WHAT IS PERSONAL AND CONSUMER COMPUTING

OBJECTIVES

- Understand how we use computers on a day to day basis
- Be able to discuss the types of computing devices are in our homes

TYPES OF COMPUTING DEVICES - PERSONAL

- Home computers
- TV's
- Internet Modems
- Wireless routers
- Portable electronics like tablets
- Printers, etc.
- Other not so common – Refrigerators, Light switches, Door locks, etc

HOME COMPUTERS

- Different needs for different people
  - Storage
  - Gaming
  - Speed
  - Plain web surfing
- Cost is pretty inexpensive - $700 - $2500 range
- You get what you pay for!

PRINTERS

- Not used very often
- Cost is minimal

NETWORKING DEVICES

- Designed to get several devices (<20) connected to the internet
- Modems and wireless routers are inexpensive - <$100 - $200

HOME AUTOMATION

- Door locks
- Refrigerators
- Light switches
- Cost is inexpensive to expensive
- Based off convienence

SUPPORT/MAINTENANCE

- Support and maintenance are generally afterthoughts
- Security – install it and forget it

CONCLUSION

- Personal or consumer computing is based off convenience NOT necessity.
- Keep in mind for next lesson!

ENTERPRISE COMPUTING

OBJECTIVES

- Understand how enterprises use on a day to day basis
- Be able to discuss how enterprise computing differs from personal computing

IT'S JUST NOT THAT SIMPLE

- Enterprise computing takes thought
- "Why can't I do this?"
  - Security
  - Continuity
  - Cost
- Example: External backup drives

PREVIOUS LESSON

- Focus was on convenience
- Cost wasn't a concern – generally

ENTERPRISE COMPUTING

- Reliability – How much does this device need supported?
- Scalability – Do I have to buy more of this?
- Manageability - Can it integrate? Can I manage it?
- Cost – Can we afford not to do the 2 points above?

RELIABILITY

- Power is on all the time
- Parts are constantly used
- Equipment takes more abuse because you directly don’t own it!

SCALABILITY

- Do I have to buy more of something to keep making it work?
- How much power does it consume?

MANAGEABILITY

- Can I control the device?
- Can I install what I want to?
- Who's data is really on this device?

COST

- In the long run – Can I afford not to care about reliability, scalability, manageability? Probably not!
- Enterprise equipment costs money! It's not cheap

PERSONAL VS ENTERPRISE FROM LAST LESSON

- Computers – Enterprise computing is focused on bottom line, productivity, not what the user wants.
- Printers – Designed for large workloads, service contracts usually are best because they are expensive.

PERSONAL VS ENTERPRISE FROM LAST LESSON

- Networks – Many devices must control data, not just a wireless router or modem, focus is on client connectivity, not speed necessarily.
- Careful thought is put into how users connect, what construction looks like
  - “How thick are the walls you say?”
- Automation:
  - Industrial control systems are not convenience, they are standard.
  - Lighting, heating, security controls, all are standard

CONCLUSION

- Enterprise computing is based off necessity not convenience
- Enterprise computing is thought out

ROLES IN SYSTEM MANAGEMENT

OBJECTIVES

- Discuss the different roles for system administrators
- Understand common tasks for administrators

SYSTEM ADMINISTRATION IS…

- Covers many different tasks
- Looks different from role to role
- Focusing on troubleshooting

COMMON TASKS

- Provisioning a service – putting a system into production
- Gathering user requirements
- Understanding how a system will be used
  - Will this system be used for 1 person or thousands?
- Integration – Databases, authentication systems, websites, etc.

COMMON TASKS, CON'T

- Adding, modifying, deleting users
- Reviewing permissions
- Analyze and audit logs
- Looking at security events
- Assessing security of a system
- Troubleshooting

DATABASE ADMINISTRATOR

- An administrator whose job it is to maintain databases
- Many companies use databases to store information
  - HR data
  - Financial data
  - System data
- DBA focuses on speed and correctness of data

WEB SERVER ADMINISTRATOR

- An administrator whose job it is to develop or maintain webservers
- This may seem easy. It's not.
- There are so many components that go into delivering enterprise websites
  - Multiple servers
  - Load balancing
  - Authentication
  - Database management
  - Etc.

