Information Systems Audit: Module 4

Mathew A Thomas
Grad. CWA, FCA, MCA, CDM, ISA, CISSP.

Chapter 15

- ✓ Information Processing Architecture

Components of Communication Systems

- ✓ Sender
- ✓ Receiver
- ✓ Message
- ✓ Media
  - Paper, Cable, Radio …
- ✓ Protocol
  - An agreed-upon format for transmitting data between two devices.

Signal

- ✓ Properties
  - Amplitude
  - Frequency
  - Phase
- ✓ Types
  - Digital
  - Analog

Modulation

- ✓ Amplitude, Frequency, Phase

Transmission Modes

- ✓ Modes
  - Simplex
  - Half-Duplex
  - Full Duplex
- ✓ Methods
  - Synchronous
    - o
  - Asynchronous

Synchronous Communication

- ✓ Features
  - Used for communication between the computer and terminals
  - Responsibility of grouping the bits rests with the receiver
  - More efficient and faster.

Multiplexers (MUX) I

- ? A device that combines a large number of low-speed transmission lines into one high-speed line.
- ✓ Frequency Division Multiplexing
- ✓ Time Division Multiplexing
  - ? Synchronous (fixed)
  - ? Asynchronous (dynamically allocated)

Multiplexers (MUX) II

- ✓ Wave Division Multiplexing. Used on fiber optic cables

Concentrators

- Concentration techniques use schemes whereby input channels share a smaller number of output channels on some dynamic basis.
- Can route a message over a different path.
- Concentrators and MUX, both allow more efficient use of channel capacity.
- Concentrators and MUX, both protect against subversive attacks.

Concentration techniques

- ✓ Line/Circuit Switching
  - Temporary connection between input and output.
  - Connection-oriented.

Circuit-switching

- ✓ Advantages
  - ? Propagation delay is almost constant.
  - ? Guaranteed capacity.
  - ? Fixed bandwidth.
- ✓ Disadvantages
  - ? It is inflexible. Once a circuit is established that is the path to be followed irrespective of its deficiencies.
  - ? Connection setup and tear-down introduces extra overhead and initial delay.
  - ? Other users can't use the circuit even when it is free of traffic.
  - ? Users have to pay for the circuit when they do not send data.

Concentration techniques

- ✓ Message Switching
  - A complete message is sent to the concentration point and stored until a communication path can be established.
  - Store and Forward technique

Concentration techniques

- ✓ Packet Switching
  - A message is broken up small fixed length packets which are then routed individually.
  - Connection-less
  - Packets contain
    - ? Header (Length, Packet #, Addressess)
    - ? Body
    - ? Footer (CRC, Checksums)
  - Virtual Circuit and Datagram

Packet Switching

- ✓ Virtual Circuit

Packet Switching

- ✓ Datagram

Packet Switching

- ✓ Advantages
  - Makes use of resources more efficiently
  - Has a little setup or tear down time.
- ✓ Disadvantages
  - Delay is not guaranteed
  - Algorithms are more complicated.

Modems

- ✓ Modulator-Demodulator

- ✓ Analog to Digital and Digital to Analog
  - Increase speed, correct line errors (equalization), reduce line errors caused by noise (variable speed).

Transmission Media

- ✓ Bounded (Guided)
  - Twisted Pair (Shielded, Unshielded)
  - Coaxial Cable
  - Fiber Optic
- ✓ Unbounded (Unguided / Free space)
  - Radio
  - Terrestrial Microwaves
  - Satellite Microwave
  - Infrared

Twisted Pair Circuits

- ✓ Two insulated wires that are twisted around each other.
- ✓ One wire carries electricity to the telephone or modem and the other carries electricity away from the telephone or modem.
- ✓ This reduces the opportunity of cross talk between pairs in the same bundle. Twisted pairs can also be used for some dedicated data networks.

Coaxial Cables

- ✓ Have higher capacity than twisted pairs.
- ✓ A single coaxial cable can carry many voice, data and video signals at one time.
- ✓ Structure
  - Centre wire conductor, strand or solid
  - Plastic insulator
  - Outer conductor (shield) that confines to electric and magnetic fields within the tube.
  - Outer Jacket

Fiber Optic Systems

- ✓ Glass fibers used to carry binary signals as pulses of light.
- ✓ Structure
  - Core (Glass or Plastic)
  - Cladding
  - Coating

Fiber Optic Systems

- ✓ Advantages
  - Low transmission loss as compared to- twisted pairs.
  - Do not radiate energy or conduct electricity.
  - They are non-conductive
  - Free from cross talk
  - No lightening-induced interference
  - Significantly lower risk of wiretapping.
  - Optical fiber is smaller, lighter and cheaper than metallic cables of the same capacity.

Radio Systems

- ✓ Communicate data between using low powered systems that broadcast (or radiate) and receive electro magnetic signals representing data.
- ✓ Types of Propagations
  - Ground Wave
  - Line of Sight
  - Ionosphere

Radio Systems

- ✓ Communicate data between using low powered systems that broadcast (or radiate) and receive electro magnetic signals representing data.
- ✓ Types of Propagations
  - Ground Wave
  - Line of Sight
  - Ionosphere

Microwave Radio Systems

- ✓ Used by line-of-sight carrier systems to carry large quantities of voice and data signals.
- ✓ Transmitted through the air.
- ✓ Requires no right of way acquisition between transmission towers.
- ✓ However, it can be affected by atmospheric conditions and solid objects.

