Objectives

• Learn to enhance security using security devices
• Understand virtualization concepts
• Use basic terminology associated with network functions related to information security

Reading: relevant parts of Chapter 10 (pp. 466-501) in textbook,

Some of the topics in chapter 10 have been covered in ISE218
Securing a Desktop System

- Keep the operating system (OS) patched
- Install an antivirus program and update it
- Remove all protocols and SW that are not necessary
- Rename the administrator account, securing it with a strong password
- If no corporate firewall exists between the machine and the Internet, install a firewall.
- Restricting physical access to the workstation to only approved personnel

Servers

- Virtual machine architecture enhances security
- Minimal functions per server
- Recording message digests of all critical files enables detection of unauthorized code changes
- Use of anti-virus software depends on mission of server
Virtualization

• Allows multiple operating systems to operate concurrently on the same hardware
• Allow for added security, as virtual machines can be deleted at the end of a session
• Malware prevented from spreading to the other systems

Virtualization

• Abstraction of the OS layer – application requests for resources are mapped into the physical HW
• Allows computers to have more than one OS present
• Allows for a clean separation of HW and SW
• Creates a barrier that can improve security
• Involves a hypervisor
• Examples
  • VMWare
  • Microsoft Hyper-V
  • Oracle VM VirtualBox

Compare with high level language abstraction of the HW instruction set
Advantages of Virtualization

- Reduced number of HW devices
- Easier load balancing
- Security
- Preconfigured system images that allow faster system deployment
- Easy rollback to previous states

For security purposes, all applications should be housed and run in a virtual environment

Hypervisor

- Interface between a virtual machine and the host machine HW
- Virtualization implemented with a hypervisor, which is either
  - Built into the OS – Type 1
  - An application that manages the Virtual Machines (VMs) – Type 2
Virtual Memory

- Provides greater memory capacity
- Allows the OS/HW to manage migration of data
- Entire address space required by a process need not be in memory at once.
- Main memory page frames or pages are written (paged) to disk when they are not immediately needed.

*Makes application programming much easier*

Virtual Memory

- Main memory and virtual memory are divided into equal sized pages
  - **Page frame** – physical memory
  - **Page** – virtual memory
- Pages allocated to a process do not need to be stored contiguously—either on disk or in memory.
- Only the needed pages are in memory at any time
- Unnecessary pages are in slower secondary storage
- Can be implemented with paging or segmentation (paging most common)
Virtual Memory Advantages

- **Protection:**
  - Different threads (or processes) protected from each other.
  - Different pages can be given special behavior
    - (Read Only, Invisible to user programs, etc.).
  - Kernel data protected from User programs
  - Very important for protection from malicious programs

- **Sharing:**
  - Can map same physical page to multiple users
    (“Shared memory”)

Virtual Machines

- Software implementation of a computer that executes programs like the corresponding physical computer

- **Types**
  - System Virtual Machine – e.g., IBM VM
  - Process Virtual Machine – e.g., Java Virtual Machine

Virtualized OS, ISAs, I/O, etc. by mapping the virtual request to a physical request

Enables multiple servers to be combined onto one or more physical server
Network Interface Controller (NIC)

- Also referred to as a Network Interface Card (in text), LAN Adapter, and network adapter
- Connection between device and the network
- Implements the physical / data link protocols (usually Ethernet)
- Each NIC has unique 48-bit code built in, called a Media Access Control (MAC) address - assigned by the manufacturer.
  - 24 bits - the manufacturer
  - 24 bits - serial number

Switches

- Forms the basis for connections in most Ethernet-based LANs
- Operate at a lower level in the OSI stack
- Have become the primary network connectivity device
- Added features
  - Security – e.g., disable a port
  - Traffic filtering based on MAC address
Switch Security Issues

- As an intelligent device, it is subject to hijacking by hackers
- A compromised device can eavesdrop on communications
- Switches are administered by SMTP and Telnet, both of which have security weaknesses (e.g., cleartext passwords)
- Switches are usually shipped with default passwords
- Vulnerable to other attacks

Routers

- Operates at the network layer of the OSI model
- Connects different network segments together
- Uses routing protocols to determine optimal paths across a network
- Enables network traffic on the Internet
- Can be attacked due to vulnerabilities in both SNMP and Telnet
- May include a firewall, VPN handling, and other security functions
Firewalls

- Hardware, software, or combination
- Enforce network security policies across network connections
- Security policies are rules that define
  - What traffic is permissible and
  - What traffic is to be blocked or denied
- Security policies should follow the principle of least access
- Some firewalls perform routing and some routers include firewalls

