CISSP Bootcamp: VOLUME TWO

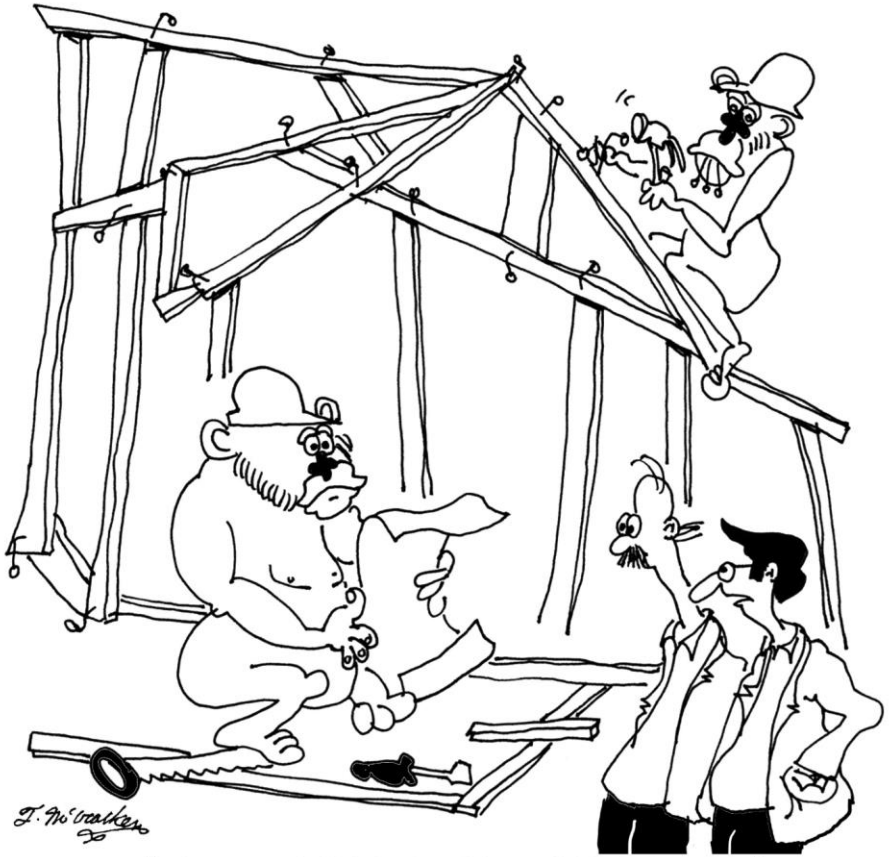
Certified Information Systems Security Professional

Kelly Handerhan, Instructor, Owner, CyberTrain.it
CISSP, CCSP, CISM, CRISC, PMP, Security+, etc.
KellyH@CyberTrain.IT

Domain 3

Security Architecture and Engineering

Part 2 : Security Architecture and Design



Domain 3 Part 2: Security Architecture and Design Agenda

- Security Models
- System Architecture
- The Trusted Computing Base
- Hardware Architecture
- Software: Operating System Architecture
- Software: Application Architecture
- Secure Modes of Operation
- Certification and Accreditation

Security Models

Security Models and Architecture

- A **security model** Provides the means to formalize a system policy into an explicit set of **rules** that a computer can follow to implement the fundamental security concepts, processes, and procedures that make up a security policy
- The **system architecture**, in turn, is the overall design and description of the interaction of (HW, SW, Applications, etc.) of an information system.
- This architecture should enforce the specifications provided by the security model.

Security Models

- State Machine Model
- ****The Bell-LaPadula Model**
- ****The Biba Model**
- **The Clark-Wilson Model**
- **The Brewer & Nash Model**
- The Information Flow Model
- The Non-Interference Model
- The Lattice Model

State Machine Model

- The state of a system is its snapshot at any one particular moment. The state machine model describes subjects, objects, and sequences in a system. The focus of this model is to capture the system's state and ensure its security.
- When an object accepts input, the value of the state variable is modified. For a subject to access this object or modify the object value, the subject should have appropriate access rights.
- State transitions refer to activities that alter a systems state.

