Information Technology Concepts

Module 3

START

COMPUTERS

History of Computers

- Before 1940s: Concepts & electro-mechanical prototypes
- Before 1960s: Very specialized needs
- Before 1980s: Managing government responsibilities, research & development, banking, managing big businesses
- Today: Nearly ever facet of living involves computers
  - Initially computing was convenient
  - Now we are dependent

Why Are Computers Necessary?

- Reliance on enabling:
  - Analysis
    - Complex models that cannot be calculated manually
      - Weather forecasting
      - Flood prediction
      - Pharmaceutical research
  - Control
    - Digital control is versatile
      - Airplane flight
      - Automobile engine management & breaking
  - Access
    - Information collections – databases, libraries
  - Communication
    - Personal, mass

What Do Computers Do?

- Given a set of instructions
- Given a set of input data
- A computer manipulates the input data according to those instructions
  - Presents the results
  - Stores the results

Computer Components

- Central Processing Unit (CPU)
- Memory
- Input/Output (I/O)
  - Video presentation support
  - Serial data channels (ex. USB)
    - Uses: Keyboard, mouse, printer, audio
  - Parallel data channels (instructions, data)
  - Storage – non-volatile memory – (ex. Hard drive)

Broad Categories of Computing

- Special Purpose
  - Embedded computing
    - Tuned for specific purpose (speed, power, cost)
    - Limited flexibility in performing alternative instructions or providing functionality beyond original intention
  - Super Computing
  - Control Systems
- General Purpose
  - Functionally flexible
  - Extendable
  - Manageable

Common IT Computer Catalog

- Personal Computer (PC) / Workstation
  - Stationary
  - Mobile (laptop, notebook, netbook)
- Servers
  - Standalone
  - Clusters
  - Mainframe
- Personal Computing Devices
  - Tablets, Smartphones

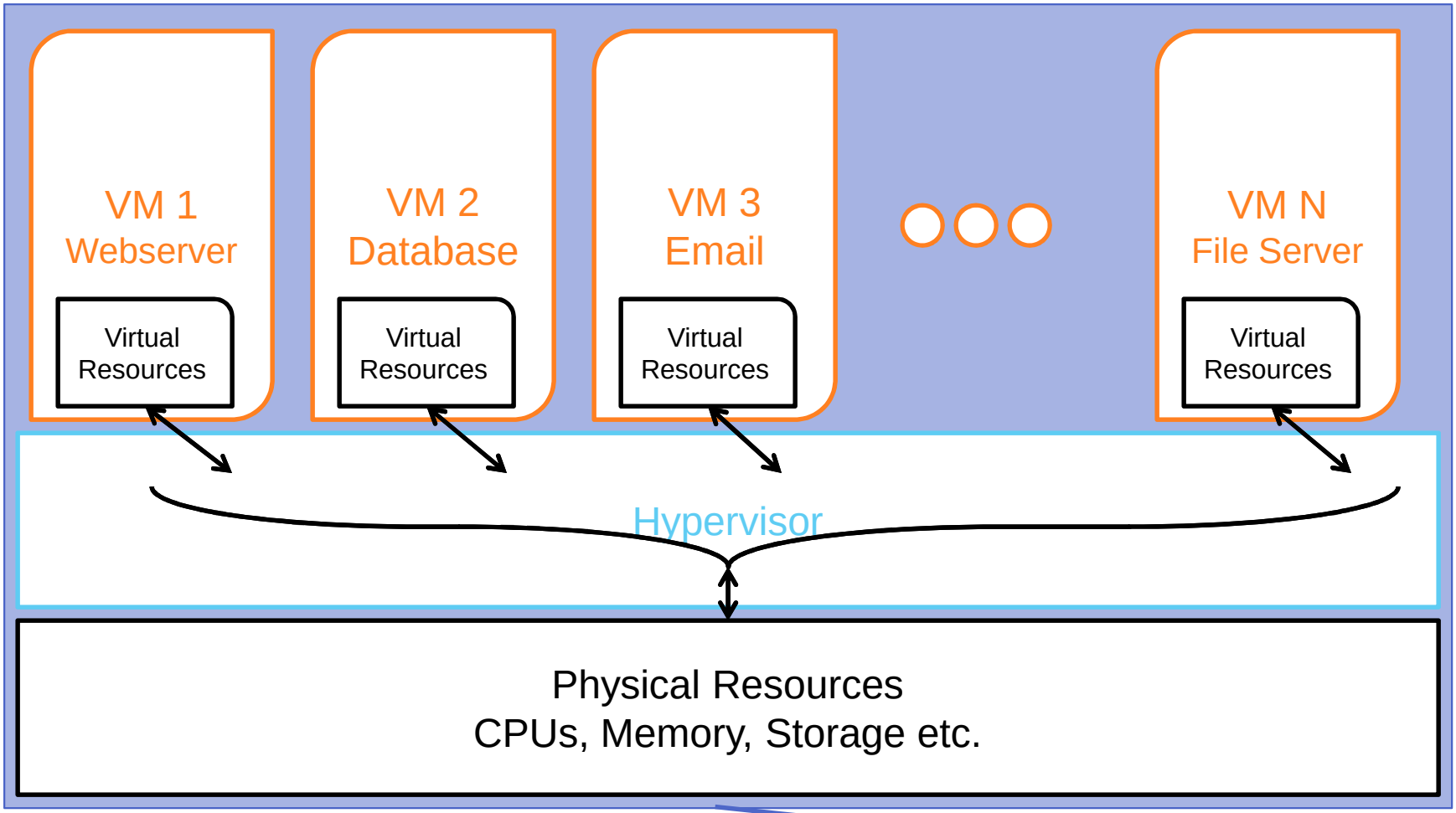
Virtual Computing

- What is it?
  - The ability to run a computing platform entirely as software (a sophisticated collection of prepared computer instructions).
  - One physical computing platform or Server supports the operation of multiple computing platforms.
- Why use it?
  - Physical computers require:
    - Space, Cooling, Power, Cabling, Physical installation
  - Operational realities:
    - Many servers not so busy, power consumption when idle still large, server room space is expensive

Virtual Computing

- Terminology
  - "Bare metal" – A physical computing platform that requires space, power, cooling etc.
  - Virtual Machine (VM) – A computing platform that runs as a software program. This computing platform runs as if it is on "bare metal."
  - Hypervisor – Key ingredient – Provides VMs a fully functional story that the VM has actual CPUs, Memory, Storage etc. It emulates these physical devices for each VM and spreads their needs across all actual CPUs, Memory and Storage of host platform.

