FANSHAWE

INFO-6003

O/S & Application Security

Week 02

FANSHAWE

Agenda

- Virtual Networks Revisited
- Virtualization & Security
- Operating Systems & History
- Need for O/S Security
- Access Control Concepts
- Lab Details

FANSHAWE

Virtual Networks Revisited

FANSHAWE

Virtual Networks

- Pay attention to how your virtual networks are set up
- It is important to know what level of network access your VMs have, especially when conducting network scans, etc.
- If you are testing Malware, ensure you are isolated from any production networks

FANSHAWE

Virtual Networks

- If you require internet connectivity on your virtual machine and it doesn't exist, ensure you go through the basic troubleshooting steps
  - Check what type of virtual network connection you have and that NAT or Bridged is selected
  - Ensure that the virtual NIC is connected
  - Check your IPv4 settings
    - DHCP
    - Static

FANSHAWE

Virtual Networks

- There may be times where the VM doesn't establish a connection after you have done troubleshooting
- You may have virtual networks set up incorrectly
- You can always start with a clean slate in VMWare Workstation by going to Edit -> Virtual Network Editor and clicking on the "Restore Default" button which is located on the bottom left of the menu

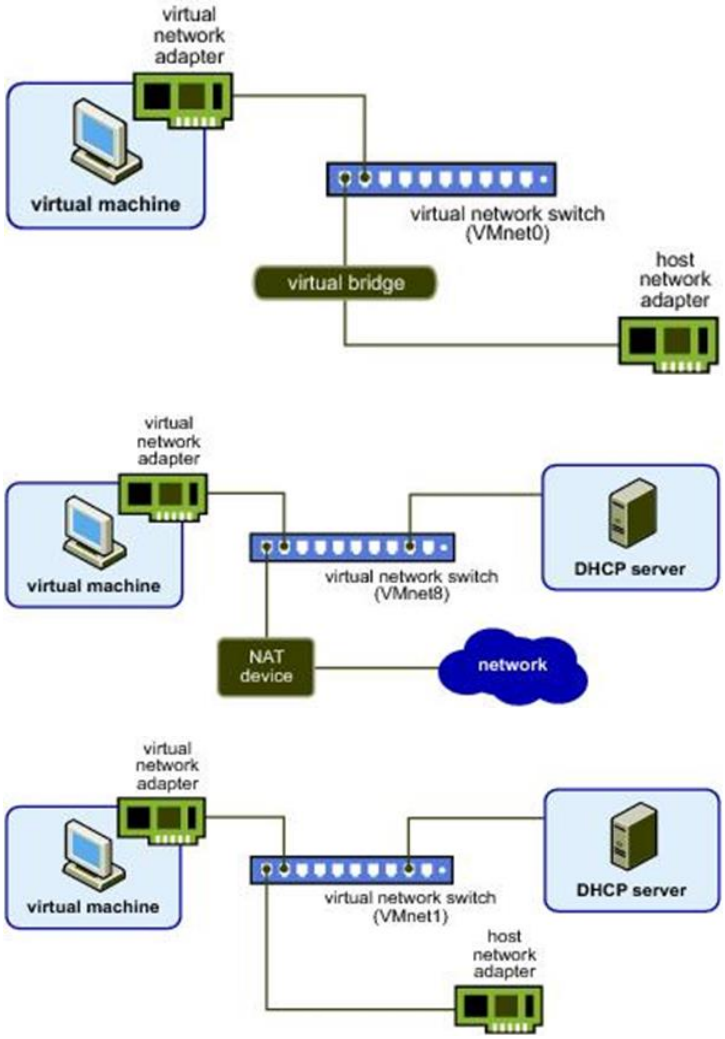
FANSHAWE

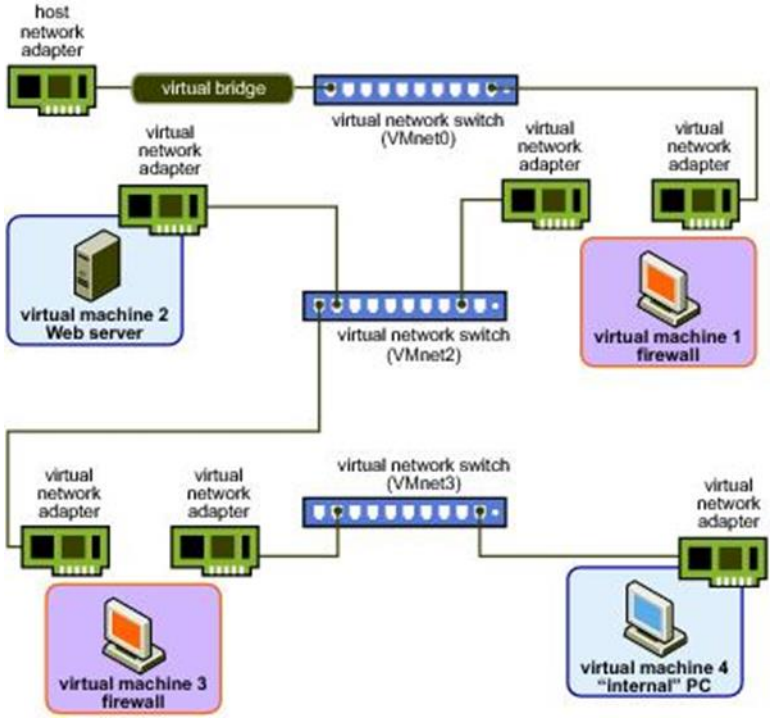
Virtual Switches

Network Type	Switch Name	DHCP
Bridged	VMnet0	No
NAT	VMnet8	Yes
Host-only	VMnet1	Yes