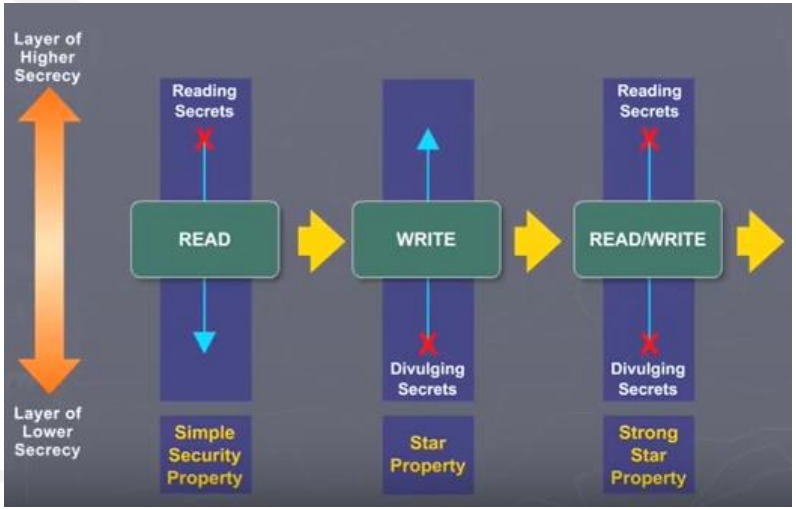
Bell-LaPadula Model

- Confidentiality model
- Developed by David Elliot Bell and Len LaPadula
  - ➢ This model focuses on data confidentiality and access to classified information.
  - ➢ A Formal Model developed for the DoD multilevel security policy
  - ➢ This formal model divides entities in an information system into subjects and objects.
  - ➢ Model is built on the concept of a state machine with different allowable states (i.e. Secure state)

Bell Lapadula

Three Rules to enforce confidentiality:

- Simple Security Property – "no read up"
  - A subject cannot read data from a security level higher than subject's security level.
- * Security Property – "no write down"
  - A subject cannot write data to a security level lower than the subject's security level.
- Strong * Property – "no read/write up or down".
  - A subject with read/write privilege can perform read/write functions only at the subject's security levels.

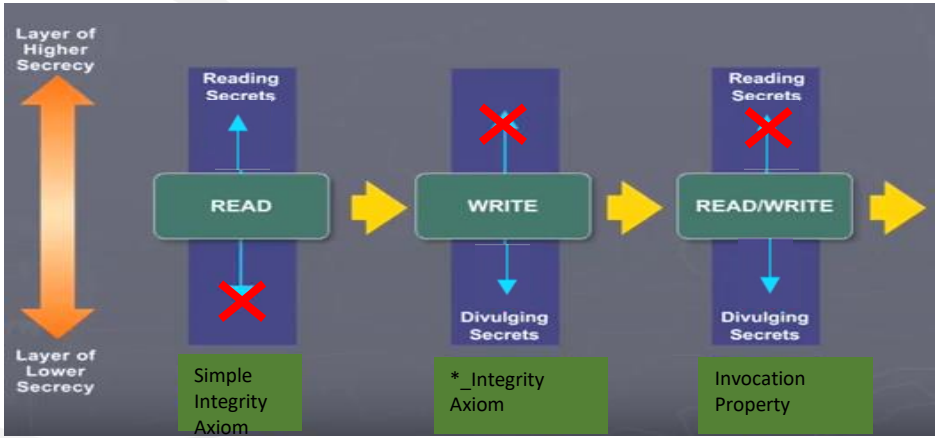


Biba Integrity Model

- Developed by Kenneth J. Biba in 1977 based on a set of access control rules designed to ensure data integrity
- No subject can depend on an object of lesser integrity
- Based on a hierarchical lattice of integrity levels
- Authorized users must perform correct and safe procedures to protect data integrity

Biba Integrity Model

- Three Rules:
- Simple integrity axiom – “no read down” – A Subject cannot read data from an object of lower integrity level.
- * Integrity axiom – “no write up” – A Subject cannot write data to an object at a higher integrity level.
- Invocation property – A subject cannot invoke (call upon) subjects at a higher integrity level.