Virtual Computing



END

COMPUTERS

START

OPERATING SYSTEM (OS)

Role of an Operating System

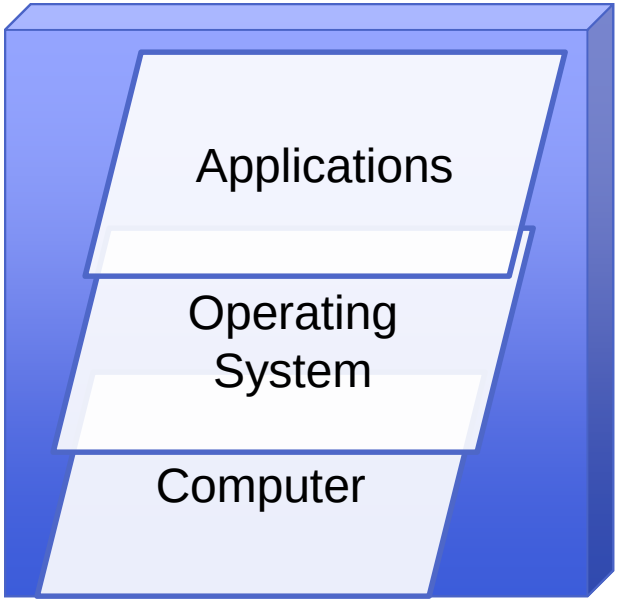
- Computers can be used for many things
  - But it cannot without instructions
- Operating Systems
  - Allow multiple applications to run “simultaneously”
  - schedule execution of instructions
  - provide interfaces between applications and physical resources
  - provide user interfaces

Role of an Application

- Computer + Operating System = Computing Platform
  - Has potential to do much, but still isn't doing much that is very useful
- Applications/Apps
  - Software that addresses a user's needs
    - Examples: Word processing, email client, web server
  - Supplied by 3rd parties (ex. Microsoft, Apple)
  - "In-house" developed
    - Custom application for internal use

Useful Computing Platform

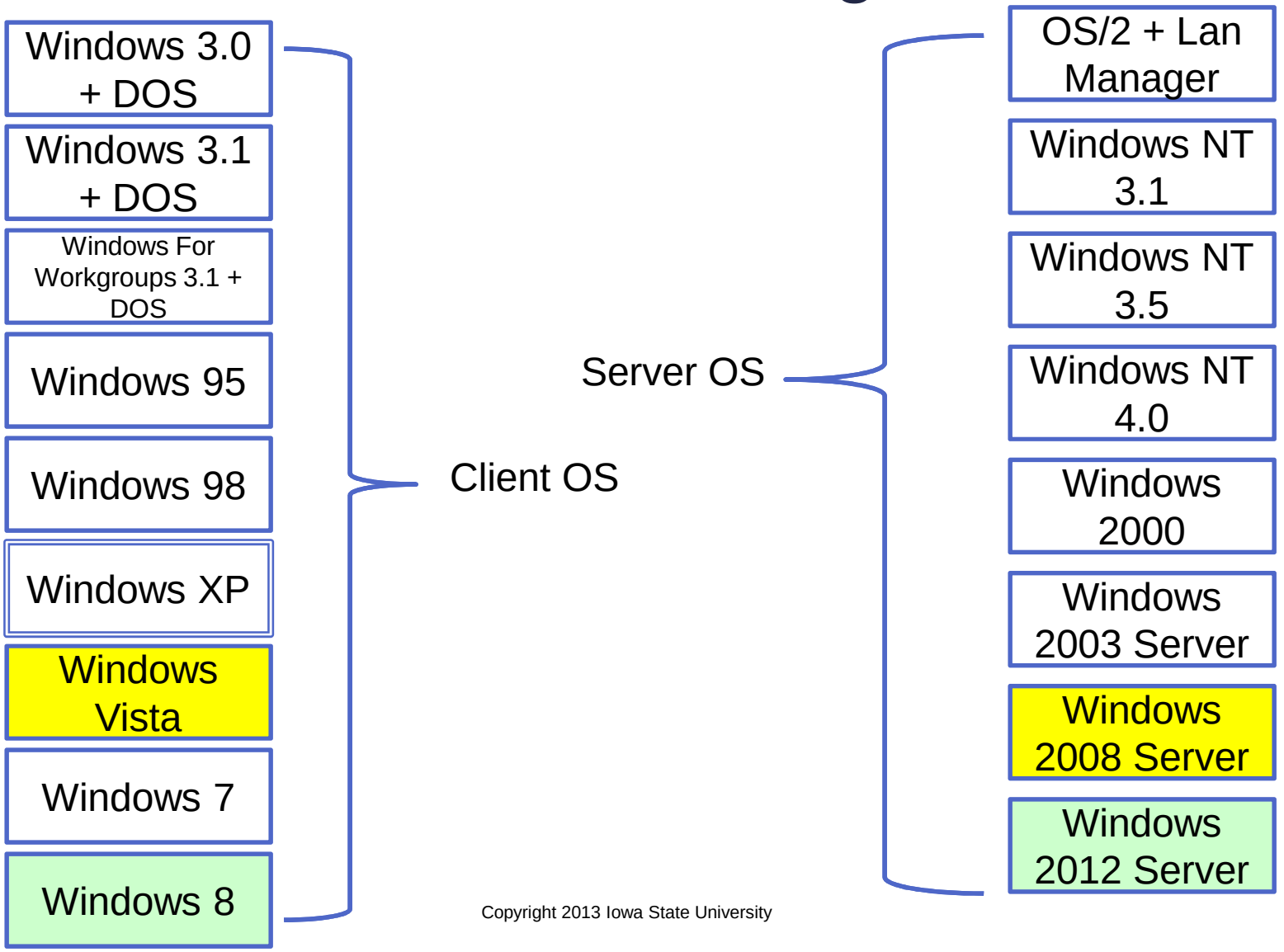
- Computer + Operating System + Applications = Useful Computing