Satellite Radio link

- ✓ Systems contain several receiver/amplifier/transmitter sections called transponders.
- ✓ Each transponder operates at a slightly different frequency.
- ✓ Like microwaves, satellite signals can be affected by weather.

Transmission Media Comparison

Transmission Media Comparison II

Transmission Impairments I

- ✓ Attenuation
  - ? Weakening of a signal as the signal traverses the transmission medium.
  - ? Analog-Amplifier, Digital – Repeaters.
- ✓ Delay Distortion
  - ? Different signals frequencies traverse at different velocities. Only on bounded media.

Transmission Impairments II

- ✓ Noise
  - Random electrical signals that degrade performance.
  - Types
    - ? Thermal/White noise. Function of temperature.
    - ? Inter-modulation noise. Component Malfunction.
    - ? Crosstalk. Coupling of Signal Path
    - ? Impulse noise. Lightening, poor contacts.

Types of Network

- ✓ By Topology
  - Bus, Ring, Star etc.
- ✓ By Spatial Arrangement
  - LAN, MAN, WAN.
- ✓ By Signaling
  - ? Broadband and Baseband.
- ✓ Virtual Private Network (VPN)
  - ? Connect users or network to another network through Internet or other public Network.

Network Topologies

- ✓ Bus
- ✓ Ring
- ✓ Star
- ✓ Tree

- ✓ Mesh (Completely Connected)
- ✓ Irregular/Hybrid

Bus I
Bus II

- In a Bus, all the devices on the network are connected to a common cable. Normally, this cable is terminated at either end, and cannot form a closed loop.

- ✓ Advantages
  - ? Cabling costs are minimized because of the common trunk.
- ✓ Disadvantages
  - ? Difficult to trouble shoot because no central distribution points exist.
  - ? Cable breaks can disable the entire segment because they remove the required termination from each of the two cable fragments.

Ring I
Ring II

- In a Ring, all the devices on the network are connected to a common cable which loops from machine to machine. After the last machine on the network, the cable then returns to the first device to form a closed loop.

- ✓ Advantages
  - ? Ring topology has the advantage of being able to span larger distances than a bus topology because the message is sent from one computer to the next then that same message is regenerated in the receiving computer and sent on to the next computer.
  - ? Each repeater duplicates the data signals so that very little signal degradation occurs.
- ✓ Disadvantages
  - ? A break in the ring can disable the entire network. Many ring designs incorporate extra cabling that can be switched in if a primary cable fails.
  - ? Because each node must have the capability of functioning as a repeater, the networking devices tend to be more expensive.
  - ? Adding or removing computers can disrupt the network.

Star
Star II

- In the star configuration all nodes or servers (computers) connect to a central hub server. This configuration type is relatively easy to install, components can be easily attached or detached from the LAN without interfering with neighbouring components. If one node (computer) goes bad the rest of the system can function without interference. If, however, the hub server goes bad the whole system goes down.

- ✓ Advantages
  - ? Each device is isolated on its own cable. This makes it easy to isolate individual devices from the network by disconnecting them from the wiring hub. Adding and removing nodes is also easy.
  - ? All data goes through the central point, which can be equipped with diagnostic devices that make it easy to trouble shoot and manage the network.
  - ? Hierarchical organization allows isolation of traffic on the channel. This is beneficial when several, but not all, computers place a heavy load on the network. Traffic from those heavily used computers can be separated from the rest or dispersed throughout for a more even flow of traffic.
- ✓ Disadvantages
  - ? Because point-to-point wiring is utilized for each node, more cable is required.
  - ? Hub failures can disable large segments of the network.

Tree I
Tree II
Mesh I
Mesh II

- A Mesh topology consists of a network where every device on the network is physically connected to every other device on the network. This provides a great deal of performance and reliability, however the complexity and difficulty of creating one increases geometrically as the number of nodes on the network increases.

- ✓ Advantages
  - ? Yields the greatest amount of redundancy in the event that one of the nodes fails where the network traffic can be diverted to another node.
  - ? Network problems are easier to diagnose.
- ✓ Disadvantages
  - ? Cost of installation and maintenance is high (more cable is required than any other configuration

Audit Perspective - I

- ✓ Bus
  - ? Taps attenuate and distort signal. Performance degrades as nodes increase.
  - ? Taps are passive. Node failure will not lead to network failure.
  - ? Controls to protect privacy required.

Audit Perspective - II

- ✓ Ring
  - ? Point to point protocol. Repeaters do not introduce attenuation and distortion.
  - ? Timing errors may arise as bits of data transmitted.
  - ? Repeaters are active components. Failure of the repeater will bring the network down.
  - ? Controls to protect privacy of data required.

Audit Perspective - III

- ✓ Star
  - ? Reliability of the central hub is critical. Hub failure will bring the network down.
  - ? Failure of a node or link to a node will not bring the network down.
  - ? Security of the central hub is critical.
  - ? Servicing and maintenance relatively easy as diagnosis can be performed from the central hub.

Audit Perspective - IV

- ✓ Tree
  - ? Same as that of Bus/Tree.
- ✓ Mesh
  - ? Inherently reliable.
  - ? Cable length is maximum.
  - ? Very expensive.
  - ? Used mainly for WAN's.