- Can be viewed through the Virtual Network Editor
- By Default there are three network types
  - Bridged
  - NAT
  - Host-Only

Virtual Network Switches





FANSHAWE

Virtualization & Security

FANSHAWE

Virtualization & Security

- Security concerns include:
  - Guest OS isolation
    - Ensuring that programs executing within a guest OS may only access and use the resources allocated to it
  - Guest OS monitoring by the hypervisor
    - Which has privileged access to the programs and data in each guest OS
  - Virtualized environment security
    - Particularly image and snapshot management which attackers may attempt to view or modify

Virtualization & Security

- If the O/S running on physical hardware can be compromised, it will also be vulnerable when running in a virtualized environment
- Need to ensure that network traffic is isolated between guest Operating Systems if they do not need to communicate
- Ensure that the Hypervisor is secured as a compromised guest O/S may access the Hypervisor if such vulnerabilities exist
  - This is known as “VM Escape”

FANSHAWE

Virtualization & Security

Organizations using virtualization should:

- **Carefully plan the security of the virtualized system**
- **Secure all elements of a full virtualization solution and maintain their security**
- **Ensure that the hypervisor is properly secured**
- **Restrict and protect administrator access to the virtualization solution**

FANSHAWE

Hypervisor Security

- The Hypervisor should be:
  - Secured using a process similar to securing an operating system
  - Installed in an isolated environment
  - Configured so that it is updated automatically
  - Monitored for any signs of compromise
  - Accessed only by authorized administration

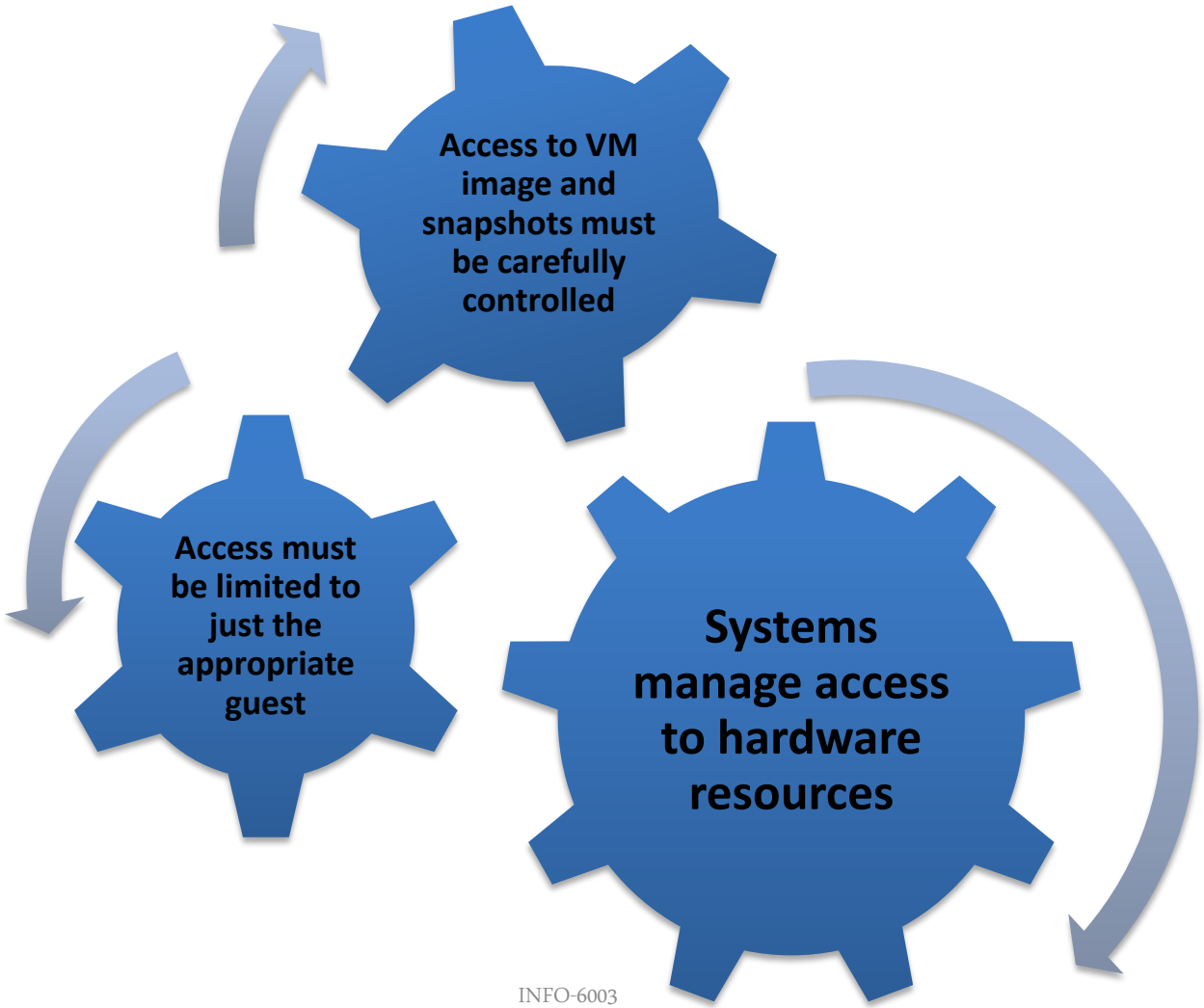
FANSHAWE

Hypervisor Security

- May support both local and remote administration so must be configured appropriately
- Remote administration access should be considered and secured in the design of any network firewall and IDS capability in use
- Ideally administration traffic should use a separate network with very limited access provided from outside the organization