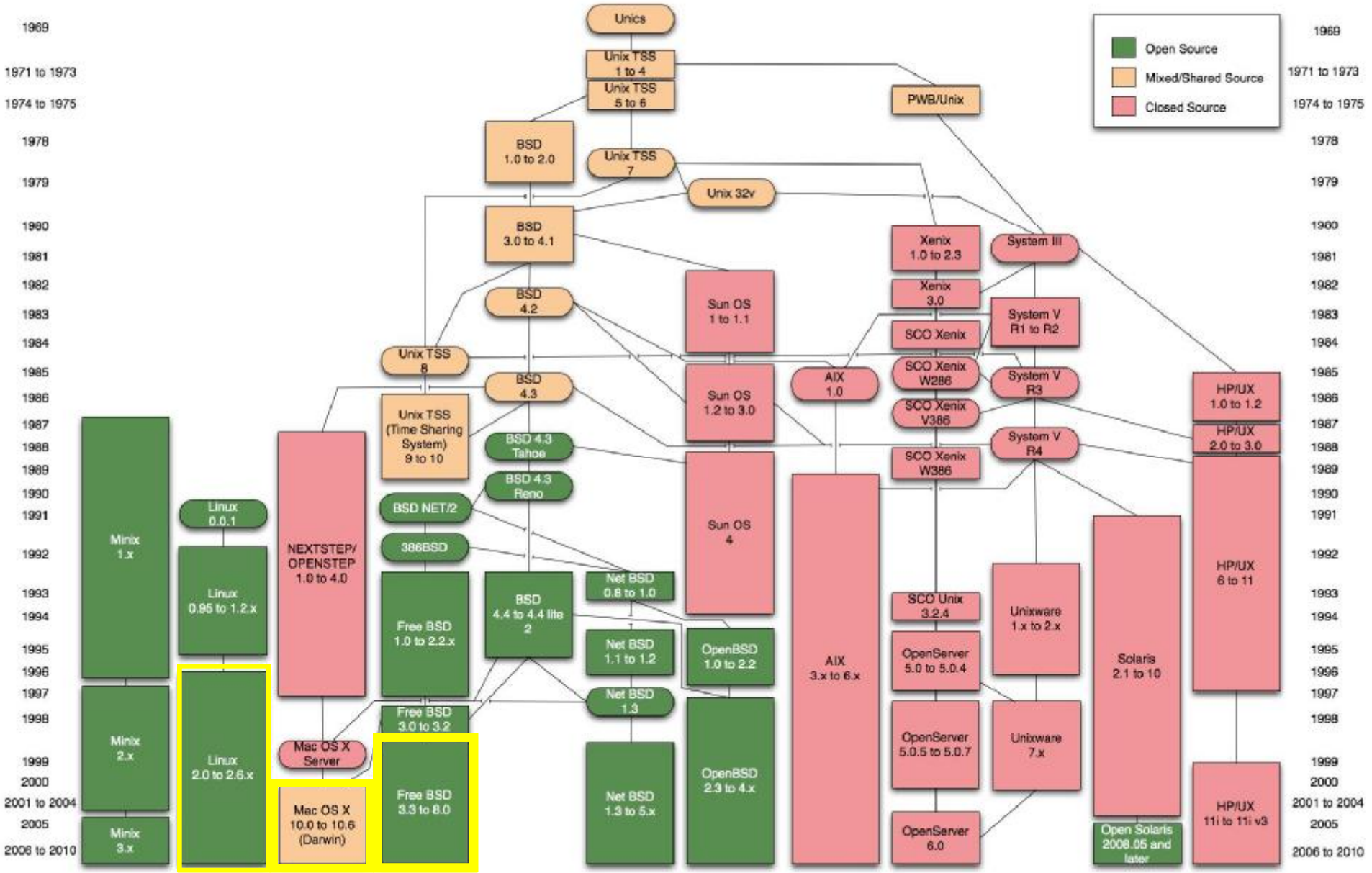


Available Operating Systems

- Many
- Popular
  - Microsoft Windows
  - Apple Mac OSX
    - iOS
  - Unix
    - BSD
    - System V
    - Linux

Windows Lineage





Source: http://commons.wikimedia.org/wiki/File:Unix_history-simple.png

Value of History

- New Versions **è** New Features
  - But, old design decisions, popular features, operational concepts change slowly
  - Knowing that Mac OS X 10.x is based on FreeBSD 3.0 – 3.2 helps you understand how Mac OS X works.
  - Knowing that Ubuntu is Linux based we expect it be pretty different from Mac OS X.
  - Windows has no history in common with Unix, so we should expect it be very different.

Client-Server Model

- Pervasive Concept of Distributed Computing
- Two Party Interaction
- Party 1: The Client – Requests information and actions. Initiates interaction.
- Party 2: The Server – Provides information, performs actions on behalf of this client and other clients who may make contact
- Examples –
  - Web browser & Web server
  - Email client & Email server

Client & Server OS Objectives

- Client OS
  - Usage: Used by a single user
  - Proximity: User has physical contact with computing platform
  - Resources: Rich support for interactive applications, graphics, multi-media
- Server OS
  - Usage: Used by many users
  - Proximity: User has no physical contact.
  - Resources: Access to large storage, tuned for sharing resources, commonly fault tolerant

Comparing Client and Server OSes

- Within same OS Family (ex. Windows, Mac OS X)
  - Common core technology
  - Common user interfaces and commands
  - Server OSes have management features that make remote administration practical
  - Running on Server console is potentially a minimal Client environment or is Headless
    - Once running, server administration is done remotely.
    - No additional admin interfaces available on console

Interaction

- Physical interfaces
  - Keyboard
  - Mouse
  - Touch screen (more common with Client OS)
    - Gesture based interactivity
  - Touch pad (not common on servers)
  - Display (Client – High Resolution, Server – Something adequate)

Proximity of Interaction

- Console
  - Using keyboard, mouse, display attached to computer
- Remote session
  - Full interactive experience – Ex. MS Remote Desktop
  - Specialized interfaces that run locally but manage remote systems
  - Centralized management – 1 action changes multiple devices

GUI & Command Line

- GUI – Graphical User Interface
  - Point and Click
  - “Easier” to learn – no memorization of commands
  - Interface can guide user through a procedure
  - Interface may prevent big mistakes
  - Many repetitive actions needed to accomplish the same objective multiple times

GUI & Command Line

- Command Line Interface (CLI)
  - Interface is simply a prompt for input
    - Examples: `C:\ dir`, `sh-3.2$ ls -l`
  - "Harder" to learn because more knowledge and understanding needed
  - Typically supports packaging multiple commands and program logic into executable text files – batch jobs or scripts
  - Potentially faster experience with no mouse tracking and interface rendering

Transaction & Batch Computation

- Transaction is an activity that is completing in near real-time
  - Any delay mostly related to performance of system
  - User intends action to be committed now
    - Optimistic banking customer cashing a check
    - Amazon shopper ordering a book
- Batch is commonly a set of activities, scheduled to be performed in the future
  - These jobs can be hourly, daily, weekly, monthly
  - Check collection and clearing are done in bulk
  - U.S. Mail is collected and transported in bulk

Information in Chunks

- Smallest unit of data is a bit. A single value that can be assigned a 0 or 1.
- Multiple bits are consolidated to represent numerical values.
- 4 bits combined can represent a value from 0 – 15, 8 bits can represent 0 - 255
- CPU and Memory handle data in chunks
- Chunk size is related to the “data width” or number of parallel data paths and CPU’s internal storage

Information in Chunks

- 8 bits are called a byte
  - Most common unit of data
- Memory addressing does not allow access to chunks smaller than 8 bits
- Bytes can be combined to store a single numerical value, so larger numbers can be represented
- Negative number needs one bit to be the sign, so the possible range of numbers is smaller than a strictly positive number

Information in Chunks

- Although literal memory content is numerical we can use numbers to represent other things like:
  - images, text or sound
- The software processing the information is aware of the convention of how numerical memory values have been assigned

Information in Chunks

- Assembling data into chunks happens throughout computing and is mostly transparent to the user.
- Chunk sizes vary based on limitations of technology at the device level and software
  - Hard drives use geometric defined chunks
  - File systems use chunks useful for addressing files
  - Networking breaks up data as well
- Interfaces between technologies have instructions on how to assemble and disassemble chunks

END

OPERATING SYSTEM (OS)

START

NETWORKING

Why is Networking Necessary?