NETWORK ADMINISTRATOR

- An administrator whose job it is to ensure connectivity to internet, services, servers, etc.
- Day to day might focus on firewalls, switches, routers,
- Might need to look up data on users who are using or abusing network resources

SECURITY ADMINISTRATOR

- An administrator whose job it is to protect the organization through systems
- Job duties probably include
  - Analyzing events
  - Investigating what happened in an investigation
  - Analyzing permissions
  - Granting/Denying permissions

CONCLUSION

- There are so many more specialized fields
- Common tasks are understood by every system administrator to make their systems run effectively

WHY DO WE NEED TO LEARN NETWORKING

OBJECTIVES

- Understand the reasons why we need networking
- Understand why there are standards for networking
- Discuss why we use networks

EVERYTHING IS CONNECTED!

- Personal devices
  - TV's
  - Watches
  - Tablets
- Enterprise devices
  - HVAC systems
  - Lighting
  - Security systems

WIRELESS IS EVERYWHERE

- Wireless typically will connect our small devices, but what about reliability?
- Systems that need to be connected 100% of the time shouldn't necessarily run off wireless – Security systems for example
- Labs – high bandwidth

OPEN WIRELESS NETWORKS

- Can pose a security risk!
- Open wireless networks send information that anyone can look at
- Coffee shops, hotels, other retailers provide this for free usually
- We don’t want to run everything off an open wireless connection
  - Financial data
  - Personal data

CONSIDERATIONS WHEN DESIGNING A NETWORK

- Keep outsiders out
- Keep insiders in
- Keep insiders out

KEEP OUTSIDERS OUT

- We want to protect privacy
- Industry and organization based
- Could be implemented because of compliance (HIPAA, PCI-DSS)
- Technology such as:
  - Firewalls
  - Access Control Lists (ACLs)
  - Virtual Local Area Network (Virtual LAN or VLAN for short)

KEEP INSIDERS OUT

- Segmenting certain portions of the network so most critical data is not compromised
- Financial networks, open wireless, industrial control systems
- May also be driven by compliance needs (HIPAA, PCI-DSS)
- Technology such as:
  - Firewalls
  - Access Control Lists (ACLs)
  - Virtual Local Area Network (Virtual LAN or VLAN for short)

KEEP INSIDERS IN

- Safe guarding users from themselves
  - Protect users from viruses
  - Target breach?
- Driven by compliance, regulations (HIPAA,
  - SCIFF - Sensitive Compartmented Information Facility
- Technology such as:
  - Firewalls
  - Access Control Lists (ACLs)
  - Virtual Local Area Network (Virtual LAN or VLAN for short)
  - Keep in mind that security is only as good as the upstream devices – meaning if a firewall is compromised, doesn't matter if you have these technologies or not.

CONCLUSION

- Always think about how users are using a system before deciding on your network
- 3 primary security considerations need analysis
  - Keeping outsiders out
  - Keeping insiders out
  - Keeping insiders in

OSI MODEL

OBJECTIVES

- Why we need the OSI model
- What each layer is used for
- Give examples of how each layer is used

OSI MODEL

- Open Systems Interconnect or Interconnection – said both ways
- Developed in 1980's
- Latest standard defined in 1996
- Describes the way computers or networking devices talk to each other

WHY DO WE NEED TO KNOW THIS?

- You may use it every day
- Helps us troubleshoot connection issues
- Issues can arise at any layer when there is connectivity involved
- As an example think of a website accessing Google

LAYER 7 – APPLICATION LAYER

- Responsible for displaying data
- Example includes Outlook, Google Chrome, Windows, etc. Anything that displays the final data to you

LAYER 6 – PRESENTATION LAYER

- Data conversion from one form into another – such as HTML or email
- Data compression

LAYER 5 - SESSION

- Handles establishment and tear-down of a connection
- Manages requests and responses between applications

LAYER 4 - TRANSPORT

- Very important layer!
- Handles acknowledgements and communications between client and server
- Responsible for connection and connectionless protocols
- End to end connections and reliability of the connection

LAYER 4 CON'T

- Connection based protocol - TCP
  - Most all communication over the internet is TCP
  - Video, Website traffic, etc.
  - Needs connections to guarantee information was sent and received on both sides
- Connectionless protocol UDP
  - Connectionless protocol
  - Gaming, logging
  - Doesn't care if it's received
  - Relies on speed

LAYER 3 – NETWORK LAYER

- Responsible for logical addressing of devices
- IPs!
- Responsible for routing between physically connected devices
  - BGP, OSPF, RIP, EIGRP
- Data is transmitted in packets

LAYER 2 - LINK

- Responsible for the physical link addressing
- Responsible for establishment and termination of links
- Connects each device physically – think MAC addresses
- Data transmitted in frames