FANSHAWE

Virtualization Infrastructure Security



FANSHAWE

Virtualization Infrastructure Security

- Virtualized systems manage access to:
  - Hardware resources such as disk storage and network interfaces
  - This access must be limited to just the appropriate guest OSs that use any resource
  - The configuration of network interfaces and use of an internal virtual network may present issues for organizations that wish to monitor all network traffic between systems

Virtualization Infrastructure Security

- Hosted virtualized systems, as typically used on client systems, pose some additional security concerns
- These result from the presence of the host OS under, and other host applications beside, the hypervisor and its guest OSs
- Hence there are yet more layers to secure. Further, the users of such systems often have full access to configure the hypervisor, and to any VM images and snapshots

FANSHAWE

Virtualization Infrastructure Security

- It is possible to design a host system and virtualization solution that is more protected from access and modification by the users
- This approach may be used to support well-secured guest OS images used to provide access to enterprise networks and data, and to support central administration and update of these images
- Cloud Providers often use an API to allow clients access to virtual machine hypervisors which allow for an automated approach to configuring new VMs

FANSHAWE

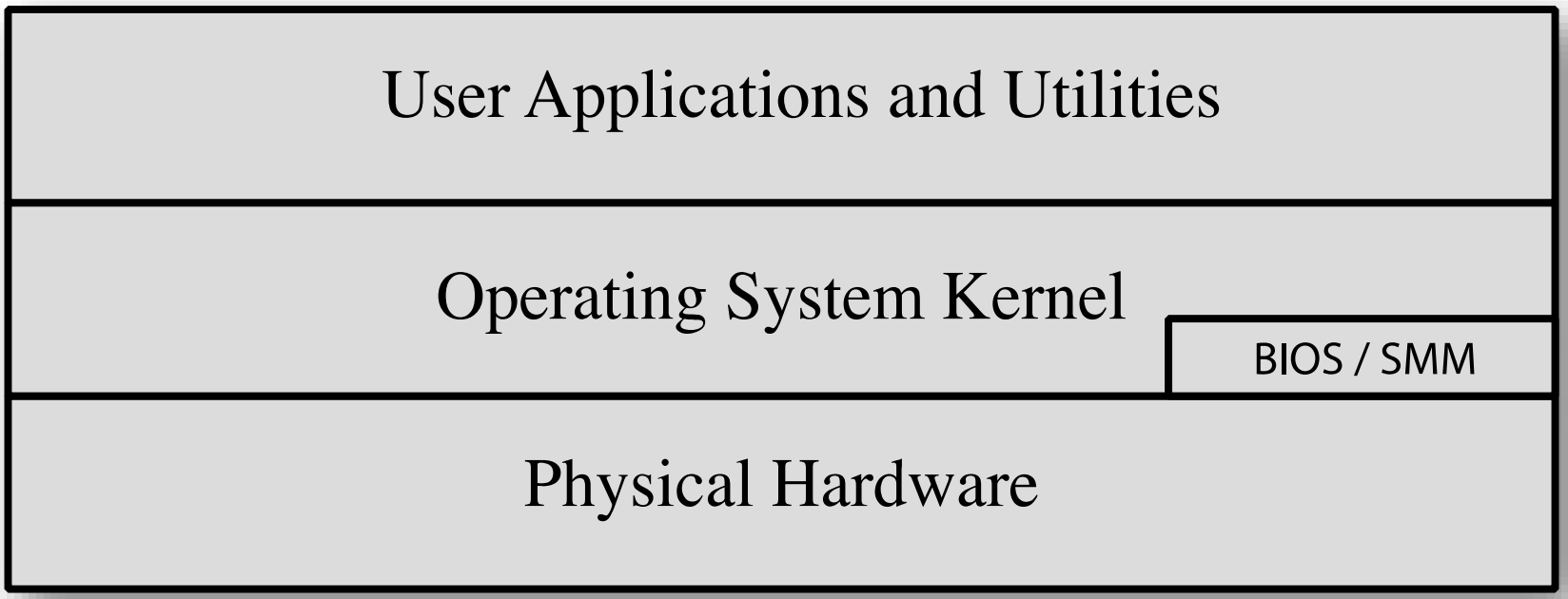
Operating Systems & History

FANSHAWE

Operating Systems

- An Operating System is a resource manager
- We view a system as having a number of layers, with the physical hardware at the bottom; the base operating system above including:
  - Privileged kernel code
  - APIs, and services
  - User applications and utilities in the top layer

Operating Systems



- Each of these layers is vulnerable to attack so they all need to be secured appropriately