Clark-Wilson

Integrity model

Model Characteristics:

Clark Wilson enforces well-formed transactions through the use of the access triple:

User➔Transformation Procedure➔CDI (Constrained Data Item)

Deals with all three integrity goals

SEPARATION of DUTIES

➢Prevents unauthorized users from making modifications

➢Prevents authorized users from making improper modifications

➢Maintain internal and external consistency – reinforces separation of duties

Commercial Models: Brewer-Nash

Brewer-Nash Model – a.k.a. Chinese Wall

- Developed to combat conflict of interest in databases housing competitor information

➢Publish in 1989 to ensure fair competition

➢Defines a wall and a set of rules to ensure that no subject accesses objects on the other side of the wall

➢Way of separating competitors data within the same integrated database

Information Flow Model

- Data is compartmentalized based on classification and the need to know
- Model seeks to eliminate covert channels
- Model ensures that information always flows from a low security level to a higher security level and from a high integrity level to a low integrity level.
- Whatever component directly affects the flow of information must dominate all components involved with the flow of information

Non-interference Model

Model Characteristics:

- Model ensures that actions at a higher security level does not interfere with the actions at a lower security level.
- The goal of this model is to protect the state of an entity at the lower security level by actions at the higher security level so that data does not pass through covert or timing channels.

Lattice Model

- Model consists of a set of objects constrained between the least upper bound and the greatest lower bound values.
- The least upper bound is the value that defines the least level of object access rights granted to a subject.
- The greatest lower bound is value that defines the maximum level of object access rights granted to a subject
- The goal of this model is to protect the confidentiality of an object and only allow access by an authorized subject.

System Architecture

Security Architecture Overview

- Security architecture directs how the components included in the system architecture should be organized and interact to ensure that security requirements are met.
  - A description of the locations in the overall architecture where security measures should be placed.
  - A description of how various components of the architecture should interact to ensure security.
  - The security specifications to be followed when designing and developing the system.

The Trusted Computing Base

The Trusted Computing Base

- Trusted Computing Base: The trusted computing base (TCB) consists of all hardware, software, and firmware within a system that provide enforces the security of a system and provides a description of the trust of a system.
- Security Perimeter: Conceptual separation between the TCB and the untrusted elements of a system
- TCB components include the CPU, RAM, the OS Kernel, BIOS, etc.
- The TCB is what is evaluated when certifying a system

Hardware Architecture

Hardware Architecture

- Central Processing Unit (CPU)
  - Registers
  - ALU
  - Math Co-processor
- Memory
  - ROM
  - RAM
    - SRAM
      - Cache L1, L2, etc
    - DRAM
    - Flash
    - Virtual Memory
- Input/Output (I/O)
  - System Bus & Channels
    - System Bus
    - Data Bus
    - Control Bus
  - Storage
    - Magnetic
    - Optical
    - Solid State

CPU Protection Mode

- The unrestricted mode is often called **kernel** mode (aka supervisor mode, privileged mode, etc.).
  - the CPU may perform any operation, access any location in RAM, perform I/O operations, without restrictions
- Restricted mode is usually referred to as **user** mode or **problem state.** In this mode, the CPU is prevented (by other elements of the architecture) from performing any activity that may impact the security of a system

Memory

- Memory
  - ROM (Read Only Memory)
  - RAM (Random Access Memory)
    - SRAM (Static RAM)
      - Cache L1, L2, etc
    - DRAM (Dynamic RAM)
    - Flash
    - Virtual Memory (Swap or paging file located on permanent storage