CSMA/CD
Physical and Logical Topologies
Chapter 16

- ✓ ISO/OSI

Network Standards/Protocols

- ✓ IBM's SNA
  - System Network Architecture
- ✓ ISO/OSI
  - International Standards Organization/ Open Systems Interconnection
- ✓ TCP/IP
  - Transmission Control Protocol/Internet Protocol

ISO/OSI-I
ISO/OSI-II

Physical

- ✓ A hardware layer specifying
  - ? mechanical features (transmission medium and connectors)
  - ? electromagnetic features (voltage, signal strength, amplification, modulation).
- ✓ Receives data from some device and sends an unstructured bit stream.
- ✓ Network topology is part of the physical layer.

Data Link

- ⮝ Primarily a hardware layer specifying channel access control method (e.g., CSMA/CD, Token ring, etc.).
- ⮝ Ensures reliable transfer of data across the transmission medium.
- ⮝ The bit stream is divided into frames.
- ⮝ Synchronization
- ⮝ Error control and flow control
- ⮝ Link encryption is done at this level.

Network

- ⮝ Chooses the physical route through which a message packet is sent through the network.
- ⮝ Creates a virtual circuit for the upper layers so that they are independent of the data transmission and switching technologies used to connect nodes.
- ⮝ Ensures correct routing of data through the network.
- ⮝ Congestion Control and Addressing

Transport

- ✓ Ensures a reliable end-to-end transfer of a between user processes
- ✓ Assembly and disassembly of message packets.
- ✓ Flow control
- ✓ Connection Control
  - ? whether to send all data packets by a single path or not
- ✓ End-to-end error recovery
- ✓ End-to-end encryption

Session

- ✓ Establishes, maintains and terminates sessions (interactions) between user processes.
- ✓ Token Management
- ✓ Checkpoints (e.g. to resume file transfer)

Presentation

- ✓ Controls how data appears on the screen.
- ✓ Transforms data to provides a standard application interface.
- ✓ Format Conversion
- ✓ Compression
- ✓ Encryption

Application

- ✓ Provides services to users.
  - ⮝ Electronic mail, File sharing, File transfer, etc.

Devices

- ✓ Networking Components
  - ? Transmission Media
  - ? Hubs, Repeaters, Switches
  - ? Modems
  - ? Multiplexers & Concentrators
- ✓ Internetworking Components
  - ? Bridges, Routers and Gateways

Repeaters

- ✓ Operate on Digital Signal
- ✓ Physical Layer

Bridges

- ⮝ A bridge is a device that transparently connects similar and dissimilar local area networks (LANs).
- ⮝ Bridges function at the Data Link layer.

Bridges

Routers

- ⮝ Routers connect heterogeneous networks.
- ⮝ Routers determine the optimal path between two end stations.
- ⮝ Routers communicate with each other and share information that allows them to determine the best route through a complex internetwork that links many LANs.
- ⮝ Routers operate in the Network Layer

Brouter

- ✓ Combination of Bridge and Router
- ✓ Acts as Router for one Protocol and as a Bridge for another Protocol

Gateways

- ⮝ They perform protocol conversion to allow interoperability between two different types of communications architectures.
- ⮝ Application gateways connect two parts of an application in the application layer.
- ⮝ A gateway passes data between networks having similar functions but dissimilar implementations.
- ⮝ They operate in the Application Layer.

Error Control I

- ✓ Feedback (backward) error control
  - ⮝ Receiver can only identify that an error has occurred.
  - ⮝ An associated retransmission control scheme is then used to request that another copy of the information be sent.
- ✓ Forward error control
  - ⮝ Additional redundant information is transmitted with each character or frame so that the receiver can not only detect when errors are present, but can also determine where the error has occurred and thus correct it.

Error Control II

- ✓ Error Detection
  - ? Loop Check
  - ? Parity Check
  - ? Cyclical Redundancy Check
  - ? Checksum
- ✓ Error Correction
  - ? Forward Error Correcting Codes.
    - ★ Corrected at the receiving end.
    - ★ Hamming Code
  - ? Retransmission
    - ★ ACK, NAK

IEEE Standards

Chapter 17

- ✓ Firewall, Cryptography,
- ✓ Client/Server, Network Management

Firewall

- ✓ A firewall is a system or group of systems that enforces an access control policy between two networks.
- ✓ Components
  - ? Packet Filtering Router
  - ? Application Level Gateway or Proxy Server
  - ? Circuit-level Gateway
- ✓ Implementation
  - ? Screened host firewall
  - ? Screened subnet firewall
  - ? Dual-homed gateway

Packet Filters

- ✓ A packet-filtering router makes a permit/deny decision for each packet that it receives.
- ✓ Compromises
  - ⮝ Source IP Address Spoofing Attacks
    - ? The packets falsely contain the source IP address of an inside system.
  - ⮝ Source Routing Attacks
    - ? The source station specifies the route and causes the packet to follow an unexpected path to its destination.
  - ⮝ Tiny Fragment Attacks
    - ? The intruder creates extremely small fragments forcing the TCP header information into a separate packet fragment.
    - ? Designed to circumvent user-defined filtering rules.