- Computers are islands of information and computing power
- Networking allows information to flow and computing to be distributed
  - Example: www.wikipedia.com, client-server, peer-to-peer, cluster computing, cloud computing, high performance computing

What Does Networking Do?

- A number of different technologies work in concert to transform, transmit, route and deliver information between one sender and one or more recipients.
- Physical distance between sender and receiver is not a concern of the sender.
- Methods of transmission are transparent to the parties.

Elements of Networking

- Identifiers
  - A label to differentiate one party from another
  - Examples: www.iastate.edu, 192.168.10.2, 80, 40:6c:8f:2e:31:dc
- Protocols
  - Formal rules that govern the exchange of information between parties
  - Examples: Ethernet, WiFi, IP, TCP, HTTP

Elements of Networking

- Transmitting and Receiving Technology
  - Devices
    - Capable of transforming supplied information to a signaling scheme appropriate for the channel
    - Capable of transforming the received signals into a form useful to its consumer
  - Communication channels
    - A path for a signal
    - Example: Ethernet twisted pair cable, fiber optic cable, 10MHz at 1800 MHz band, barbed wire

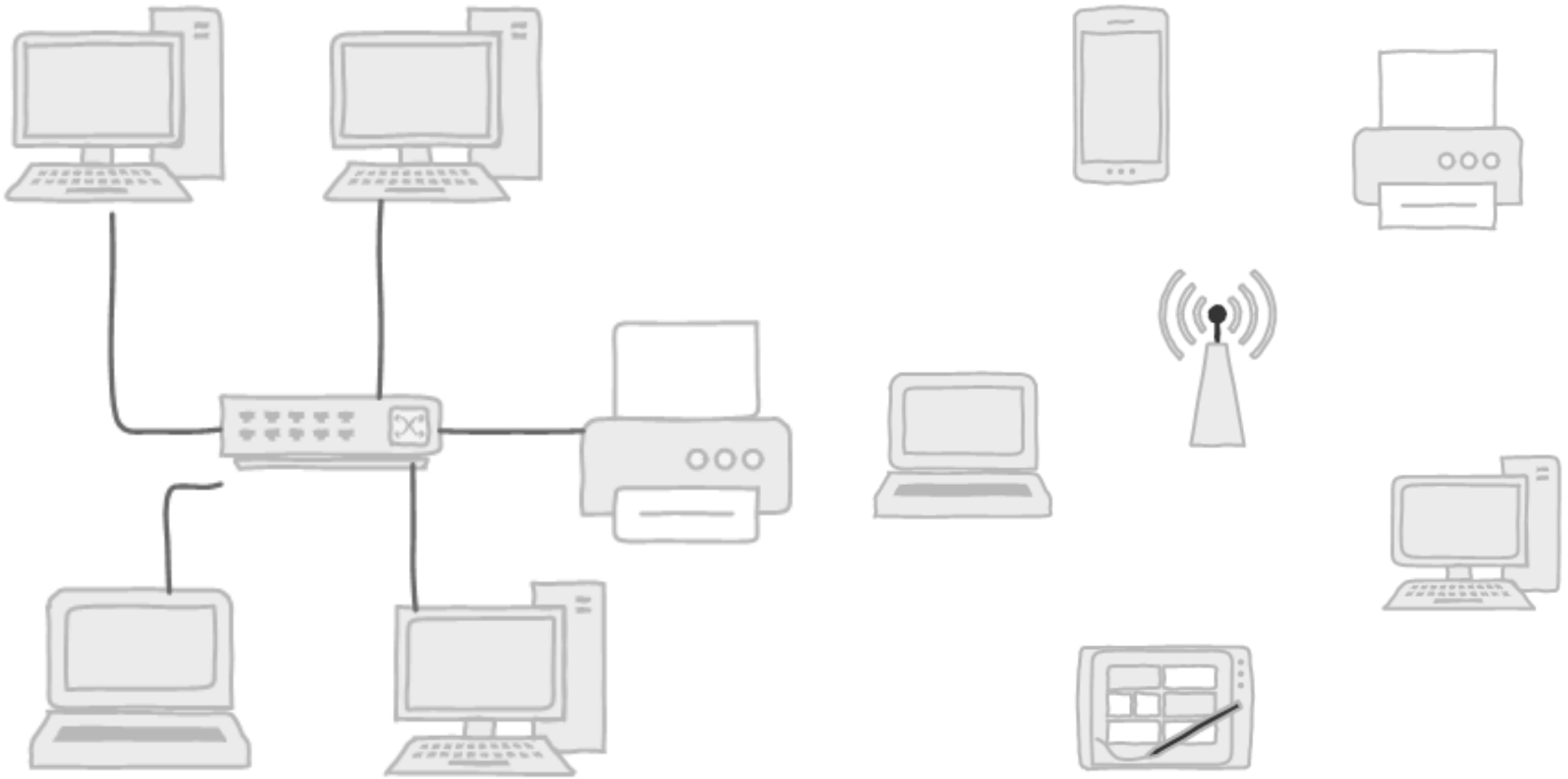
Elements of Networking

- Routing
  - Directing information
    - The action of forwarding information along a path that leads to the intended destination or recipient.
  - Knowing where to direct
    - The agents that direct information need instructions regarding what paths lead to what destinations.

