the screen
- ➲ Windows GUI also has been known for its large memory requirements, where it usually uses a huge chunk of RAM for visual components

Linux GUI

LFS Project Homepage - Mo | linux.odp - OpenOffice.org In | LinuxvsWindows.ppt - Open | Linux.ppt - OpenOffice.org In

root@linux

SuSE Linux 9.3 (i586) VERSION = 9.3

Kernel: 2.6.11.4-20a-default
KDE: 3.4.0 Level "b"

Intel(R) Pentium(R) 4 CPU 3.00GHz
CPU: 20%
MHz: 3001.458
Cache: 1024 KB

RAM: 387 MB / 1012 MB
Swap: 3 MB / 1028 MB

/   9305 MB / 31%
/home   21254 MB / 52%
/mnt/win_c 0 MB / 0%
/mnt/win_d 0 MB / 0%
USB-Stick 0 MB / 0%

Download: 9.7 kb/s   (1029.8Mb)
Upload: 0.0 kb/s   (708.8Mb)
IP: 10.10.10.50

Uptime: 1d 08:31
Time: 16:48:57
Date: 29. Aug 2005

August 2005
Su Mo Tu We Th Fr Sa
    1 2 3 4 5 6
 7 8 9 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30 31

email1:
email2:
email3:

Firefox

دوشنبه
۷
شهریور

Linux advantages in Kernel and the OS environment

- ➲ Linux support multiple architecture.
- ➲ Linux program installation seems to be easier since it only requires a restart when hardware device has been changed.
- ➲ Linux supports multiple copies of the Kernel on the system such that if an error is encountered and the Kernel becomes corrupted, a different copy of the Kernel can be used to boot up the system.

Security Comparison

- ⮑ Linux seems to be more prepared for pro-tecting itself because of the beginning de-velopments of Linux, UNIX, and FreeBSD which were aimed at top notch security
- ⮑ Linux allows does not create registry keys in a way Windows does allowing a user to browse installed components registry keys, which contain important information
- ⮑ Linux is more virus proof since viruses – ma-licious programs either cannot be run auto-matically on the Linux machine
- ⮑ Windows is often known for a large amount of loop holes

Reliability Comparison

- OS it must not crash, even under extreme loads.
- OS should process requests even if the operating system or hardware fails
- Windows seems to be less stable even though the latest versions of Windows – 2000 and XP are far more improved than the incredibly buggy Windows 95

Agenda

- ➲ Linux Overview
- ➲ Linux Distributions
- ➲ Linux vs Windows
- ➲ Linux Architecture
- ➲ Linux Security

What is Kernel?

- ➲ Modules or sub-systems that provide the operating system functions.
- ➲ The Core of OS

Type of Kernel

- Micro kernel (Modular kernel)
- Monolithic kernel

Micro Kernel

- ➲ It includes code only necessary to allow the system to provide major functionality.
  - IPC
  - Some memory management
  - Low level process management & scheduling
  - Low level input / output
- ➲ Such as Amoeba, Mach and …