Storage

- Temporary
  - RAM
- Permanent
  - Magnetic
  - Optical
  - Solid State

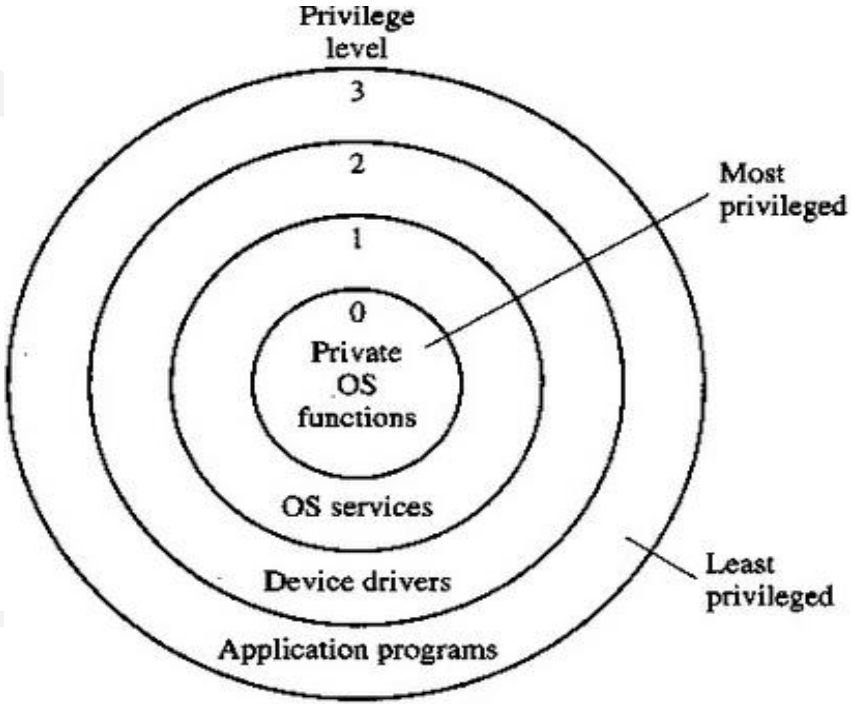
System Buses

- There are generally two buses within a computer. The first is the **internal bus** (sometimes called the **front-side bus**, or **FSB** for short). The internal bus allows the processor to communicate with the system's central memory (the RAM).
- The second is **the expansion bus** (sometimes called the **input/output bus**), which allows motherboard components (i.e. USB, serial, sound, NIC], cards inserted in expansion slots, hard drives, CD-ROM and CD-RW drives, etc.) to communicate with one another.

Software: Operating System Architecture

CPU Modes & Protection rings

- Protection Rings isolate layers of trust to ensure that competing processes do not affect each other or harm critical system components.
  - Ring 0 – Operating system kernel (supervisor /privilege mode)
  - Ring 1 – Remaining parts of the operating system (OS)
  - Ring 2 – Operating system and I/O drivers and OS utilities
  - Ring 3 – Applications (Programs) and user activity



Operating System Kernel

- The **reference monitor concept** defines the set of design requirements to make the determination regarding subject/object access. It provides the rules that govern access. Think: The law
- The **security kernel** are the actual components which enforce the rules of the reference monitor. Think: The police
- Three requirements for the reference monitor/security kernel
    - Must facilitate isolation of processes
    - Must be invoked at every access attempt.
    - Must be small enough to be tested and verified in a comprehensive manner.
- Security Policy – a set of rules on how resources are managed within a computer system.

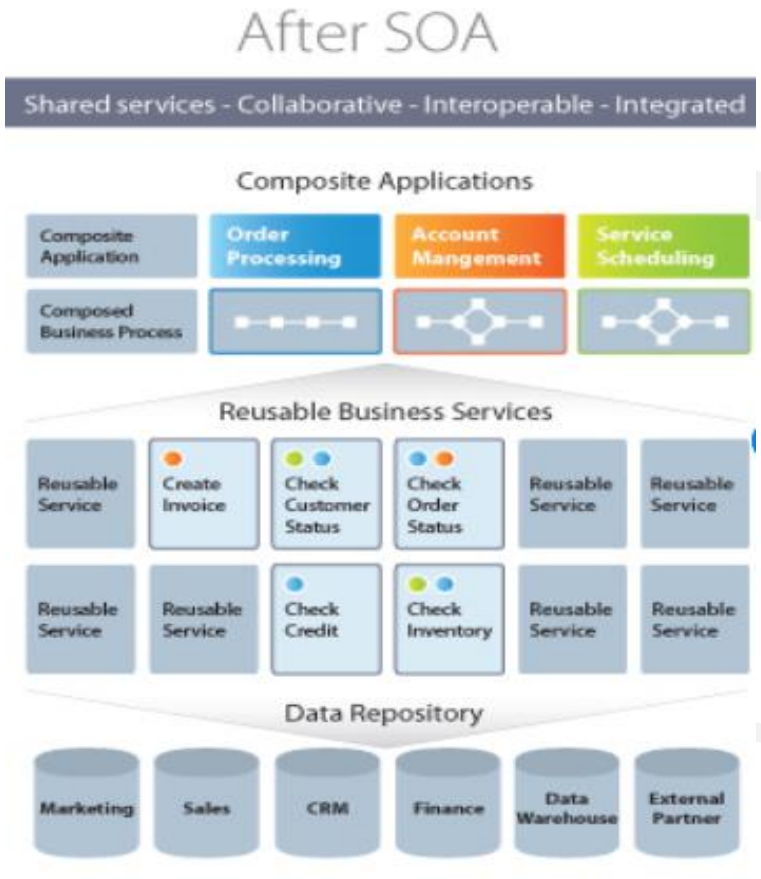
Programs, Processes, Threads

- Program: An Application
- Process: A program loaded into memory
- Thread: Each individual instruction within a process
- Multi-programming: Multiple programs “open” but no true isolation
- Multi-tasking: Isolation of processes—more than a single Process can run at one time
- Multi-processing – more than one CPU
- Multi-threading—in the past multiple CPUs were needed.
- Multi-core processors provide hardware multithreading