Two Common Connectivity Approaches

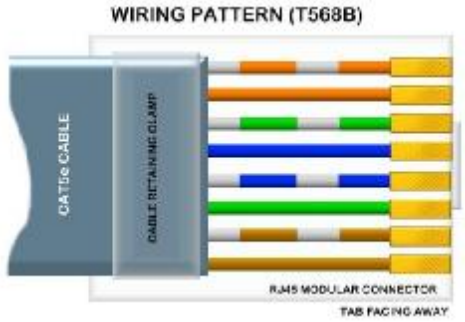
Wired

Wireless



Wired Connectivity

- Historically
  - Wired connections most prevalent means to connect devices for networking
- Common Type - Today
  - Ethernet – Twisted pair cables



Source: en.kioskea.net

Wired Connectivity

- Advantages
  - Large capacity communication channel
    - High bandwidth => High data rates
  - Reliable
    - Properly installed cabling lasts many years
      - Higher speeds, not decay, will prompt change in cabling
  - Private
    - Physical attachment to network needed
      - Typically means access to a building or a room

Wired Networking

- Disadvantages
  - Cost
    - Cabling and related components cost money and labor is also expensive.
  - Inflexible
    - Network ports are stationary once installed
  - Delay
    - New network connections need to be planned, scheduled, installed and tested
  - Tethered
    - Connectivity stops if cable is removed

Wireless Networking

- Historically
  - Limited to microwave transmission used by communications companies
- Common Type – Today
  - IEEE 802.11n
  - 3G & 4G

Amazon.com

Pcworld.com

Wireless Networking

- Advantages
  - Convenient
    - No cables to carry or attach
  - Mobility
    - Connectivity does not stop as you move, within limits
  - Smaller Form Factor
    - Designer does not need to provide space for cable attachment

Wireless Networking

- Disadvantages
  - Relatively smaller channel capacity
    - Limited spectrum and noise limit data rates
  - Reliability
    - Building design, quantity of users, distance from access point can degrade performance
  - User Privacy
    - Signal broadcast can be received by anyone in proximity
  - Environment perimeter
    - Anyone with enough signal strength can access network channel
    - Leakage outside buildings

Spatial Scope

- Spatial scope
- Personal Area Network (PAN)
  - Interconnects personal devices in close proximity (within 10 meters)
    - Uses: Hands free calling, picture transfer, backup etc.
  - Typical wireless – Bluetooth, near field communications (NFC)
  - Typical wired - USB, Firewire, ThunderBolt

Spatial Scope - LAN

- Local Area Network
  - Interconnects computing devices across a building or smaller spaces
  - Commonly a mix of wired and wireless connectivity
    - Typical wired: Ethernet (10/100/1000 Mbps)
    - Typical wireless: WiFi (IEEE 802.11 a/b/g/n)
  - Many to many network
    - Many simultaneous senders and receivers
    - Each node is equally accessible (no hierarchy)

Spatial Scope - LAN

- Local Area Network (continued)
  - Relatively cheap high speed data rates
  - Applications perform best for users on the common LAN
  - Entire infrastructure is commonly owned by one entity (ex. Homeowner, local government, business)
  - Sophisticated LANs require knowledge to design and operate

Spatial Scope - WAN

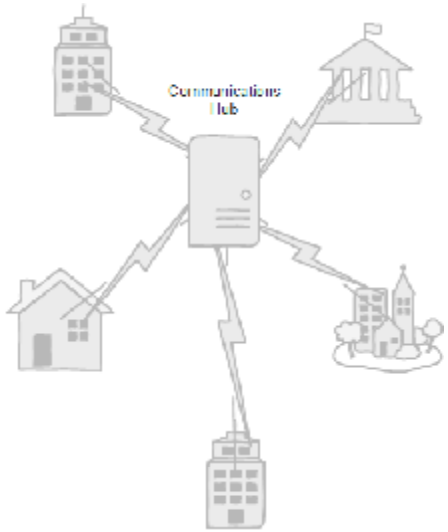
- Wide Area Network
  - Interconnects networks
  - Distances between networks can be 1000s of miles
  - Typically owned by a communications company
  - Private option: Multiple locations interconnected with communication paths accessible to only those locations

Spatial Scope - WAN

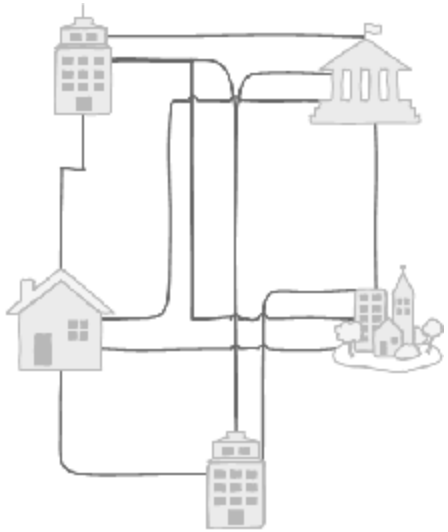
- Semi-Private or Member Option: Only entities that qualify and follow rules may connect to share information with each other
  - Example: Banking, Airline ticketing, Classified nets
- Public/Internet: Any entity willing to contract with an Internet Service Provider (ISP) may connect and potentially communicate with any other Internet node.

Spatial Scope - WAN

- Wide Area Networking
  - Physical Topology
    - Hub and spoke



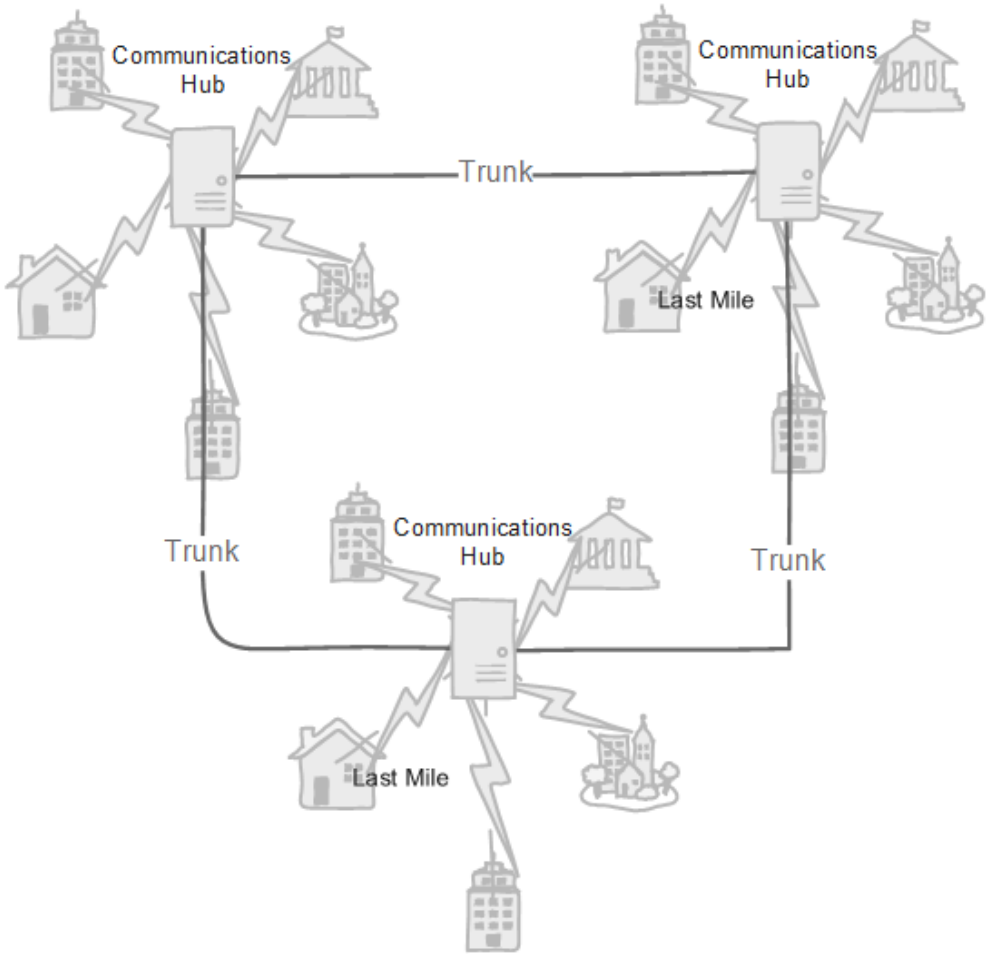
  - Logical Topology
    - Fully connected mesh