Monolithic Kernel

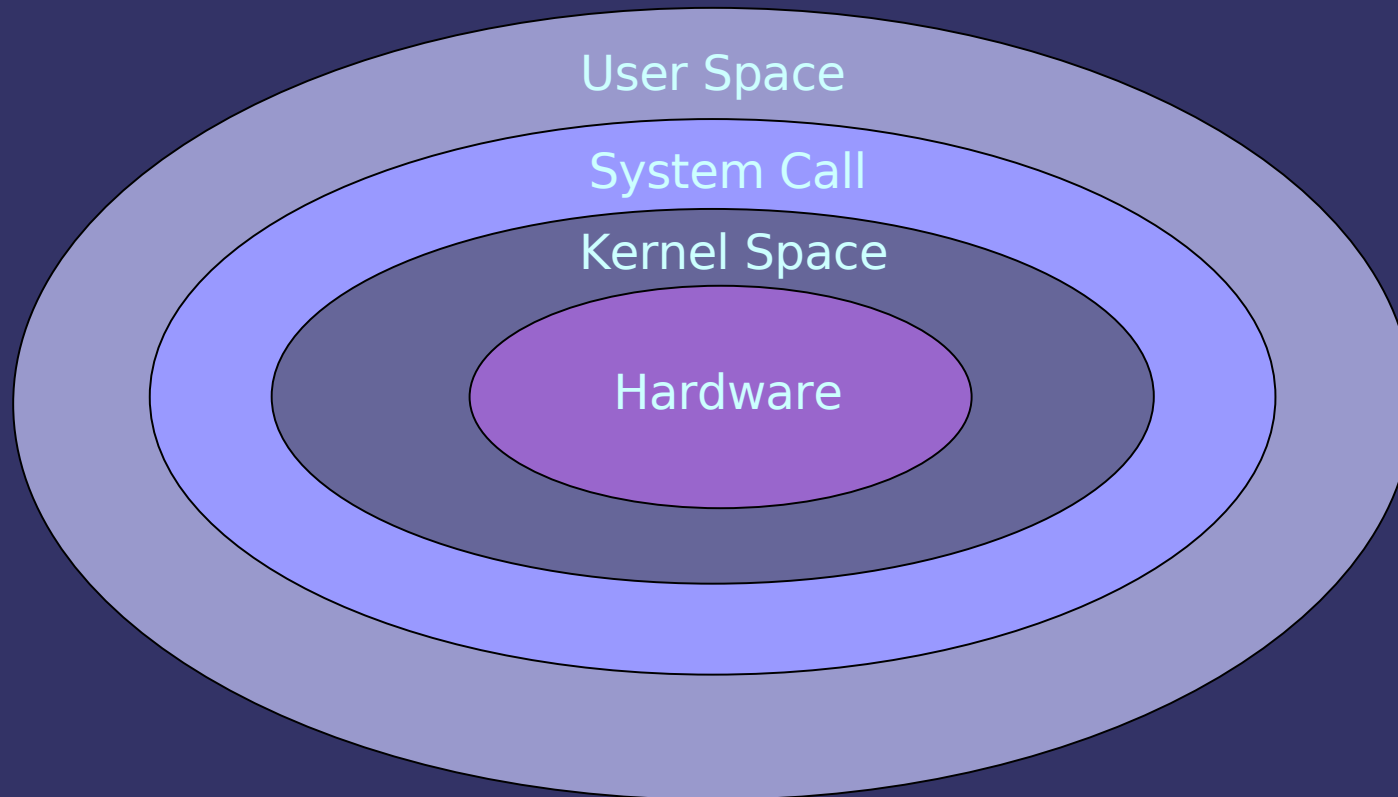- ➲ It includes all the necessary functions.
- ➲ Such as Linux and …

Monolithic vs Micro Kernel

- ⮕ Micro
  - Flexible
  - Modular
  - Easy to implement
- ⮕ Monolithic
  - Performance

Kernel Architecture

User Space

System Call

Kernel Space

Hardware

User Space

➲ The User Space is the space in memory where user processes run.

➲ This Space is protected.
- The system prevents one process from interfering with another process.
- Only Kernel processes can access a user process

Kernel Space

- ➲ The kernel Space is the space in memory where kernel processes run.
- ➲ The user has access to it only through the system call.

System Call

- ➲ User Space and Kernel Space are in different spaces.

- ➲ When a System Call is executed, the arguments to the call are passed from User Space to Kernel Space.

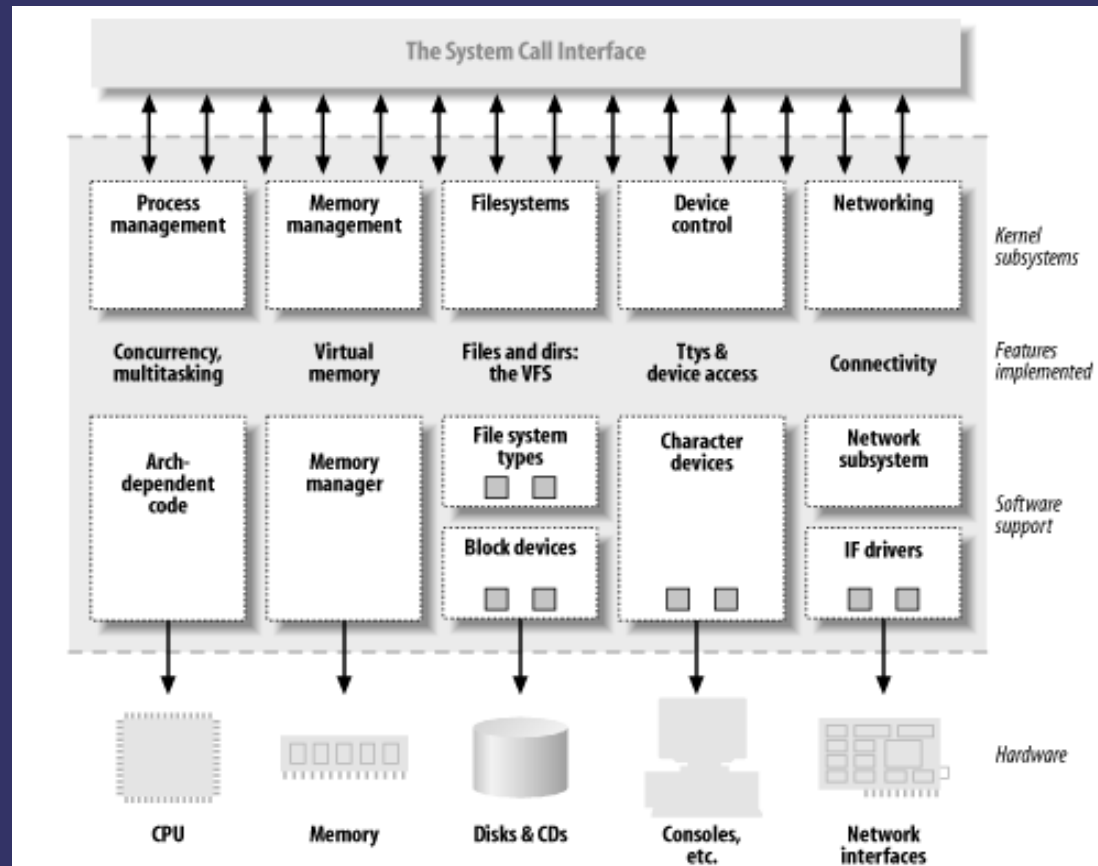- ➲ A user process becomes a kernel process when it executes a system call.