Software: Application Architecture

Software Architecture

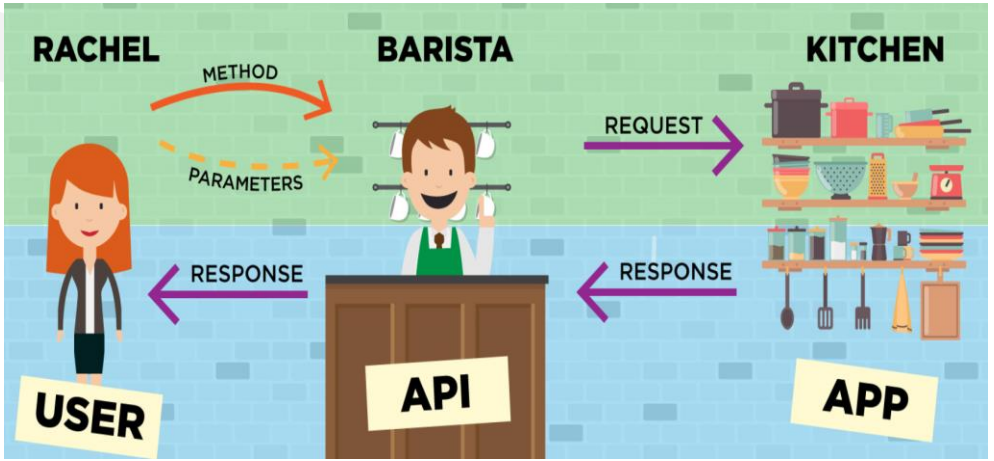
Web Services



- Web Services allow different applications to communicate with each other regardless of platform, programming language or operating system
- Web Services rely on standards-based APIs and Service Oriented Architecture

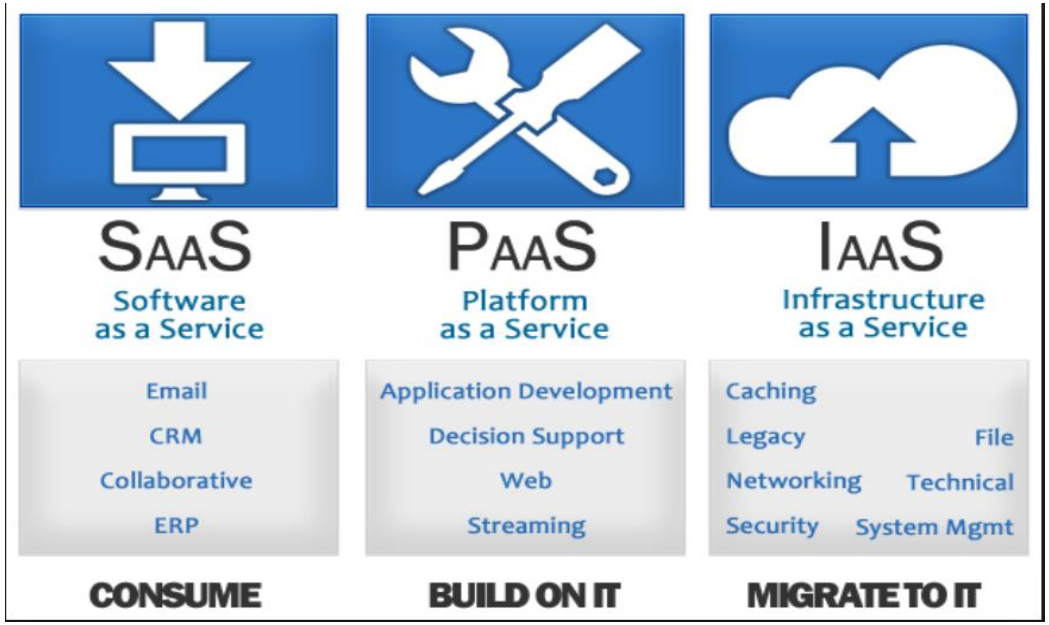
APIs

- Programing code that governs how a web service can request information or services. APIs define 3 primary elements:
- **Access**: who is allowed to ask for data or services.
- **Request**: what data or services can be asked for (e.g., if I give you an address can you tell me how to get there?). Requests have two main parts:
  - **Methods**: the type of questions you can ask, assuming you have access (it also defines the type of responses available).
  - **Parameters**: additional details you can include in the question or response.
- **Response**: the data or service for your request.