FANSHAWE

Operating Systems - BIOS

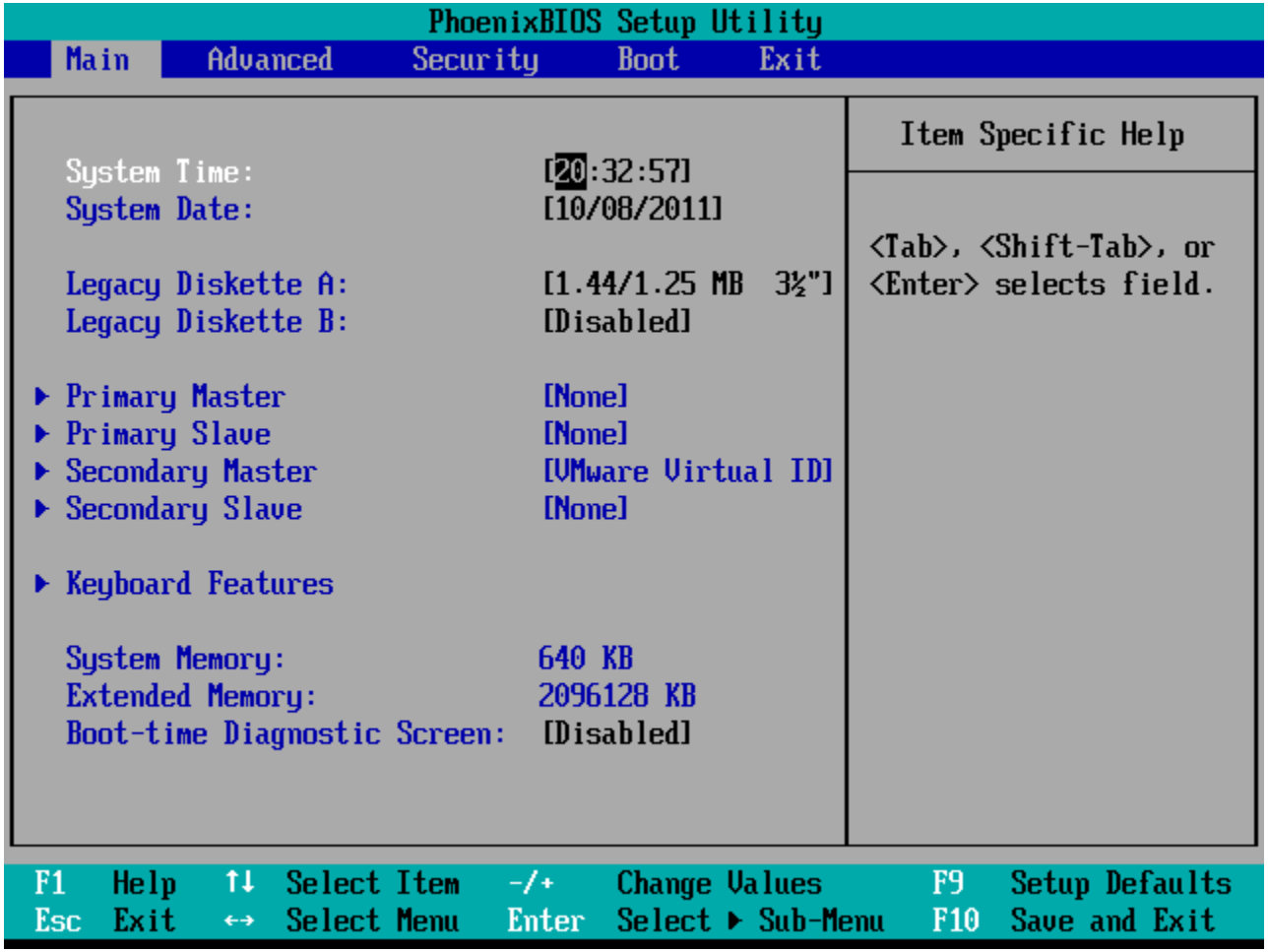
- Basic Input / Output System (BIOS)
- Manages data flow between the O/S and attached devices such as the keyboard, etc.
- It is external to the O/S and typically not visible by the O/S
- Manages the computer upon boot up
- Supports low-level hardware control
- Generally designed for a specific Motherboard model

FANSHAWE

Operating Systems - BIOS

- Historically the BIOS was stored on a ROM chip
- Newer systems store BIOS on flash memory which allows for updates / bug fixes
- This led to security problems where attackers could infect the BIOS chip with Malware such as Viruses and Rootkits
- In the last few years, BIOS has been replaced with the Unified Extensible Firmware Interface (UEFI)

Example of BIOS Screen



FANSHAWE

Operating Systems - UEFI

- Replaced BIOS as the interface between an operating system and the firmware in a computer
- Allows for remote access to troubleshoot computer systems without the O/S
- Provides a more intuitive graphical interface than BIOS
- Caused some firmware issues with certain laptop manufacturers in the past
- Microsoft introduced secure boot with UEFI starting with Windows 8

FANSHAWE

Example of UEFI Screen

FANSHAWE

Operating System History

- Originally, computer systems did not necessarily require an operating systems
  - Mainframe computers
- Operating systems can have many different interfaces
- Older Operating Systems used a Command Line Interface (CLI)
- Newer Operating Systems have incorporated a Graphical User Interface (GUI)

Operating System History

- Development of Operating systems had an early start in the 1950's
- In the late 1960's, MIT, AT&T Bell labs, GE started developing various operating systems (Unics, Multics) which eventually led to the development of the UNIX O/S
- UNIX became quite popular

FANSHAWE

Operating System History

- The 1970's saw more development of Operating Systems including various versions of the Disk Operating System (DOS)
- Microsoft's version of DOS (MS-DOS) came out in the early 1980's
- MS-DOS quickly became a popular Operating System as it was included with early IBM Personal Computers (PCs)