Kernel Functional Architecture

- File System
- Process Management
- Device Control
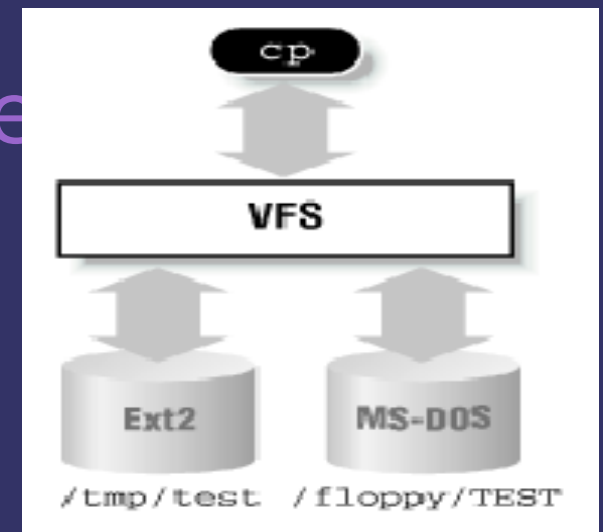- Memory Management
- Networking

Kernel Functional Architecture

File System

- ➲ It is responsible for storing information on disk and retrieving and updating this information.
- ➲ It manages all the different file sys-tem.
- ➲ In Linux everything is file

Process Management

- ➲ The Unix OS is a time-sharing system.
- ➲ Every process is scheduled to run for a period of time (time slice).
- ➲ Kernel creates, manages and deletes the processes