Spatial Scope - WAN

- Wide Area Networking
  - Communication paths
    - “Last Mile” Technology
      - Cheapest: Digital Subscriber Line, Cable TV Network, Residential Fiber
      - Expensive: Satellite, T1, T3, OC3 and more
    - Trunk Technology
      - ATM (Asynchronous Transfer Mode), Frame Relay
      - Very high speed fiber cable, microwave, satellite

Spatial Scope - WAN



Secure or Non-Secure Network

- Importance of distinction
  - Expectation of threats
  - Consciousness of weaknesses
  - Location of IT functionality and data
  - Evaluating risk
- Many IT environments have a mixture
  - Connecting to the Internet is a risk
- Security techniques manage the transition between the two types of networks

What makes a secure network?

- Trust – Confidence placed in people, technology and information to be reliable and true to their intended purpose as defined by the owner.
  - No more, no less
- Control – The ability of limiting or preventing people, technology and information from violating the expected level of needed confidentiality, integrity and availability.

What makes a non-secure network?

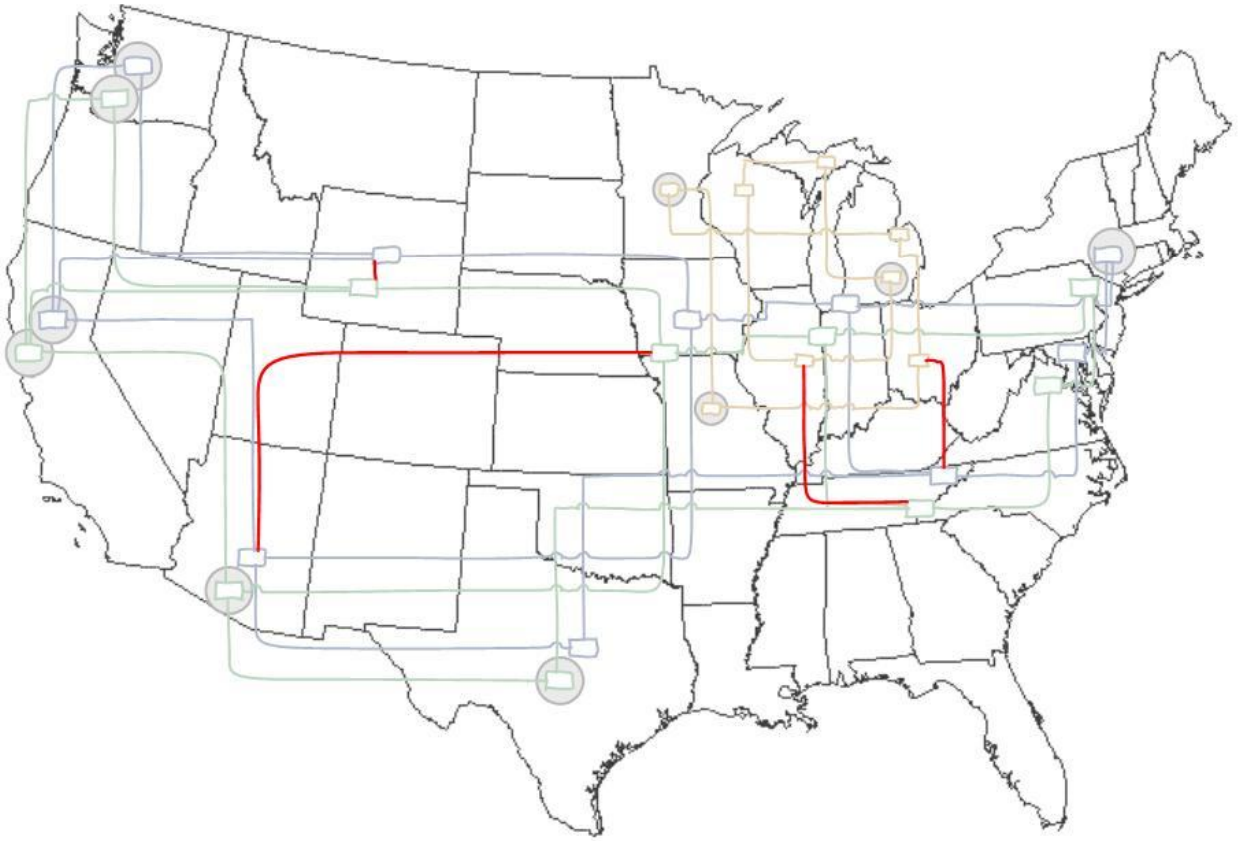
- Lack of Trust
  - Don’t know if people, technology and information can be relied upon to be true to the owner’s needs.
  - Open and universal access means any person can connect (ex. Internet)
    - Strangers are hard to trust
      - It only takes one malicious stranger to make it hard for the owner to trust.
- Inadequate control

Internet

- History
  - 1982 – TCP/IP protocols were standardized
  - 1980s – Research institutions connected with support from U.S. government
  - Early 1990s – Commercial Internet Service Providers (ISPs) formed
  - 1995 – U.S. government dropped support and full commercial use was permitted

Internet - Structure

- Network of Networks



Internet – Operational Control

- ISPs are independent
  - Success requires cooperation
- Governments may influence ISP operations within their borders
- ICANN – International Corporation for Assigned Names and Numbers
- IETF – Internet Engineering Task Force

Internet - Challenges

- Functional
  - Reliable operations
  - Performance for more data intensive or time sensitive applications
  - Pervasive interconnectivity
    - Refrigerators placing orders to grocery stores
  - Universal access
    - Urban, suburban, rural

Internet - Challenges

- Security
  - Critical infrastructure (ex. Power companies)
    - Use the Internet as their WAN
  - Limited control on who has access
  - Limited accountability
  - Implied trust in communication
  - Limited control of applications being operated
  - Limited control on content (type, accuracy, trustworthiness)

END

NETWORKING

START

ACTIVITY 3 REVIEW

END

ACTIVITY 3 REVIEW

START

CYBER SECURITY: AN OVERVIEW

Origins of Cyber Security

- Foundations, are still relevant today
  - Physical security
    - Protecting life and valuables
      - Limiting access to known trusted people
  - Information security
    - Protecting information in all forms
      - Historical approaches for secrecy
        - » Hiding written messages
        - » Speaking in code
        - » Scrambling and substituting letters
    - Unauthorized change and destruction prevention
      - Physical documents are harder to change, replace or destroy with good physical security

Origins of Cyber Security

- Information Assurance
  - Risk management related to information and information systems
  - Preventing loss under difficult circumstances
  - Compliance to regulations and standards
  - Disaster recovery of information systems

What is Cyber Security?

