# SECURITY

# OF

# WINDOWS SYSTEM

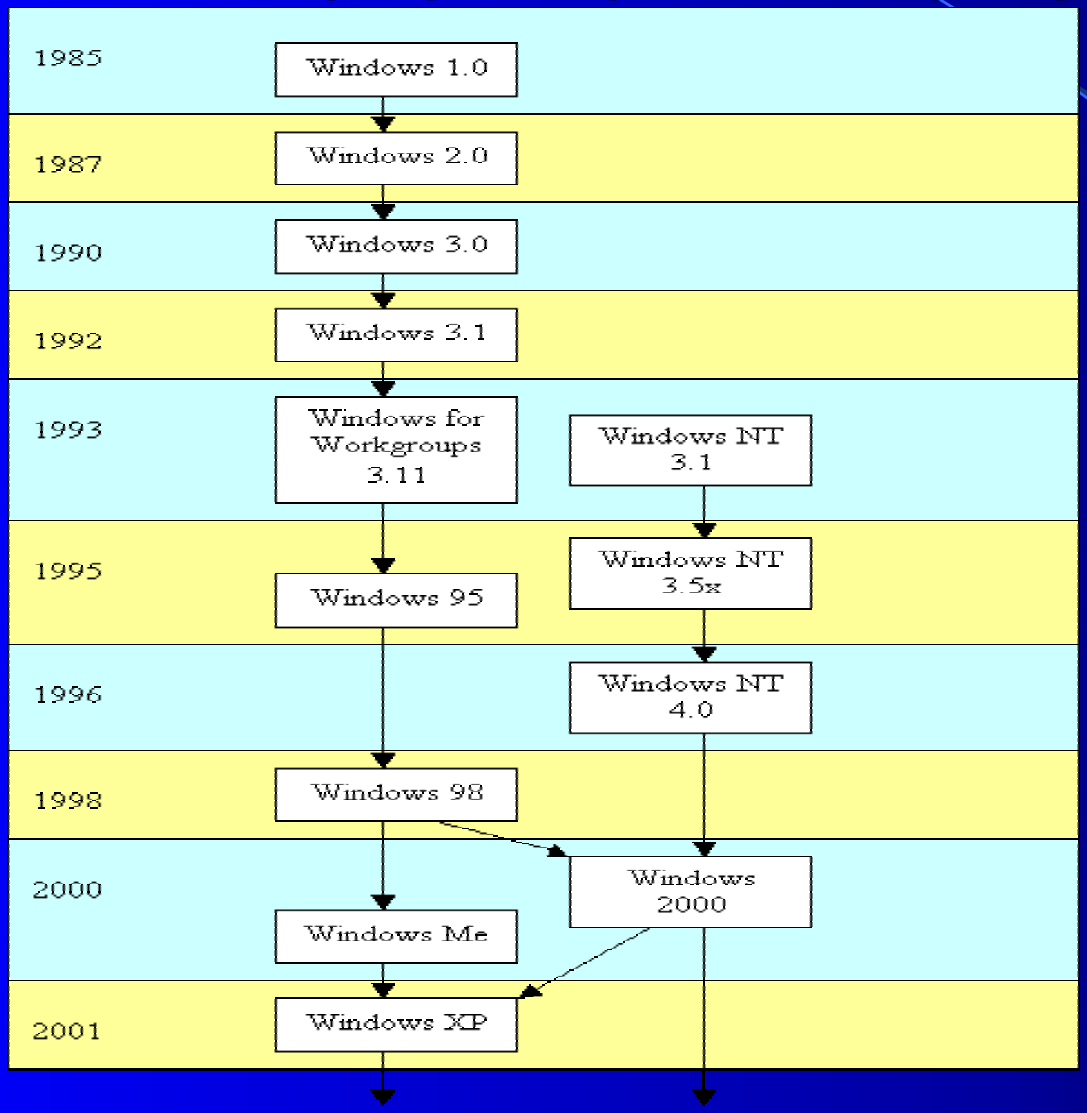
# WHAT IS AN OPERATING SYSTEM

- Manager for the computer
  - hard disk
  - printer
  - monitor screen
  - memory
  - .....

# THE EVOLUTION OF OPERATING SYSTEMS

- Before 1960s, programs and jobs, were all loaded on to a single tape
- In the 1960s, the concept of ”multiprogramming”
- The end of 1960s, UNIX was born
  - it has grown to become the most widely used Operating System
- The year of 1985, Microsoft released Window 1.0
- In the early 1990s, Microsoft introduced its new operating system—Windows NT

# THE HISTORY OF WINDOWS FAMILY



# WINDOWS 98

- **Windows 98**, released in June of 1998
- Integrated Web Browsing
- Active Desktop
- Internet Explorer 4.0 New browser
- ACPI supports

# WINDOWS 98

- FAT32 with Conversion
- Multiple Display
- New Hardware support
- Win32 Driver model Uses same driver model as Windows NT 5.0 Disk Defragmentor Wizard

# WINDOWS 2000

- **Windows 2000** provides an impressive platform of Internet, intranet, extranet, and management applications that integrate tightly with Active Directory.
- You can set up virtual private networks - secure, encrypted connections across the Internet - with your choice of protocol.
- You can encrypt data on the network or on-disk.
- You can give users consistent access to the same files and objects from any network-connected PC.
- You can use the Windows Installer to distribute software to users over the LAN.

# PROCESS AND FILE ACCESS

- Process
  - Program as a file stored on the hard disk or floopy
  - Process as the program stored in memory
- File Access
  - Gathering up requests and accessing the disk at once

# WINDOWS NT INTERNALS

- Workstation and Server
  - Workstation can function either as clients within a network consisting of one or more window NT servers, or they can be part of peer-to-peer network such as a workgroup
  - Servers provide additional functionality, such as maintaning domain-wide user and security information as well as providing authentication services

# ADVANTAGES OF WINDOWS NT

- Microsoft has called Windows NT a ”multiple-personality operating system”
  - It was desinged to support more than one application programming interface(API)
  - Designed as a module operating system
  - Easily use
  - Smaller code be needed
  - Sharing certain code

# SECURITY BASICS

- Real threats
  - Hacking has become an almost cult phenomenon with newgroups, magazines, and even their own language
  - Hackers are not just randomly trying systems across the country
  - Most system administrators are aware that there needs to be seurity
- Dictionary attack
- Trojan horses

# WINDOWS NT SECURITY BASICS

- Unique identifier
- SAM – Security Account Manager
- LSA – Local Security Authority
- SRM – Security Reference Monitor
- SSO – Single Sign On
- SID – Security Identifier

# WHAT WE CAN DO ABOUT DANGER

- Don’t just follow a checklist to secure our system
- Try to become a hacker (3 steps by doing this)
  - learn more about security
  - find security holes
  - begin to think like a hacker

# SECURITY POLICY

- A set of decisions that collectively determines an organization's posture or attitude toward security
- The security policy for you IS department shoud contain thinking like :
  - what defines necessary access
  - In what circumstances is particular access necessary
  - who decides what access is necessary
  - in which cases should access furnishings be increased or decreased

# SECURITY POLICY

…

- can a user lost access? if so, how?
- how can the user get access back one it is lost
- how often are the access privileges reviewed
- who is authorized to request that a new user be created
- how is this request reported to the system administrators
- is the creation of a new user, adding a user to a group, and similar changes documented in some kind of log file
- are users removed when the employee leaves the company, or are they just deactivated