LAYER 1 – PHYSICAL

- Physical signals – electronic, optical, or other medium such as wireless
- Responsible for voltage of the device

COMMON ISSUES

- Layers 1-3 typically have the issues
- Troubleshooting should be done at all layers

CONCLUSION

- Each layer is important
- All layers work together continuously to create communication

WHAT IS VIRTUALIZATION

OBECTIVES

- Discuss history of virtualization
- Explain execution levels in applications

WHY DO WE NEED VIRTUALIZATION

- Security
  - Allows segmentation
  - Allows reverting to known good state
- Footprint
  - Less power per VM than physical server
  - Commodity of scale

HISTORY

- 1974 – Popek and Goldberg defined formalized requirements for building virtualization
- Three Requirements
  - Equivalence – Must act like a real system
  - Resource Control – Complete control from host and not outside host
  - Efficiency – Instructions must be executed without the help of the host
- In order to achieve these, we must be able to use a privileged instruction set architecture or ISA

VIRTUALIZATION THEOREMS

- The first theorem says for any conventional third-generation computer, an effective VMM may be constructed if the set of sensitive instructions for that computer is a subset of the set of privileged instructions.
- The second states that for any conventional third-generation computer is recursively virtualize a bowl if it is virtualizable and two a VMM without any timing dependencies can be constructed for it.
- The third theorem states a hybrid VMM may be constructed for any third-generation machine in which the set of sensitive instructions are a subset of privileged instructions.

HOW THE KERNEL IS BUILT

- Instructions are executed in “Rings”
- Privileged instructions are executed at ring 0
- User instructions are executed at ring 3
- There may or may not be ring’s 1 or 2 according to some operating systems
  - Windows 7 and 2008 and below only use 2 rings – Ring 3 and Ring 0
- Device drivers may live at rings 1 and 2 if they are built in

CPU ARCHITECTURE

- Intel and AMD both have virtualization instruction sets
- Intel Nahalem and newer chips (Intel VT-x/EPT), AMD –V/RVI
    - Starting with these chips, we are able to do second level translation
- Allows translation of addressing to second level – example Windows 7 inside Hyper-V inside of VMWare Workstation

CONCLUSION

- History is important to understand how we use virtualization today
- The kernel of an OS is important to understanding virtualization
- Virtualization is a technology that will not go away anytime soon.

TYPES OF VIRTUALIZATION

OBJECTIVES

- Discuss types of hardware or software virtualization
- Discuss differences between platform virtualization technologies
- Explain which technology, specifically software is used for what purpose

PLATFORM VIRTUALIZATION

- Software implementation of a computer system
- Platform virtualization separates an operating system from the underlying platform resources
- Types:
  - Full or binary translation
  - Hardware-assisted
  - OS-level / Paravirtualization

FULL VIRTUALIZATION

- Also called binary translation
- Executes direct instructions
- Translates kernel code to replace nonvirtualizable instructions
- Each VM has own BIOS, devices and memory management
- Requires no hardware or operating system assistance to virtualize sensitive and privileged instructions
- Excellent performance
- Examples: Vmware ESXi, QEMU, Parallels for Mac

OS ASSISTED /PARAVIRTUALIZATION

- Hypercalls to VM layer replace non-virtualziable instructions
- May use API to integrate
- Poor compatibility due to modification of OS
- Performance is fair and not predictable
- Examples: Xen, Docker, VMware Server(old)

HARDWARE ASSISTED

- Privileged instruction are executed below Ring 0
- Sensitive and privileged instructions trap to hypervisor removing need for binary translation or paravirtualization
- Software is limited due to execution only in hardware
- Performance is fair
- Examples: VMware Workstation, older Virtual PC, Hyper-V

SOFTWARE VIRTUALIZATION

- Allows applications to be run in a virtual platform or container
- Many advantages – *usually* contains the virtual instance, portable
- Examples: Java, Flash, Mono, V-apps
- Since these applications are generally cross platform, viruses may be introduced to effect the OS running it

HARDWARE VIRTUALIZATION

- Memory – Aggregation of RAM from many sources into virtual memory pool
- Storage – Abstracting logical storage from physical
- Network – Software Defined Networks, VPN, VLANs
- Desktops – VDI, allows for 1 experience for a user across many platforms

CONCLUSION

- We have started to see the emergence of virtual everything
- Virtualization allows us flexibility to use what we need when we need it