- The discipline that ensures the trust placed in the information technology environment and information contained therein is not violated, and remain suitable for the purpose for which they are intended.

Why is Cyber Security needed?

- Promotes confidence that:
  - Honorable people will remain honorable
  - Mischievous or malicious people will be thwarted
  - Customers, investors, partners and employees can entrust their sensitive information to or rely on the IT environment to meet expectations resulting from trust

Security Policy

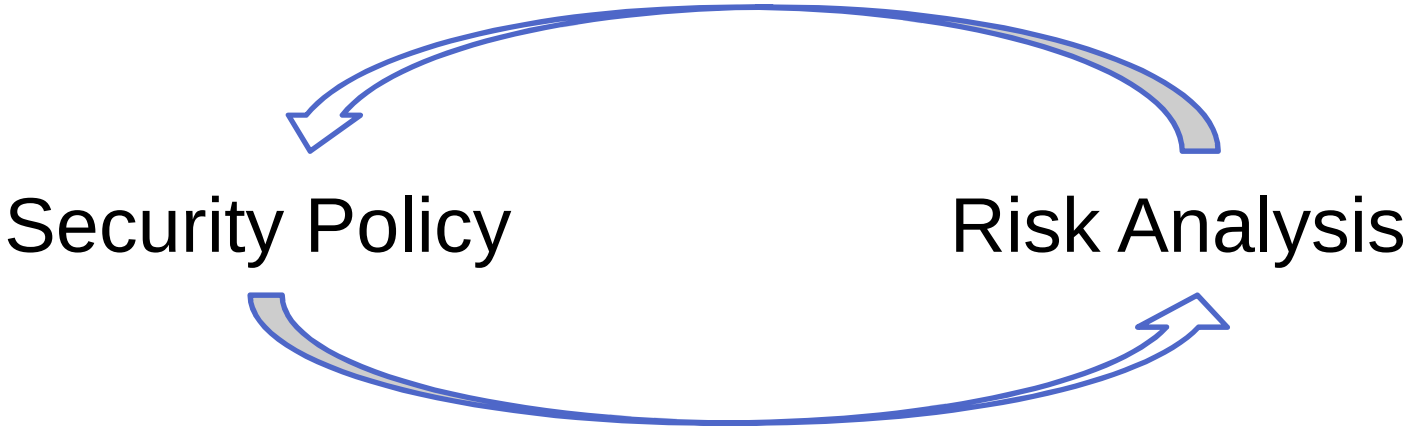
- Formal statements that identify:
  - Organization's responsibilities to
    - Law, regulation, contracts, mission/business
  - Value and types of information and systems
  - Expectations for, care to be provided to and appropriate use of those types of information and systems
  - Leaders to be directly responsible for meeting policy
  - Authority to enforce

Why is security policy necessary?

- Security costs money
  - Policy legitimizes the spending of money
- Security is relative
  - Defining what is or is not secure is based on policy
    - Something not secure does not comply with policy
  - Defining what is permitted or denied is based on policy
- Security can make business decisions complicated
  - Policy commits leaders to a standard to be applied across all decisions

Security Policy Development

- Combines the understanding of:
  - Organization's purpose
  - Organization's culture
  - Applicable laws, regulation and obligations
  - Catalog of information assets and information systems
  - The value of those information assets and systems
  - Threats to and vulnerabilities of those information assets, systems and the environment as a whole
  - Approaches to minimizing risk
- Policy updates are infrequent, kept at high level



Risk Analysis

- Terminology
  - Asset – An owned resource, product, process, information, system that is valued
  - Threat – The occurrence of an event that will cause an undesirable impact on an asset(s)
  - Vulnerability – A flaw or shortcoming of the asset or its safeguards that provides a means for the asset to be negatively impacted

Risk Analysis

- Terminology
  - Expected loss – A value (typically in dollars) of loss resulting from a threat negatively affecting an asset
  - Risk – Expected loss X probability of threat occurrence X confidence in threat assessment
    - A measure of possible losses to an asset commonly within a timeframe like a year
      - Example: Internet web server risk is Medium or $5,000/yr

What is Risk Management?

- Managing risk:
  - Identify and Review risk
    - Evaluate risk to information, systems, people and environment
  - Prevent risk
    - Avoid activity or possessing the asset
    - Avoid threat or stop threat access
    - Correct weaknesses
  - Reduce & Accept risk
    - Add additional protection
    - Minimize reliance or use of asset

What is Risk Management?

- Managing risk:
  - Transfer risk
    - Pay someone else to build, operate and maintain information systems and related information
    - Insurance – pay someone to cover your losses
  - Repeat the process
    - Organization's interests change so risk changes
    - Technologies change so risk changes
    - Threats change so risk changes
    - New vulnerabilities are discovered so risk changes

Two Philosophies

- Risk avoidance – No risk is acceptable, so prevent or transfer all risk
  - Very difficult and expensive to avoid all risk
- Risk management – Minimize risk and accept the remaining risk
  - Most people and organizations adopt this philosophy
  - Allows for objectives to be achieved while living with risk
    - Getting to school – Traveling to school is not risk free. Traffic laws, automobile features and skill gets you to school most days without harm. An accident is less damaging because of safe driving speeds, automobile construction and seat belts.

END

CYBER SECURITY: AN OVERVIEW

START

CYBER SECURITY: CONTROL CONCEPTS

Controls

- A means to reduce risk or the potential for loss
  - Objectives
    - Prevention
    - Detection
    - Recovery/Corrective
  - Implementation Approaches
    - Administrative
    - Logical or technical
    - Physical

Identity

- Who a person is
  - The unique individual
- Names and IDs are assigned to label an individual
  - Analogy: Numeral is a symbol or word that represents a number (a value or quantity)
- Names and IDs help differentiate one person from another

Authentication

- The means by which the identity offered by an individual is verified to be indeed that individual's identity
  - It should be difficult for an imposter to succeed in offering the identity of someone else as their own.
- Verification will rely on one or more of:
  - What the individual knows
  - What the individual has
  - What the individual is
  - Where the individual is

Authentication

- Single factor – most common
  - What you know – typically a password
  - What you have – a badge, a key
- Multiple factor
  - What you have and what you know – ATM card, building or room access card + pin
- More factors should improve confidence in individual being truly who they claim to be

Authorization

- Permitting or denying an action based on established rules for an asset
  - Rules relate identities to actions on assets that are permitted or denied
- Dependent upon authentication
  - Don’t know who they are, you can’t know what they should be doing other than nothing
- Commonly implemented as a technical or physical control

Why is Authorization necessary?