Application Level Gateway

- ✓ A proxy service is installed on the gateway for each desired application.
- ✓ If there is no proxy code for a an application, that service is not supported
- ✓ The proxy code can be configured to support only acceptable features

Circuit-level Gateway

- ✓ A circuit-level gateway simply relays TCP connections without any additional packet processing or filtering.
- ✓ Because the connection appears to originate from the firewall system, it conceals information about the protected network.
- ✓ Circuit-level gateways are often used for outgoing connections where the system administrator trusts the internal users.

Bastion Host

- ✓ An application-level gateway is often referred to as a "bastion host" because it is a designated system that is specifically armoured and protected against attacks
- ✓ Features
  - ⮝ "secure" version of operating system
  - ⮝ Additional authentication
  - ⮝ Subset of an application's command set
  - ⮝ Allows access only to specific host systems
  - ⮝ Detailed audit information

Packet Filters

- ✓ Packet-filtering router deployed between the private network and the Internet

Screened Host Firewall

- ⮝ Here a router operating at a network level controls access to and from a single host.
- ⮝ Network-layer security (packet-filtering)
- ⮝ Application-layer security (proxy services)

Screened Subnet Firewall

- ⮝ A router at the network level controls access to and from a whole network.
- ⮝ It is similar to a screened host, except that it is effectively a network of screened hosts.

Dual-homed Gateway

- ⮝ a highly secured host that runs proxy software. It has two network interfaces, one on each network, and blocks all traffic passing through it.

Limitations of Firewalls

- ✓ Firewall cannot protect against attacks that do not go through it.
  - ⮝ Dial-up connections, media theft, etc.
- ✓ Virus Attacks

General Controls associated with Firewalls

- ✓ Physical security controls
- ✓ Operating System Security
  - ⮝ A firewall must run on a secure and tamper-proof operating system.
- ✓ Change Control Procedures :
  - ⮝ Patching/Updating process is complete
- ✓ Verification of documents
  - ⮝ Documentation of network diagrams, changes, log analysis
- ✓ Examination of log

Firewall Lifecycle

- ✓ Definition of Security Policy
- ✓ High-Level Design
- ✓ Selection of Firewall Components
- ✓ Implementation, Configuration
- ✓ Review, Testing and Validation
- ✓ Maintenance

Intrusion Detection Systems

- ✓ An "Intrusion Detection System (IDS)" is a system for detecting attempts to break into or misuse the protected system.

Cryptography

Introduction I

- ✓ Cryptology
  - ? is the science of secret codes incorporating cryptography and cryptanalysis.
- ✓ Cryptography
  - ? Deals with systems for transforming data into codes (cryptograms) that are meaningless to anyone who does not possess the system of recovering the initial data.

Introduction II

- ✓ Cryptanalyst
  - ? A person who breaks ciphers. Code-breaker.
- ✓ Cryptographer
  - ? One who designs cryptographic system.

- ✓ Plaintext (Cleartext), Ciphertext, Key.
  - ? Plaintext, the message to be encrypted.
  - ? Ciphertext, the output of the encryption process.
  - ? Key consists of a relatively short string that selects one of many possible encryptions.

Threats

- ✓ Threat addressed by Cryptographic Systems
  - Interruption
  - Interception
  - Modification
  - Fabrication
- ✓ Goals of Cryptographic Systems
  - Privacy/Confidentiality
  - Integrity
  - Authentication
  - Non-Repudiation (Origin, Receipt and Content)
  - Minimality

Cryptanalysis

- Ciphertext-only attack
- Known-plaintext attack
- Chosen-plaintext attack
- Adaptive-chosen-plaintext attack
- Chosen-ciphertext attack
  - ? Access to a tamperproof box that does automatic decryption
- Chosen-key attack
  - ? Knowledge about the relationship between different keys
- Rubber-hose cryptanalysis
- Purchase-key attack

Cryptographic Model Classification

- ✓ Symmetric Cryptosystem
  - Stream ciphers
  - Block Cipher
- ✓ Asymmetric Cryptosystem

Substitution Ciphers

- ✓ Caesar Cipher
  - ? Shift by 3 letter
  - ? Message: PEACE
  - ? Cipher text: SHDFH
- ✓ Mono-Alphabetic
- ✓ Poly-Alphabetic

Mono-Alphabetic Substitution Ciphers

- ✓ Cleartext: ABCDE FGHIJ KLMNO P…
  Key: IDEAS BCFGH JKLMN O…
- ✓
- ✓ Message: PEACE
  Ciphertext: OSIES

Poly Alphabetic Ciphers

- ✓ Message
  - CABBAGE
- ✓ Ciphertext
  - ECDDCKH
  - IGHHGMK
  - EGDHCMH

Transposition Cipher

- ✓ Cleartext:
  Key:
- ✓
- ✓ Message: PEACE TO ALL
  Ciphertext: EPCA EOTA LL

Transposition Ciphers

- ✓ Message:
  - Please transfer 1 million dollars to my Swiss bank account six two two
- ✓ Ciphertext:
  - AFLLSKSO SELAWAIA TOOSSCTC LNMOMANT ESI LYNTW RNNTSOWD PAEDBUO ERIRICXB
- ✓

Product Cipher

- ✓ Use a combination of substitution and transposition ciphers.
- ✓ Widely used today.

Desirable Features

- ✓ High Work Factor
  - ? Harder for the Cryptanalyst to break.
- ✓ Small Key
  - ? Can be changed easily and frequently.
- ✓ Simplicity
- ✓ Low Error Propagation
  - ? While using a chained encryption system.
- ✓ Little expansion of Message Size
  - ? When introducing noise.