Device Control

- ➲ On of the purpose of an OS is to hide the system's hardware from user.
- ➲ Instead of putting code to manage the HW controller into every application, the code is kept in the Linux kernel.
- ➲ It abstracts the handling of devices.
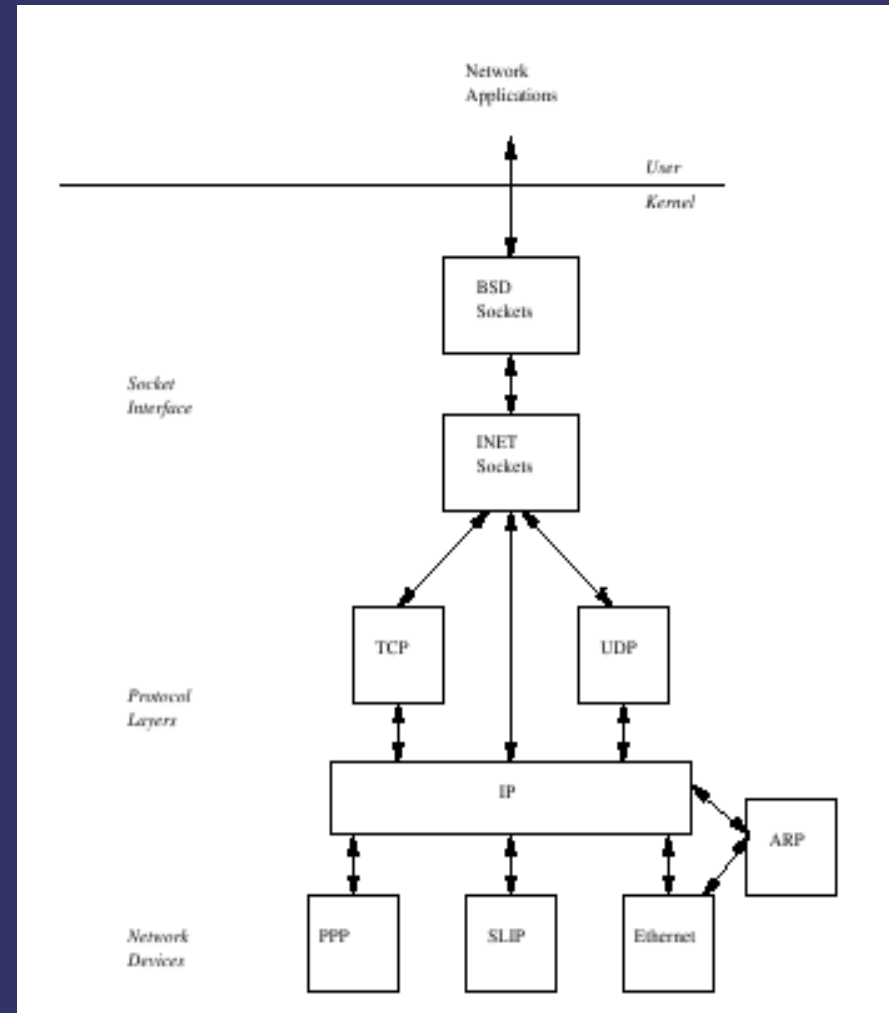 - All HW devices look like regular files.

Memory Management

- ➔ Physical memory is limited.
- ➔ Virtual memory is developed to overcome this limitation.
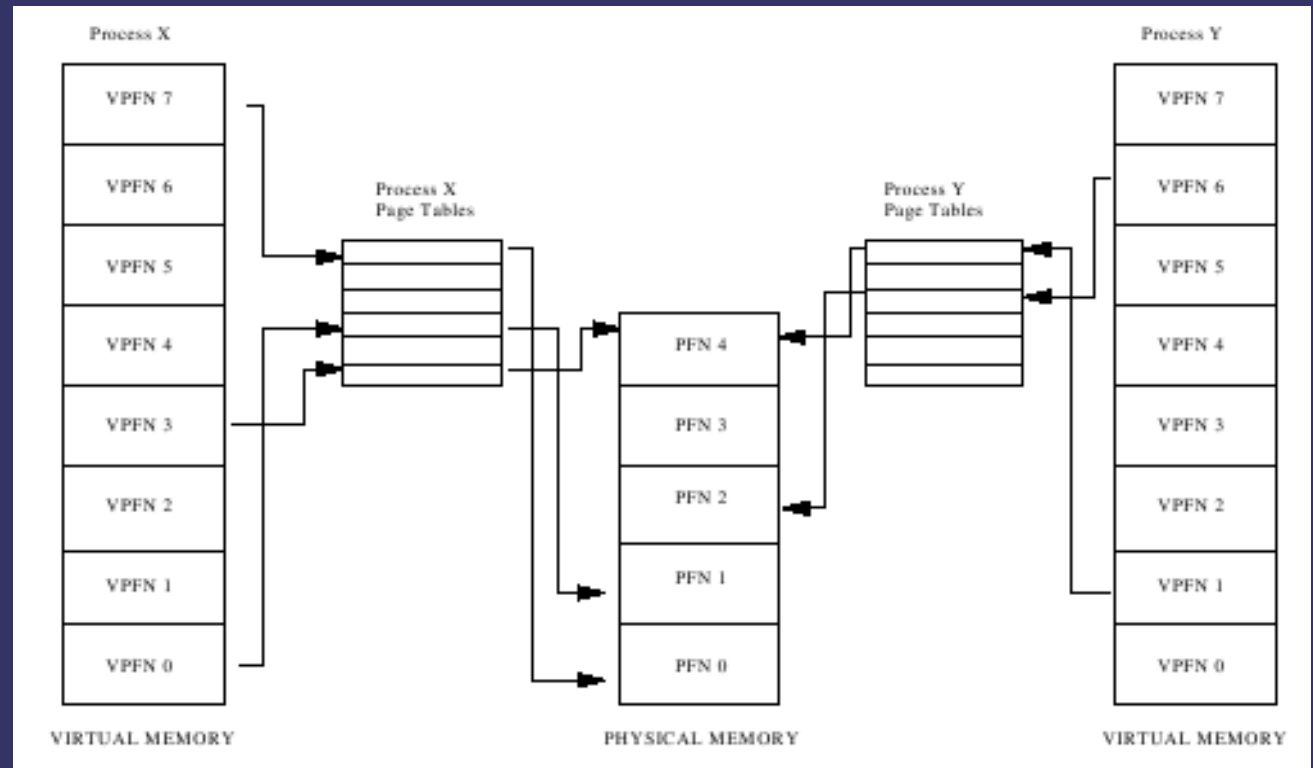
Networking

⮑ Most network operations are not specific to a process: incoming packets are asynchronous events.