- A key preventative control
- If vulnerability cannot be corrected, authorization can limit both the threats and the opportunity for remaining threats to access the vulnerability

Authorization Approaches

- What is not explicitly denied is permitted.
- What is not explicitly permitted is denied.
  - Considered to be more secure
  - It is more reliable to identify what is permitted then it is to identify all the things that should not be
  - A control following this approach permits nothing by default

Authorization Mechanisms

- Access Control Lists (ACL)
  - Common mechanism in file systems
    - Rules on files and directories
- Firewalls
  - Enforces network activity restrictions
    - Rules are very similar to access control lists
- Role based access control
  - A user is assigned a role. Activities are authorized for that role

Effective Authorization

- You need:
  - Policy that provides guidance on what is important and how important things should be handled and by whom.
  - Authentication that verifies an individual's identity with accuracy.
  - Authorization mechanisms that allow a user to perform their duties without interference, but limit the user from doing things not consistent with job responsibilities.

Accountability

- Both a detective and preventative control
- Being able to identify the actions taken by individuals and their corresponding identities.
- Those concerned about being held accountable for their actions will limit their activities to those that are acceptable.
  - A masked robber of bank hopes to rob the bank but not get caught if he gets away successfully
- After an unauthorized activity has been discovered, the identity of the perpetrator can be determined

Why is accountability necessary?

- Many people will act improperly at least occasionally if there is no risk of consequences
  - If taking $100 from a cash register will not be noticed, why not take it?
  - If giving stuff away that should be sold wont be noticed, why not give some jeans away to your friends when they visit?
  - Carelessness would be common.

Effective Accountability

- Reliable detection & recording of activities
  - Recording occurs when it is needed
  - Recording cannot be altered without authorization & additional accountability
- Review of activity records
- Reliable means to identify actions
- Reliable means to identify actors
- Reliable means to identify assets being acted upon

Types of Accountability

- Physical controls
  - Cameras
  - Metal and dangerous substance detectors
  - Inventory control tags and detectors at doors
  - Guest log at security desk or hotel front desk
  - Logs of card readers for room access
- Technical controls
  - ACL enforcement logs
  - Login logs

Mechanisms that support Accountability

- Identification – government issued documents help
- Authentication – provides greater assurance the identity is correct
- Authorization – these explicit decisions are an opportunity to capture potential or attempted action
- Recording or logging – activity records need to stored in order to be used later

END

CYBER SECURITY: CONTROL CONCEPTS

START

CYBER SECURITY: IDEAS TO CONSIDER

Three states of Information

- Information State – The setting that information is in at a particular time
- “At rest” – information is stationary located in holding area (e.g. file cabinet, hard drive)
- “In transit” – information is in the process of being relocated (e.g. transmission, courier)
- “In process” – information is either contributing to the change or creation of other information or is being changed (e.g. calculating a test grade, updating your birthday wish list)

Usefulness of State distinctions

- In process – Typically the most vulnerable setting for information with respect to remaining confidential, to ensuring it remains useful and available and it has not been improperly altered.
- In transit – Information in transit can be intercepted (taken and replaced; altered, copied) and replayed (sent again with or without modification)
- At rest– Stationary information can be read, copied, replaced, altered and destroyed

Security Considerations – In Process

- Information being processed is not protected
  - Practical challenges for “bad guy”
    - Information fragments being processed are numerous (millions per second)
    - The context of what the information fragments mean is difficult to construct
    - Storing and transmitting lots of unauthorized information will be discovered. Finding the “crown jewels” in the blizzard of information is very challenging.
    - It requires additional or altered instructions and computing mechanisms to do something other than intended
  - Solution:
    - Trust your hardware and operating system vendors
      - Patch firmware and operating systems
    - Trust your hardware operators

Security Considerations – In transit

- Information in transit is not protected until something is done to protect it.
  - Practical challenges for the “bad guy”:
    - Needs access to the transmission channel
    - Needs to be able to piece together the information fragments received
    - Replay, alteration and disruption require the receiver not to notice and the receiver not telling the original sender
  - Solutions
    - Limit access to transmission channels
    - SSL/TLS and other transmission protocols scramble or encrypt making it hard for bad guy to reassemble useful info.
    - Security aware transmission protocols require authentication and check for replay and unexpected alterations
    - Alternative transmission paths and automatic resend try to avoid disruptions

Security Considerations – At rest

- Stored information is not protected until something protect it.
  - Practical considerations for the “bad guy”:
    - Access is needed to storage
    - Need to know what to look for
    - Need tools to find and manipulate stored info
    - Information needs to legible before it is useful
    - Raw file fragments on media require context in order to understand how the fragments fit together.
  - Solutions
    - Limit access to storage through authentication and physical proximity
    - Patch applications and services that may provide access to storage
    - Use prevention controls like ACLs to limit access to files and tools
    - Encrypt storage of portable media and mobile devices
    - Encrypt individual files and directories that need extra protection
    - Use detection controls to observe unusual access patterns that may imply unauthorized searches for valuable information
    - Use application level authentication and authorization to limit unauthorized exploration and information manipulation.

Security Management

- Security is not a destination, but a journey
  - The organization, IT environment and world are constantly changing, so securing an IT environment never ends
- Managing security requires continuous involvement with design, implementation and maintenance of systems, services and controls
- Managing security requires continuous reassessment of risk and verifying operation of security measures
- Managing security requires updating policy, standards, guidelines and procedures
- Managing security requires awareness by and training of everyone

Guidance beyond Policy

- Policy statements are typically broad
- They require interpretation and refinement
- Policy commonly authorizes the creation of guidance documents that provide more detail
- Standards
- Guidelines
- Procedure

Common Security Management Approach

- Prevent – Detect – Respond
- Prevent
  - Prevent violations of security policy
    - Influence design, implementation and maintenance to avoid or correct vulnerabilities, limit threats and limit use of unnecessary assets
    - Design, implement and maintain controls to complement or supplement systems and services
- Detect
  - Identify and verify violations of security policy
- Respond
  - Take actions to remedy the situation
  - Possibly take legal or administrative action against violator

END

CYBER SECURITY: IDEAS TO CONSIDER

START

ACTIVITY 6 REVIEW

END

ACTIVITY 6 REVIEW