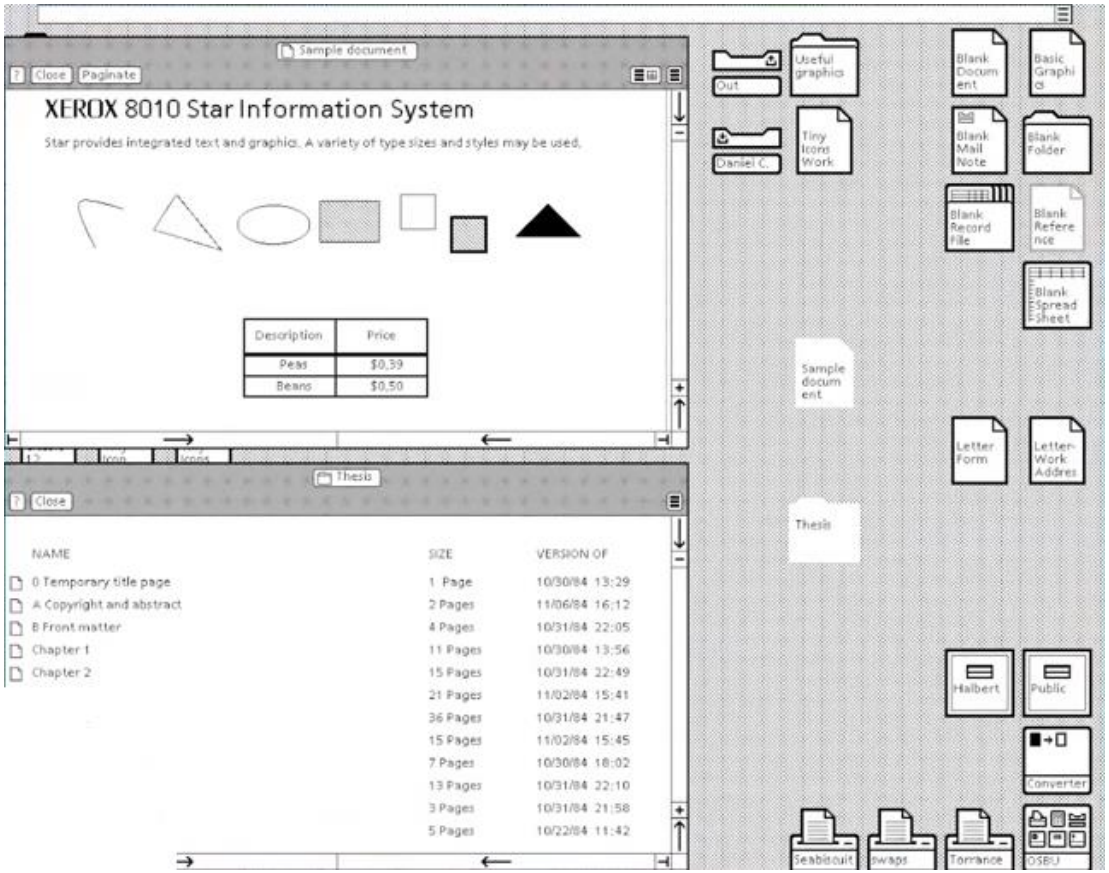
FANSHAWE

Operating System History

- The 1980's saw the development of smaller Personal Computers
- In 1981 Xerox created the Xerox Star Operating System
- This was a pioneer of the Graphical User Interface
- Brochures for this O/S boasted the ability to create documents with words and pictures