Data Encryption Standard

Data Encryption Standard

Other Symmetric Cryptosystem

- ✓ Triple DES
- ✓ Skipjack
  - ? 80-bit key.
  - ? Scrambles 32 times.
  - ? Divided & Shared secret key.
  - ? Clipper Chip.

Asymmetric Cryptosystem

- ✓ Whitfield Diffie and Martin Hellman
  - ? Introduced the concept in 1976.
  - ? Different keys for Encryption and Decryption
  - ? Symmetric keys and the problem of key exchange.
- ✓
- ✓ RSA Algorithm
  - ? Ronald Rivest, Adi Shamir, Leonard Adleman

Public Key Cryptosystem I

Public Key Cryptosystem II

Public Key Cryptosystem III A

Public Key Cryptosystem III B

Digital Signature I

- ✓ One Way Hash Function
  - ? Takes a variable amount of data and computes a fixed length string
- ✓ Message Digest

- ? MD5, SHA1
- ✓ Clearsigning
  - ? Sign the hash value with the private key.

Digital Signature
Hybrid Method
Digital Signature II

- ✓ Ensures:
  - ? Data Integrity
  - ? Message Authentication
  - ? Non-repudiation
  - ? Replay Protection
    - ★ With sequence numbers and digital timestamping.
- ✓ Certifying Authority
  - ? Trusted Third Party who signs the public key of clients using its own private key.

Digital Signature Certificate.

- ✓ Contains
  - ? Public Key of the user
  - ? Name of the User
  - ? Name of the certification Authority
  - ? Validity period of the key.

Client Server
Network Management
Client /Server Introduction

- ✓ Mainframes/Machines and Time-sharing
- ✓ Network-based / File-sharing architecture:
- ✓ Client/server architecture.
  - ⅄ The applications are split so that the processing may take place on different machines.
  - ⅄ A C/S environment is one in which one computer acts as the server and provides data distribution and security functions to other computers that are independently running various applications.

2-Tier Client/Server I
2-Tier Client/Server II

- ✓ A Client or front-end program
  - ? GUI tasks (usually developed in 4GLs).
  - ? Business rules and application logic (data validation, computation, decisions etc.).
- ✓ A file or (more usually) a database server
- ✓ Limitations:
  - ? As the application logic becomes more complex, the client needs more memory and CPU power (fat-client syndrome)
  - ? As the number of concurrent users increase, bottlenecks appear. 50-200 users (non-scalable)

3-Tier Client/Server I
3-Tier Client/Server II

- ✓ A thin client
  - ? GUI tasks (example browser).
- ✓ One or more Application Servers.
  - ? Running the application logic/business rules.
- ✓ One or more Database servers

Middleware II

- ✓ Transaction Processing (TP) Monitors
  - ⅄ Programs that handle and monitor database transactions and are used primarily for load balancing.
- ✓ Remote Procedure Calls (RPC)
  - ⅄ A protocol that enables a program on the client computer to execute another program on a remote computer (usually a server).

Middleware III

- ✓ Object Request Broker (ORB) Technology
  - ⅄ The use of shared, reusable business objects in a distributed computing environment.
  - ⅄ Ability to support interoperability across languages and platforms, as well as enhance maintainability and adaptability of the system.
  - ⅄ Examples of such technologies are Common Object Request Broker Architecture (CORBA) and Microsoft's Component ,Object Model (COM/DCOM).
- ✓ Messaging Servers
  - ⅄ Asynchronously prioritize, queue and/or process messages using a dedicated server.

Middleware Risks

- ✓ Risks
  - ⅄ System integrity may be adversely affected because of multiple operating environments attempting to interact concurrently.
  - ⅄ Lack of proper software change procedures across multiple platforms could result in a loss of system integrity.
- ✓ Controls
  - ⅄ Controls to ensure the integrity of the client/server networks.
  - ⅄ Systems should be properly tested and approved and that modifications are properly implemented.
  - ⅄ Adequate version control procedures should be properly implemented.

3-Tier Client/Server II

- ✓ Advantages
  - ? Thin clients, therefore cheaper
  - ? More scalable. 1000+ users. Load balancing among the servers.
  - ? Internal or e-Business applications.
  - ? Business Logic can be isolated from the rest of the code.

Introduction to Network Management

- ✓ ISO's Five Conceptual Areas
- ✓ Performance Management
  - ? Network performance is maintained at an acceptable level
- ✓ Configuration Management
  - ? Monitor network and system configuration information to minimize version conflicts
- ✓ Accounting Management
  - ? Measure network utilization parameters
- ✓ Fault Management
  - ? Detect, log, notify users of, and fix network problems.
- ✓ Security Management
  - ? Control access to network resources

Chapter 18

- ✓ Internet Technologies

Connecting to the Internet

- ✓ Dedicated access
- ✓ Dial up access
- ✓ BBS
  - Generally provide online services on a small sEcale
  - Usenet
- ✓ Wireless Internet connection is available from certain providers only

Terms

- ✓ Winsocks
  - Winsocks is expanded as Windows sockets.
  - Functions for the Windows Internet application.
- ✓ Terminal Emulation software
  - Enables computer to act as a terminal.
- ✓ Freenets
  - Local community computer system or free computing systems

E-Mail

- ✓ How E-mail is delivered
- ✓ Mail Client
- ✓ Mail Server

Internet

- ✓ Internet Addressing
- ✓ Domain Name System
- ✓ URL: Uniform Resource Locator
  - http://www.icai.org/isa/results.html
- ✓ HTTP, Telnet, FTP
- ✓ Gopher
  - Information browser just like FTP with enhancements for ease of use and flexibility
  - Hierarchical menu of links
  - Web Server and Clients

Internet

- ✓ Proxy Servers
  - ? A server that is empowered to act on behalf of other computers on a network is known as a Proxy Server
- ✓ Common Gateway Interface
  - ? An executable machine independent software program that can be attached to server web page that performs a specific task.
- ✓ Applets
  - ? Programs downloaded from web servers that execute on client web browser machines.