PROS AND CONS OF VIRTUALIZATION

OBJECTIVES

- Discuss pros and cons of virtualization from a practical perspective
- Discuss cost vs footprint

PHYSICAL HARDWARE

- Physical servers tend to be under utilized
- They require a lot of power
- Can be expensive per system
- Space
- You know exactly where they are

PROS

- Generally cost savings
  - Capital costs – Chassis and blades or large rack mount servers can virtualize architecture effectively
  - Operating costs – 1 server or cluster vs many
  - Data-Center expenditures
    - Power
    - Cooling
    - Space
- Efficiency
  - RAM, Processing, storage
- Migration of workloads in outages

CONS

- Licensing can be complicated
- Server sprawl
- Some hardware cannot handle virtualization
  - Dedicated network cards
  - Encryption modules
- Admins may have access to everything!
- Thought must be put into the system – redundancy is a must!
- If one technical aspect of your server is near 100% utilized, should you virtualize?

CONCLUSION

- Virtualization takes thought and planning
- Make sure all software and hardware can be virtualizaed before a strategy is put in place

YOUR COMPUTER VS ENTERPRISE SYSTEM

OBJECTIVES

- Discuss how computer resources are used
- Describe benefits of certain computing systems
- Explain how personal computing systems can be used for enterprise type computing

PERSONAL COMPUTING AND RESOURCE CONSUMPTION

- Personal computers at home or at work generally use very little resources
- Over the past several years we have been able to slow down on purchasing "fast" processors due to abundance in compute power
- Computers generally use only 5 – 10% processing resources
- RAM – "normal" usage, perhaps 25%-60% total

VIRTUALIZATION ALLOWS US TO DO MORE!

- Allows for compartmentalization
- Allows for security
- Allows for productivity and performance

DOESN'T HAVE TO BE EXPENSIVE

- We can virtualize systems easily on our home computers or laptops
- Necessities:
  - Processors: Intel i5, Intel i7, AMD FX, AMD Ryzen(soon to be released)
  - Memory: 8+ GB RAM DDR3 or DDR4
  - Software: VirtualBox, VMware Workstation, Parallels
  - Storage: Enough to hold and operate many virtual systems

ENTERPRISE ENVIRONMENTS

- More of everything
  - Storage
  - Memory
  - Processing
- Redundancy built in – in everything!

TYPICAL ENVIRONMENTS LIKE UCCS

- Smaller configurations
  - 14 blades
    - 884 logical cores
    - 3.5T RAM
    - 108T of tiered storage
  - All redundant, all active/active configurations

PERSONAL COMPUTING STILL WORKS WITH VIRTUALIZATION

- My desktops typically run 7 VM's concurrently
- Laptop runs 4 because of the RAM

CONCLUSION

- Your computer can run this
- You can experiment with this technology and learn!
- You don't have to spend a lot of money creating an enterprise class environment

WHY INFORMATION SECURITY IN THE FIRST PLACE

OBJECTIVES

- Discuss why security is important in business
- Security might impact bottom line
- Explain how users might impact security

WHY DO WE NEED TO KNOW ABOUT SECURITY

- Someone wants access to data
- Systems fail
- Poor system management

SOMEONE WANTS DATA

- Hackers
  - Someone who doesn't care how they get the data or what damage it causes
  - Profit
  - Credit
- Phishers
  - Looking to steal account information for gain
  - Could be an email or phone call
- Hackivists
  - Looking to seek change
- Next-door neighbors?
  - Free wi-fi

SYSTEMS FAIL

- Equipment fails
  - Hard drives
  - Power supplies
  - Any piece of electronics fail at some point
- Incorrect configurations
- Accidental destruction

POOR SYSTEM MANAGEMENT

- System administrators are not infallible
- “build it and forget it”
  - IOT devices – TV’s, webcams, etc.
- Nosy Neighbors
  - Did you forget to secure your wireless?

CONCLUSION

- There are many more reasons why we need information security
- CIA triad condenses these – Confidentiality, Integrity, Availability

WHAT IS A SECURE COMPUTER

OBJECTIVES

- Explain defense in depth
- Discuss security principles

PRINCIPLE 1

THERE IS NO SUCH THING AS A SECURE COMPTER!