Operating System History

- Screen shot of the Xerox Star O/S

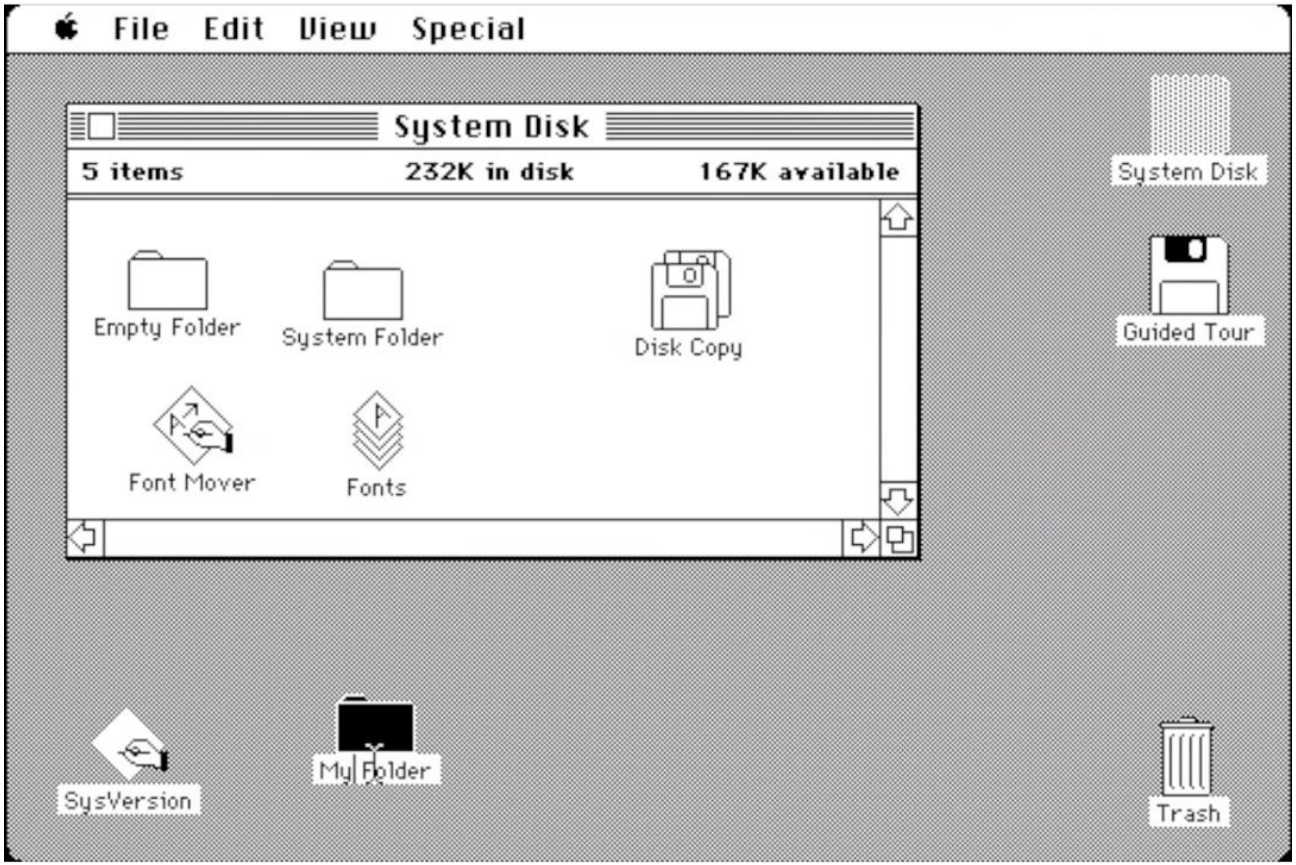


Operating System History

- The 1980's then brought us other Graphical User Interface Operating Systems
- 1983 saw the launch of Apple's Lisa O/S which was too expensive for most users and the machine itself eventually became a commercial failure
- 1984 saw the release of Mac OS 1.0 which displayed many similarities to the Xerox Star Operating System

Operating System History

- Screen shot of Mac OS 1.0

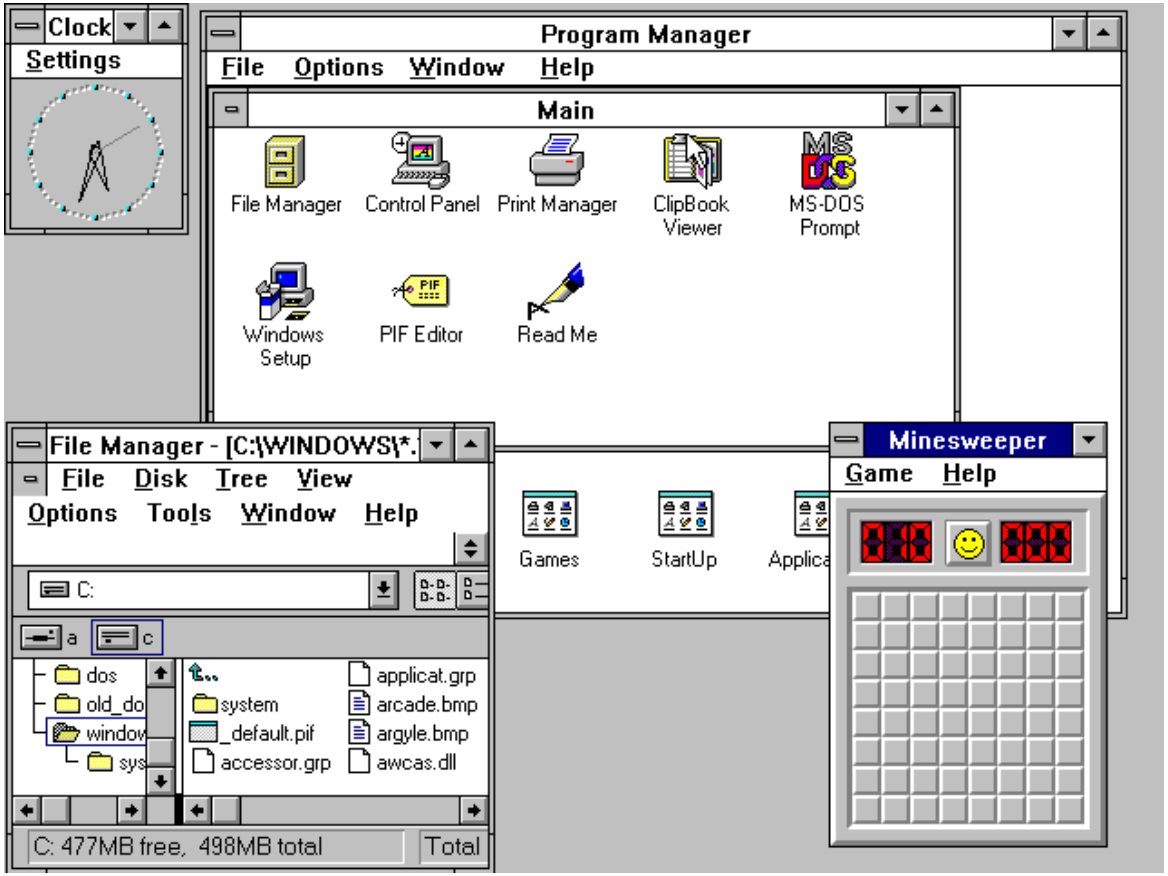


Operating System History

- The 1980's also brought us the first versions of Microsoft's Windows O/S, starting with Windows 1.0
- These Operating Systems all included what was at the time, a modern approach to the O/S interface
- Microsoft would go on to deliver further versions of Windows in the 1990's
  - Windows 3.1x
  - Windows 95
  - Windows 98