Internet

- ✓ Internet Service Provider
- ✓ Browser
- ✓ Cookies
  - ? A file stored on a client machine containing a set of attributes value pairs received from a web server.
  - Uses
    - ? Identifying the state
    - ? Determining the number of visitors
    - ? Storing user preferences
    - ? Virtual Shopping Mall
    - ? Site personalization
  - Disabling Cookies

Internet

- ✓ Search Engines
- ✓ Protocols
  - POP
  - SMTP
- ✓ ICMP
  - Send error or control messages
- ✓ SSL
- ✓ SET

Secure Socket Layer

- ✓ Developed by Netscape for transmitting private documents via the Internet.
- ✓ SSL works by using a private key to encrypt data that's transferred over the SSL connection.
- ✓ Both Netscape Navigator and Internet Explorer support SSL
- ✓ Web sites use the protocol to obtain confidential user information, such as credit card numbers.
- ✓ By convention, Web pages that require an SSL connection start with https: instead of http.

SET Credit Card Purchase Model

SET Dual Signature

Chapter 19

- ✓ TCP/IP

TCP/IP I

Internet Layer

- ✓ It is a packet switching network based on a connectionless inter-network layer.
- ✓ The internet layer defines an official packet format and protocol called IP(Internet Protocol).
- ✓ It job is to permit hosts to inject IP packets into any network and have them travel independently to the destination.
- ✓ The major concerns at this layer is packet routing and avoiding congestion.

Transport Layer

- ✓ The transport layer is designed to allow peer entities on the source and destination hosts to carry on a conversation.
- ✓ Two end-to-end protocols have been defined here, TCP and UDP.

Transport Layer - TCP

- TCP (Transmission Control protocol) is a reliable connection oriented protocol that allows a byte stream originating on one machine to be delivered without error on any other machine on the Internet.
- It fragments the incoming byte stream into discrete messages and passes each one into the internet layer.
- At the destination, the receiving TCP process reassembles the received messages into the output stream.
- TCP also handles the flow control to ensure that a fast sender does not swamp a slow receiver with more messages than it can handle.

Transport Layer - UDP

- UDP (User Datagram Protocol) is an unreliable connectionless protocol for applications that do not want TCP's sequencing or flow-control and wish to provide their own.

- It is also widely used for one-shot client-server type request-reply queries and applications in which prompt delivery is more important than accurate delivery, such as transmitting speech or video.

Application Layer

- ✓ The application layer contains all the higher level protocols.
  - TELNET (Terminal Network Emulation or Virtual Terminal) protocol allows a user on one machine to log on to a distant machine and work there.
  - FTP (File Transfer Protocol) provides a way move data efficiently to move data efficiently from one machine to another.
  - In fact, electronic mail was originally just a kind of file transfer, but later a specialised protocol, SMTP (Simple Mail Transfer Protocol) was developed.

IP Addressing

- ✓ 32 bits usually formatted as 4 octets
- ✓ $2^8.2^8.2^8.2^8$
- ✓ 202.5.20.96
- ✓ Two pieces of information
  - Network ID
  - Host ID
- ✓ Class A Network
  - First bit of the first octet is always zero.
  - The next seven bits of the first octet complete the network ID.
  - The remaining 24 bits (the last three octets) represent the host ID.

IP Addressing

- ✓ Class B Network
  - The two high-order bits in a class B address are always set to binary 1 0.
  - The next 14 bits complete the network ID.
  - The last two octets represent the host ID.
- ✓ Class C Networks
  - The three high-order bits set to binary 1 1 0.
  - The next 21 bits complete the network ID.
  - The last octet represents the host ID.
  - This allows for 2,097,152 networks and 254 hosts per network

IP Addressing
Address Resolution Protocol

- ✓ The Address Resolution Protocol (ARP) is a low-level protocol that dynamically maps network layer addresses to physical addresses.

Miscellaneous Topics
Devices I

- ✓ Terminals
  - ? An device providing access to a computer; has a keyboard and display.
- ✓ Protocol Converters
  - ? A device to convert from one protocol to another (Sync to Asynch)
- ✓ Spools
  - ? Output to Disk File / Audit Concern
- ✓ Buffers
  - ? Temporary storage space.