⮑ The packets must be collected, identified, and dispatched before a process takes care of them.

Agenda

- ➲ Linux Overview
- ➲ Linux Distributions
- ➲ Linux vs Windows
- ➲ Linux Architecture
- ➲ Linux Security

Security Setup

- ➲ Boot Security
- ➲ Kernel Security
- ➲ Operating System Security
- ➲ User and Group Security
- ➲ Root Security
- ➲ File System Security
- ➲ Application Security
- ➲ Network Security

Boot Security

- ➲ Boot configuration is decided by LILO (Linux Loader) or GRUB (Grand Unified Boot Loader)
- ➲ Set boot loader password
- ➲ Set secure permission for configura- tion files (600)

Kernel Security

- ➲ One of the most important ways to keep Linux secure is to ensure a patched kernel
- ➲ Check your kernel version
- ➲ Third-party kernel patches for en-hanced security:
  - Linux Intrusion Detection System – for en-suring integrity of critical files
  - Secure Linux Patch – prevent common buf-fer overflows, and simple security meas-ures

Operating System Security

- ➲ Check processes
- ➲ Check installed software
- ➲ Check Cron and At
  - ● Both can be misused to install time-bombs on the system.
- ➲ Do Linux auditing
  - ● Using syslogd
  - ● Recent logins
  - ● Last login time for all users
  - ● Last failed logins
  - ● Security related events

User and Group Security

- ➲ User accounts are created in */etc/passwd*
- ➲ Hashed passwords, password and account lockout policies are in */etc/shadow*
  - No dormant or generic accounts present
  - All system (non-user) accounts have /bin/false for the shell
  - Every account in passwd has a corresponding entry in shadow
  - Only one line contains 0 in the uid field in the passwd file

Root Security

- ➲ No user must login directly as 'root'
- ➲ Administrators must login with their own accounts, and then use 'su' to become root.
- ➲ This ensures accountability
- ➲ Viable alternative is the 'sudo' utility.

File System Security

- ⮑ Unix Permissions are applicable to three entities:
  - Owner of the file (everything in Unix is a file)
  - Group owner of file
  - Everyone else
- ⮑ Three main permissions apply, with numeric representations
  - Read = 4
  - Write = 2
  - Execute = 1

File System Security *(Cont.)*

- ⮑ Disk usage can be periodically verified
- ⮑ SUID and SGID files are executables that can be executed by anyone, but they execute with privileges of owner (usually root) or group – very critical checks!
- ⮑ File Integrity can be verified:
  - Size and timestamp – can be modified to fool the auditor
  - MD5 hashes – secured method, but tedi-ous

Application Security

⇨ Linux systems can be used as
- File Servers – Samba – Windows-compat-ible file server
- Print Servers – lpd, cups, etc.
- Mail Server – Sendmail, Qmail, Postfix
- VPN Server – FreeS/WAN
- Databases – PostgreSQL, MySQL, Oracle
- DNS Servers – BIND
- LDAP Servers
- Time Servers

Network Security

- ➲ Services are started by /etc/rc.d scripts and xinetd
  - Xinetd services are configured by indi-vidual files in /etc/xinetd.d/
- ➲ Close unnecessary network connec-tions
- ➲ Entries in /etc/hosts.equiv and /etc/hosts.lpd are critical
  - They allow users from those hosts to con-nect without supplying a password!

Linux Security Conclusion

- ➲ Linux is not secure in default configuration
- ➲ Security can be added to a very high level, but must be balanced with functionality
- ➲ The correct Linux distribution must be chosen, and min-imum installation done
- ➲ Patches must be diligently applied
- ➲ Syslog logs must be exported and analyzed periodically
- ➲ Network Services must be kept to a minimum
- ➲ User and groups must be periodically audited
- ➲ File/folder access control lists must be set
- ➲ File Integrity software may be used in high-security in-stallations
- ➲ Application-specific security measures are also a must

Questions

Comments