Operating System History

- Screen shot of Windows 3.11



Operating System History

- Screen shot of Windows 95

FANSHAWE

Linux Operating Systems

- In 1991, Linus Torvalds created the Linux Kernel
- Linux is considered a Unix-like Operating System
- There are many different versions/distributions of Linux (referred to as Distros)
- The underlying source code was made to be used, modified, and distributed by respective licenses (free for the most part)

Linux Operating Systems

- Major distributions of Linux include:
  - Ubuntu
  - Debian
  - Fedora
  - Linux Mint
  - openSUSE
  - FreeBSD
- Linux O/S is used by PCs, Servers, supercomputers, embedded devices, and Mobile devices

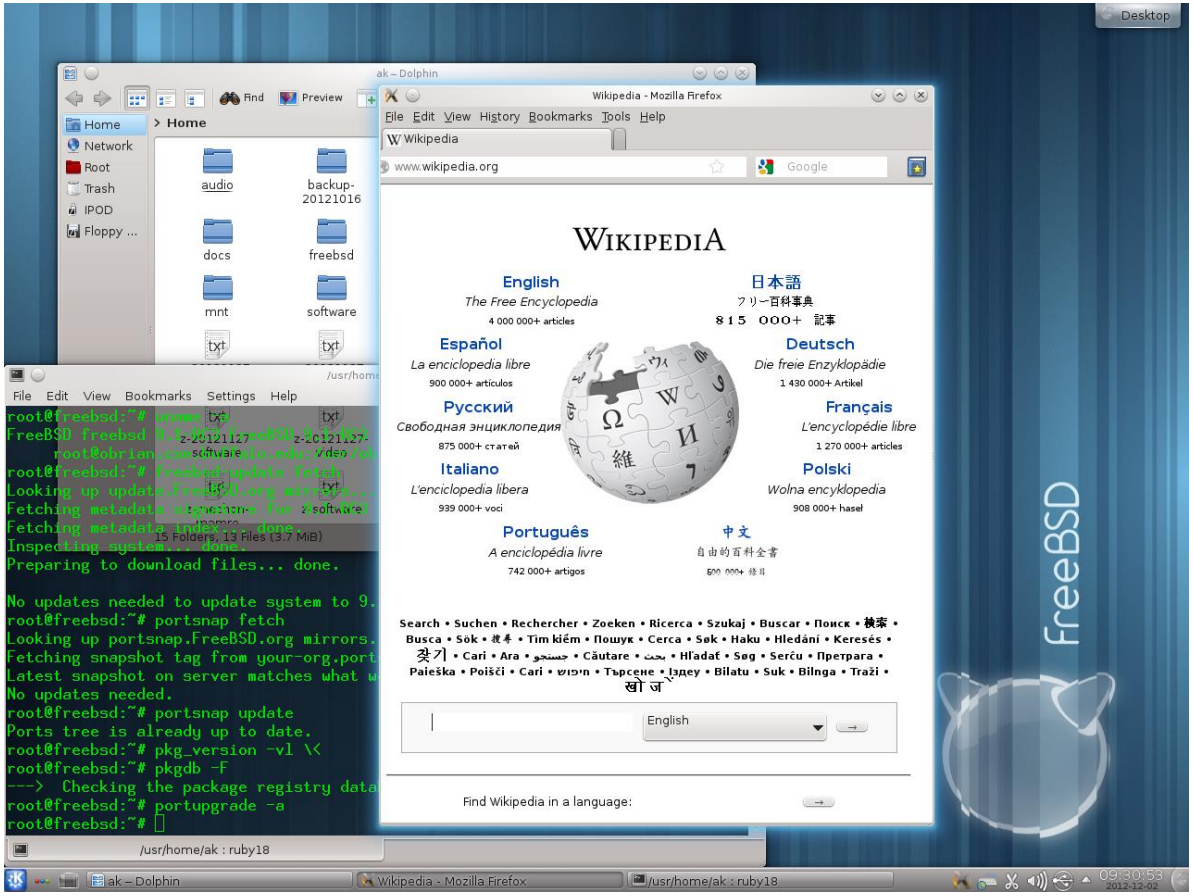
FANSHAWE

Linux Operating Systems

- The Android mobile O/S is based on the Linux Kernel
- Just like any other Operating System, Linux O/S needs to be secured
- Patches and upgrades apply to all Operating Systems
- Modern Desktop Linux distributions include a GUI
- Server versions of Linux typically only allow for the CLI which is similar to a version of Windows Server Core

Linux Operating Systems

- Screen shot of FreeBSD 9.1



Need for O/S Security

FANSHAWE

O/S Security

- No computer system can be made 100% secure
- Security is the process of taking steps to limit exposure to potentially malicious users
  - Close off avenues of attack
- Security is a trade off between ease of use by authorized users and potential exposure to attackers

FANSHAWE

O/S Security

- Security can also be compromised by regular authorized users
- Employees may do something by mistake without trying to be malicious and cause security problems
- Access should follow the principle of least privilege and always be monitored

FANSHAWE

O/S Security

- Servers must expose parts of the operating system, the services and applications they run to valid users
- Servers must allow access to valid users and run tasks on behalf of the valid users
- Securing the server requires limiting the exposure of the system to malicious users without making the system unusable