Front End Communication Processors

- A front-end processor is a programmed-logic or stored program device that interfaces data communication equipment with an i/o bus or memory of a data processing computer.
- It reduces the workload of a host computer by performing certain tasks that the host computer would be doing. Other functions include:
  - ★ Polling and addressing of remote units
  - ★ Character code translation
  - ★ Control character recognition and error checking
  - ★ Error recovery and diagnostics
  - ★ Activating and deactivating communication lines

Cluster Controllers

- Hardware device that coordinates and manages the operation of one or more input/output devices such as computer terminals, workstations, disks and printers.
- Benefits:
  - ? Cost of the communication logic is amortized over a number of terminals.
  - ? Single point of interface to a communication circuit on both the terminal and computer ends, thus saving on I/O hardware costs.
  - ? Easier to manage related resources or devices that are treated as a unit

Cluster Controllers II
Types of Network

- ✓ Broadband
  - Analog signaling. FDM. Covers longer distances as compared to baseband as analog signals are less attenuated.
- ✓ Baseband
  - Digital signaling. Entire bandwidth used by the signal. Easy to wiretap.

ISDN

- ✓ Integrated services Digital Network
  - Architecture for world wide telecommunications
  - Integrates voice, data, video through digital switching and transmission
  - Narrowband (basic-rate) ISDN
  - Broadband ISDN.

Internet Threats I

- ✓ Disclosure
  - ? Messages and data traversing the Internet can seen by other machines.
- ✓ Masquerade
  - ? A user pretending to be someone else to gain additional privileges or access to otherwise forbidden data or systems.
- ✓ Unauthorized Access
  - ? Many internet software packages contain vulnerabilities that render systems subject to attack.
- ✓ Loss of Integrity
  - ? Interception of messages and changing its contents or repeating a message.

Internet Threats II

- ✓ Denial of Service
  - ? DOS attacks occur when a computer connected to the Internet is inundated (flooded) with data or requests that must be serviced.
- ✓ Distributed Denial of Service(DDOS)
- ✓ Theft of service or resources
  - ? Where the Internet is used for delivery of service, unauthorized access to the service is effectively theft.

Network Monitoring Reports I

- ✓ Response time reports
  - ? Identify the time it takes for a command entered by a user at a terminal to be answered by the computer.
- ✓ Downtime Reports
  - ? Track the availability of the telecommunication lines.
  - ? Interruptions due to power failure, traffic overloading, operator error are identified.

Network Monitoring Reports II

- ✓ On-line Monitors
  - ? Measure telecommunication transmission and determine whether transmissions were accurate and complete.
- ✓ SNMP-Based Network Management Tools
  - ? Monitor different variables throughout the network.
  - ? Based on the operator instructions the management software sends specific requests to a device to capture the information needed.
  - ? In order to perform all of these tasks, each device (routers, switches, hubs, PCs, servers) needs to have a SNMP agent running, so the actual SNMP communications occur between all the agents and the console.

Network Monitoring Reports II

- ✓ Protocol Analyzers
  - ? Monitor and record all the packets travelling in the link in which the analyzer is attached.
  - ? They decode the different protocols that are in each protocol, display several statistics (percentage of used bandwidth, protocol distribution etc.) and in some products, provide information about problems and possible solutions
- ✓ Help Desk Reports
  - ? Provide end user with an easy means of identifying and resolving problems quickly before they have a major effect on IS performance and end user resource utilization.
  - ? The reports prepared by help desk provide a history of problems and their resolution.

Subversive Attacks

- ✓ Active Attacks
  - ? Message Insertion
  - ? Message Deletion
  - ? Message Modification
  - ? Changing Message Order
  - ? Denial of Message Service
  - ? Spurious Associations (Replay of handshake seq.)
- ✓ Passive Attack
  - ? Traffic Analysis
  - ? Release of Message Contents

Controls over Subversive Threats

- ✓ Link Encryption
- ✓ End-to-end Encryption
- ✓ Stream Cipher
- ✓ Error Propagation Codes
- ✓ Message Authentication Codes
- ✓ Message Sequence Number
- ✓ Request Response Mechanism

Encryption I

- ✓ Link Encryption
  - Protects data traversing a communication channel connecting two nodes on a network
  - The message and its associated source and destination
  - LE reduces expected losses from traffic analysis.
- ✓ End-to-end Encryption
  - Protects the integrity of data between sender an recipient.
  - No protection against traffic analysis.

Encryption II

- ✓ Stream Cipher
  - ? Plaintext is transformed bit-by-bit under the control of a stream of key bits
- ✓ Error Propagation Codes
  - ? To protect the integrity of messages, a code that is sensitive to the order of bits in a message is used.
- ✓ Message Authentication Codes (MAC)
  - ? In EFTS, a control used to identify changes to message in transit is called a MAC.
  - ? An encrypted checksum of the message. Digital Signature.

Other controls

- ✓ Message Sequence Number
  - ? Message Sequence Number are used to detect an attack on the order of messages.
- ✓ Request Response Mechanism
  - ? A timer (placed with both S and R) periodically triggers a control message from the sender. R to respond with another control message derived from the message.

Subversive Threats – Summary

IS Auditor Role

- ✓ Identify and document the following:
  - ? LAN topology and network design
  - ? LAN Administrator/LAN Owner
  - ? Functions performed by the LAN Admin/Owner
  - ? Distinct groups of LAN users
  - ? Computer applications used on the LAN
  - ? Procedures and standards relating to network design, support, naming conventions and data security.

LAN - Physical controls I

- ✓ Computers in a LAN are usually decentralized.
- ✓ Company data stored on a file server is easier to damage or steal than when on a mainframe and should be physically protected.
- ✓ Protect hardware and access points to the LAN by limiting access to those individuals authorized by management.