How a Firewall Works

- Acts like a guard at a gate
Security Policy Enforcement

• Typical Mechanisms
  • Basic packet filtering
  • Stateful packet filtering (i.e., sequence of packets)
  • Access Control Lists (ACLs) – rules for port numbers and IP addresses

• Examples
  • Only allow traffic on port 80 for HTTP to the Web server
  • Only allow traffic on certain ports to the e-mail server

Many firewall rule sets include an implicit deny

Security policies usually enforce the principle of least access

Typical Configuration

• External services (e-mail, Web servers) are usually contained in DMZ

a DMZ or demilitarized zone is a physical or logical sub-network that contains and exposes an organization's external-facing services to an untrusted network

DMZ text from Wikipedia
Firewall Techniques

- Since 1988, firewalls have advanced to higher OSI levels
  - Basic packet filtering (1st generation)
    - Checks each packet against rules pre-defined on the firewall (e.g., limited to certain ports)
    - Fairly simple, fast, and efficient
  - Source packet limitations
  - Stateful packet filtering (2nd generation)
    - Firewall maintains the context of a conversation
    - More likely to detect and catch undesired packets
    - Network efficiency is reduced

  Some DoS attacks bombard the firewall with new connections

Firewall Techniques

- Application Layer (3rd generation)
  - Knowledge of application layers (e.g., http)
  - User identity integration
  - Can identify and drop worms and viruses (when known)
  - Can monitor outgoing traffic

- Network Address Translation (NAT)
  - Can hide addresses of protected devices (IP masquerading)

Example: look for infiltration sending messages to home base
Firewall Vendors

• Firewall maturation– changes in firewalls in response to increasing sophistication of attacks
• Issues
  • Track / block how employees are using apps across a range of devices
• Examples
  • Identify / block users who post or share videos on Facebook using an iPhone, PC or other device
  • Enforce policies not allowing a specific group of employees to access games on iPads
• Market leaders
  • Cisco
  • Palo Alto Networks

Palo Alto Networks

• Next generation firewall
• Previous firewalls emphasized protocols and ports (don’t define applications)
• Manages applications, content, and users
• Up to 20Gbs
• Scans content for targeted threats and data leakage (e.g. HIPAA, financial identifiers)
Cisco (Next Generation Firewall)

- Enforces differentiated policies based on the user, device, role, and application type
  - Provides info on whether the accessing device is within the network or remote
  - Supports differentiated access policies based on this information
- Administrators enforce individual and group based access to components of an application
- Blocks port and protocol-hopping applications
- Sees the specific type of device attempting to gain access to the network

Infrastructure Defense Techniques

- Outsourcing – move public services off the internal network
  - Security then becomes a contract issue with the supplier
  - Example – Web hosting, email, application services
  - DoS attacks don’t disrupt the internal network
  - Issue – trust in provider

Hosting services often have better defensive capabilities
Infrastructure Defense Technique

• Dynamic Addressing
  • Allocate addresses dynamically from a pool of available addresses
  • Computer requests an address
  • Servers respond with an address offer, along with terms of use

• Security advantages
  • More standard system administration
  • Makes address based attacks more difficult

Proxy Server

• Proxy – a process that acts on behalf of a user or client
• Receives network traffic intended for a group of clients or servers
• The proxy can provide rule-based filtering

• Types
  • Anonymizing
  • Caching
  • Content-filtering
Proxy Security

• Misdirection
  • proxy receives traffic for network clients and services
  • Attackers attack the proxy rather than the target network
• Simplicity – reduced services in the proxy allows it possess few vulnerabilities
• Filtering – rules allow it to drop attack traffic

Wireless

• Security is not limited to physical access
• Point of entry to a wired network is the Wireless Access Point (WAP)
Wireless Networking

- IEEE 802.11 (WiFi) - family of IEEE wireless protocols (LANs)
  - 802.11b – up to 11Mbps
  - 802.11g – up to 54Mbps
- Uses radio frequencies
- Wireless access point (AP or sometimes WAP)
  - Connects to a wired network
  - Includes a router or connects to a router

Access Point

- Includes security
- Security standards
  - WEP – easy to crack
  - WPA
  - WPA2
    - resistant to hacking if using a strong password
    - 256 bit key
Example - Attacking 802.11

• Rogue access point – An AP that has either been
  • installed on a network without proper authorization or
  • created to allow a hacker to conduct a man-in-the-middle attack

Example – a hacker
network in a public access area

Did You Satisfy the Objectives?

• Learn to enhance security using security devices
• Understand virtualization concepts
• Use basic terminology associated with network functions related to information security