FANSHAWE

O/S Security

- All software has bugs (for a variety of reasons)
- Development time lines rush products out to meet market demands
  - Reach market before competitors
- Software is often tested for functionality not security
  - The bad attitude of “software security can be fixed after if problems arise”
- One cannot possibly think of all the ways that a program could be misused

FANSHAWE

O/S Security

- Keeping on top of Security patches and updates is essential to minimizing risk
- There are many open source and commercial tools available to perform what is referred to as “Patch Management”
- Many large organizations will also go through a testing phase before releasing patches onto the production environment

FANSHAWE

O/S Security

- Software patches or updates can also be released to smaller groups in a production environment to see how it affects the users
- This is also known as the Canary method
- It basically uses some users as test subjects prior to releasing the updates to the rest of the user group

FANSHAWE

Access Control Concepts

FANSHAWE

AAA

- Authentication
  - Verifying the credentials of users and system entities
    - Who are they?
- Authorization
  - Granting rights and permissions to users and system entities
    - What should they be able to do?
- Accounting / Auditing
  - Keeping track of what users and system entities have been doing
  - Used to make sure access controls are working, to ensure compliance, etc.
    - What have they done?

FANSHAWE

O/S Security

- OS security is based on the concept of subjects, objects and access controls
- **Subjects**
  - Subjects are mostly users, but may be better thought of as anything trying to access an object
- **Objects**
  - Objects are the system components to which subjects (users) are granted or denied access
- **Access Controls / Rights**
  - Access controls determine how subjects can interact with objects

FANSHAWE

Subjects & Objects

- Subjects are any entity that is capable of accessing an object
  - Users, computers, services and processes
- Objects are anything to which access is controlled
  - Files, hardware, memory etc

FANSHAWE

Subject Classification

- Subjects can generally be classified into 3 categories
  - Owner (User)
    - Often the creator of resource
      - A file is a common resource
  - Group
    - Collection of users
      - Used to control access to an object
  - World (Others, Everyone)
    - Access granted to any other users
      - Not the owner or a member of a group
      - Usually with limited access such as read only

FANSHAWE

Access Controls / Rights

- Access Controls may include:
  - Read, Write, Execute
  - Delete
  - Create
  - Search
  - Modify
- Each operating system will have different permissions which are used to control access to objects

FANSHAWE

Access Control

- In general there are 3 types of access controls
  - Discretionary - DACL or DAC
  - Mandatory - MACL or DAC
  - Role Based - RBACL or RBAC

FANSHAWE

DACL

- DACL – Discretionary ACL
  - Most common type of ACL
  - The ACL is set at the discretion of the user that creates the object (the owner)
  - Controls access of the requestor based on their authorization
  - Users who have DAC over an object can often assign other users access to the resource

FANSHAWE

MACL

- MACL – Mandatory ACL
  - The ACL is set by the system
  - Uses security labels and clearances to control access to system resources
  - Users that create objects cannot change the MACLs created by the system
  - Provides more security than a DACL
  - Require administrators to have detailed knowledge of the exact operation of the controls
  - Not user friendly

MACL

- MACL - Mandatory ACL Continued
  - Some Linux systems such as SUSE & RedHat have partial MACLs that apply to some essential services but allow DACLs for most user applications
  - Windows does not support MACLs
    - Windows uses System ACLs (SACL)

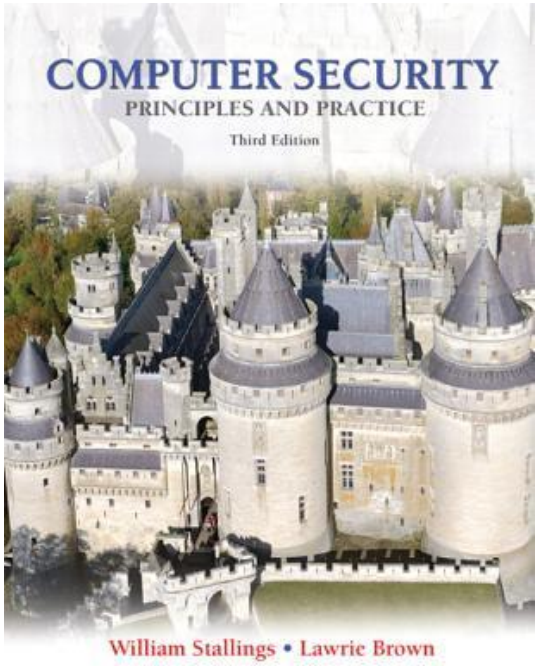
FANSHAWE

RBAC

- RBAC - Role Based Access Control
  - Used to assign permissions based on the subject's job duties
  - Assign permissions to the role and then assign users (subjects) as members of the role via groups
  - As users are assigned new job duties they can be made members of the group and their individual user permissions don't have to be changed
  - Easier to manage for temporary job duties during vacations, etc.

Homework

- Read Chapter 4 for detailed information on Access Control
  - 4.1 – Access Control Principles
  - 4.2 – Subjects, Objects, and Access Rights
  - 4.3 – Discretionary Access Control
  - 4.5 – Role-Based Access Control
  - 4.6 – Attribute-Based Access Control



Lab 01 – Basic Setup

FANSHAWE

Lab 01 Details

- Setup lab environments in VMWare Workstation
- Configure network interfaces
- Change computer names