LAN - Physical controls II

- ✓ The IS Auditor should review the following:
  - LAN hardware devices, particularly the file server and documentation, should be location in a secure facility and restricted to the LAN administrator. Other components included in the physical security review should be the wiring closet and cabling.
  - Keys to the LAN file server facility should be controlled to prevent or minimize the risk of unauthorized access.

- LAN file server housing should be locked or otherwise secured to prevent removal of boards, chips and the computer itself.

LAN - Physical controls III

- ✓ To test physical security, an IS Auditor should perform the following:
  - Inspect the LAN wiring closet and transmission wiring and verify they are physical secured
  - Observe the LAN file server computer and verify it is secured in a manner to reduce risk of removal of components and the computer itself.
  - Obtain a copy of the key logs for the file server room and the wiring closet, match the key logs to actual keys that have been issued and determine that all keys held are assigned to the appropriate people, for example, the LAN Administrator and support staff.

LAN - Environmental Controls I

- LAN file server equipment should be protected from the effects of static electricity (an static rug) and electrical surges (surge protector).
- Air conditioning and humidity control systems should be adequate to maintain temperatures within manufacturers' specifications.
- The LAN power supply should be properly controlled to ensure it remains within t manufacturer's specifications.
- The LAN should be equipped with an UPS that will allow the LAN to operate in case of minor power fluctuations or to be brought down gracefully in case of a prolonged power outage.
- The LAN file server facility should be kept free of dust, smoke and other mat particularly food.
- Backup diskettes and tapes should be protected from environmental damage and effects of magnetic fields.

Testing LAN - Environmental Controls

- ✓ IS Auditor should Visit the LAN file server facility and verify :
  - Temperature and humidity are adequate.
  - Electric surge protectors are in place.
  - Fire extinguishers are nearby
  - Observe the LAN file server facility, looking for food and beverage containers and tobacco products in the area and in the garbage cans. .
  - Observe the storage methods and media for backup and verify they are protected from environmental damage.

LAN Logical Security

- ✓ LAN logical security controls should be in place to restrict, identify and report authorized and unauthorized users of the LAN.
- ✓ Users should be required to have unique passwords and be required to change them periodically. Passwords should be encrypted and not displayed on the computer screen when entered.
- ✓ LAN user access should be based on written authorization and given on a need to know/need to do basis. This should include documenting requests for adds, changes and deletions of LAN logical access.
- ✓ A LAN workstation should be disabled automatically after a short period of inactivity.
- ✓ Remote access to the system supervisor should be prohibited. For maximum security an individual should only be able to logon to the supervisor account on the console terminal. This combination of physical security over consoles and logical security over the supervisor account provides for maximum protection against unauthorized access.
- ✓ All logon attempts to the supervisor account should be logged on the computer system.
- ✓ Up-to-date information about all communication lines connected to the outside should be maintained by the LAN supervisor.

Testing LAN Logical Security I

- ✓ To test logical security, an IS Auditor should perform the following:
  - Interview the person responsible for maintaining LAN security to ensure that person is:
  - Aware of the risks associated with physical and logical access that must be minimized
  - Aware of the need to actively monitor logons and to account for employee changes
  - Knowledgeable in how to maintain and monitor access
  - Interview users to assess their awareness of management policies regarding LAN security and confidentiality.
  - Evaluate a sample of LAN users' access/security profiles to ensure access is appropriate and authorized based on the individual's responsibilities.
  - Review a sample of the security reports to:
  - Ensure only authorized access is occurring

Testing LAN Logical Security II

- Verify timely and effective review of these reports is occurring and that there is evidence of the review
- Interview users to assess their awareness of management policies regarding LAN security and confidentiality.
- Evaluate a sample of LAN users' access/security profiles to ensure access is appropriate and authorized based on the individual's responsibilities.
- Review a sample of the security reports to:
- Ensure only authorized access is occurring
- Verify timely and effective review of these reports is occurring and that there is evidence of the review

Testing LAN Logical Security III

- Look for unauthorized users. If found, determine the adequacy and timeliness of follow-up procedures
- Attempt to gain access using a variety of unauthorized logon-IDs/passwords. Verify that access is denied and logged. Logon to and briefly use the LAN. Then, verify that access and use are properly recorded on the automated activity report.
- If the LAN logon session automatically logs off after a short period of inactivity, logon lo the terminal and visually verify the automatic logoff feature.
- Visually search for written passwords in the general areas of the computers that utilize the LAN.
- If the LAN is connected lo an outside source through a modem or dial-up network attempt to gain access lo the I.AN through these telecommunications medium using authorized and unauthorized management.
- Review a sample of LAN access change requests and determine if they are authorized by the appropriate management and that the standard form has been utilized.

Dial-Up Access Controls

- ✓ To test for dial-up access authorization, the IS Auditor should:
  - dial the computer from a number of authorized and unauthorized telephone lines.
  - If controls are adequate, successful connection will occur with the authorized numbers only.

- The IS Auditor should test the logical controls invoked after authorized connections to the computer are achieved by using the successful dial-up connections to attempt to gain unauthorized file access.

✓ Performance of this test may be coordinated through the security administrator to avoid violating security regulations.

✓

Thank You

Mathew A Thomas
mat@vsnl.com
http://www.mathomas.biz/