PRINCIPLE 1 EXPLAINED

- Computers can be secure if all threats and risks are taken into account at the very moment they are secured
- Software becomes out of date
- Vulnerabilities arise
- Accidents happen
- Misconfigurations aren't realized

PRINCIPLE 1

USE DEFENSE IN DEPTH

PRINCIPLE 2 EXPLAINED

- Defense in depth is a principle where a layered security approach is applied given threats and risks
- Designed to cover a majority of threats and risks

ADDITIONAL SECURITY PRINCIPLES

- There are so many more principles that we could go on and on forever, however here are more basic ones that will decrease risk
  - Apply software updates regularly and consistently
  - Use a desktop firewall whenever possible
  - Strong unique passwords with a minimum of 10 characters from system to system
  - Make routine backups of your critical files
  - Do not open emails that you don't recognize who the author is or look suspicious
  - Only install applications that are needed
  - Don't post usernames or passwords in plain sight or share passwords

CONCLUSION

- Securing computers is a combination and process of part hardening part auditing and part intrusion detection and response
- Defense in depth from a security principle aspect helps achieve a more secure computer in the long run
- These may be common sense to you, but may not to someone else. Especially users in your organization that tried to intentionally evade security

RISK IN SYSTEM MANAGEMENT

OBJECTIVES

- Understand and discuss what risk is
- Describe the 5 areas of risk
- Give examples of each area of risk

RISK

- Definition according to Webster's – 3a the change of loss or the perils of the subject matter of an insurance contract; also: the degree of probability of such loss
- In other words in security – probability of loss of one of the three areas of security
- Risk is everywhere!
- Risk can be broken down into a few example areas: what, where, when, how and why

WHAT

- What we access might compromise security
- Internet surfing
- Software installation
- Non-business use of computing devices
- Example: Torrenting software

WHERE

- Where we connect can pose a problem to integrity of our systems
- Mobile users are prone to security risk
- Trusted vs untrusted networks
- Example: coffee shops!

WHEN

- Risk increases when events happen
- Big reason why I read the news – get current information on events
- Example: natural disasters tend to cause and increase in phishing

HOW

- The how of risk comes in the form of not adhering to security best practices
- The more knowledge we have, the less risk is involved in doing something that compromises security
- Example: Using FTP instead of SFTP is a bad idea

WHY

- Logical reasoning and knowledge of why we use best practices lessens risk
- You don't just do what someone else tells you! - this goes back to lesson 2 of week 1.
- Risk increases when reasoning is not applied
- Example: Using unsanctioned file sharing service for storing data because it was easier

HOW RISK CANNOT CHANGE

- Operating systems
- Commercial products
- Users who refuse to follow best practices
- Up to you to assess

CONCLUSION

- Risk must be understood to lessen changes of loss
- Loss can come in the form of one of the three pillars of the CIA triad
  - Confidentiality
  - Integrity
  - Availability

CIA – CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY

OBJECTIVES

- Explain and discuss the 3 pillars of the CIA triad
- Give examples of each of the 3 pillars

WHY THE CIA TRIAD?

- Information security can really boil down to 3 key components.
- If any one of the 3 pillars breaks, we are not secure
- All parts must remain intact

FIPS 199

- U.S. federal government special publication that outlines the standards for security categorization of Federal Information and Information Systems
- Breaks down categorization of information
- Based off FISMA compliance – Federal Information Security Modernization Act

CONFIDENTIALITY

- Definition according to Title 44 of the U.S. Code: “Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information”
- How it applies according to FIPS 199: “A loss of confidentiality is the unauthorized disclosure of information”
- Brief Explanation: The ability to keep things secret
- Examples: Encryption, Passwords, Access Control Lists

INTEGRITY

- Definition according to Title 44 of the U.S. Code: “Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity”
- How it applies according to FIPS 199: A loss of integrity is the unauthorized modification or destruction of information
- Brief Explanation: The ability to ensure information remains the same and original from the source
- Examples: Hashing, checksums

AVAILABILITY

- Definition according to Title 44 of the U.S. Code: “Ensuring timely and reliable access to and use of information”
- How it applies according to FIPS 199: A loss of availability is the disruption of access to or use of information or an information system.
- Brief Explanation: The ability to ensure systems remain available and functioning
- Examples: Using load balancers, RAID, server clustering

EXAMPLES OF FAILURES

- Confidentiality – You name the latest breach – they are everywhere. Target, Home Depot, Heartland breaches
- Integrity – phpMyAdmin attack of 2012
- Availability – Large scale DDoS attacks such as Mirai botnet

CONCLUSION

- Users and admins should always consider the CIA triad in any point in the system lifecycle
- It's up to the administrator to make sure they are ensuring security is built in!