The map we left her and the fact that the coffee shop was open gave her **access** to the API.
When she got to the coffee shop, she had access to the menu with all the different options. She knew what you can ask for (**methods**) and the options and details (**parameters**). This told her how to place her **request** for food. Once Rachel placed her **request**, the barista played the role of the **API** and sent a message to the kitchen.
Rachel then just had to wait for the **response** in the form of food and beverage, which the barista, acting as the **API**, delivered to her with a smile (nice folks at The Grind).

Cloud Architecture



https://www.pinterest.com/backboneforbigd/sme/

Secure Modes of Operation

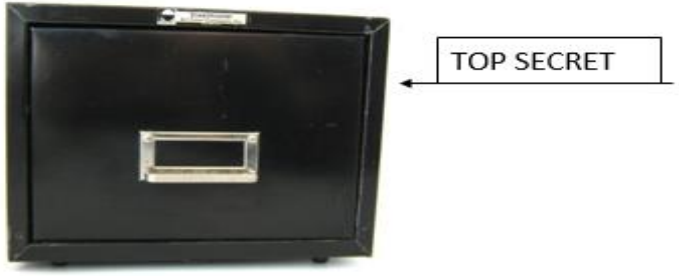
Secure Modes of Operation

- Single State
- Multi State
- Compartmented
- Dedicated

Single State

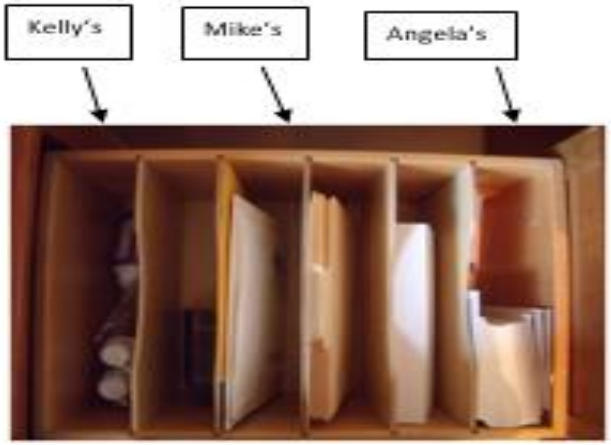
Multi-state

Single State: Clearance for everything on the system



Multi State : Clearance for what you will access

Compartmented



Dedicated

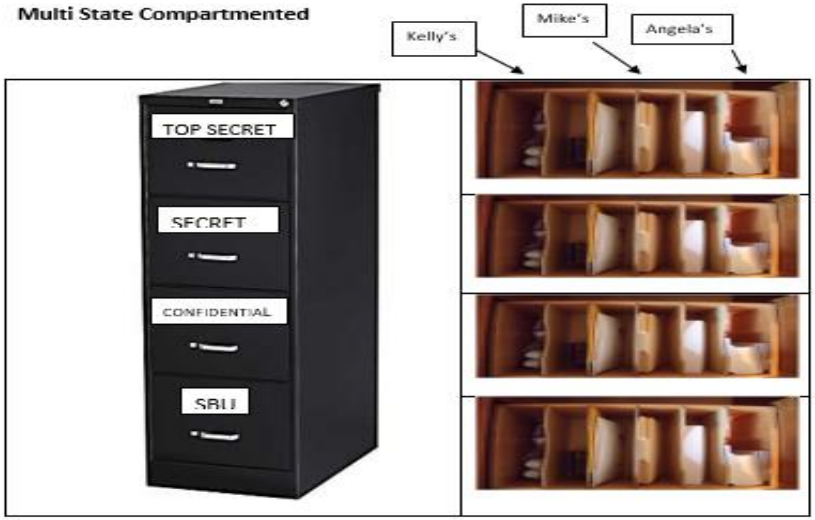
Single State Compartmented

Clearance for everything, need to know for what will be accessed

Single State Dedicated

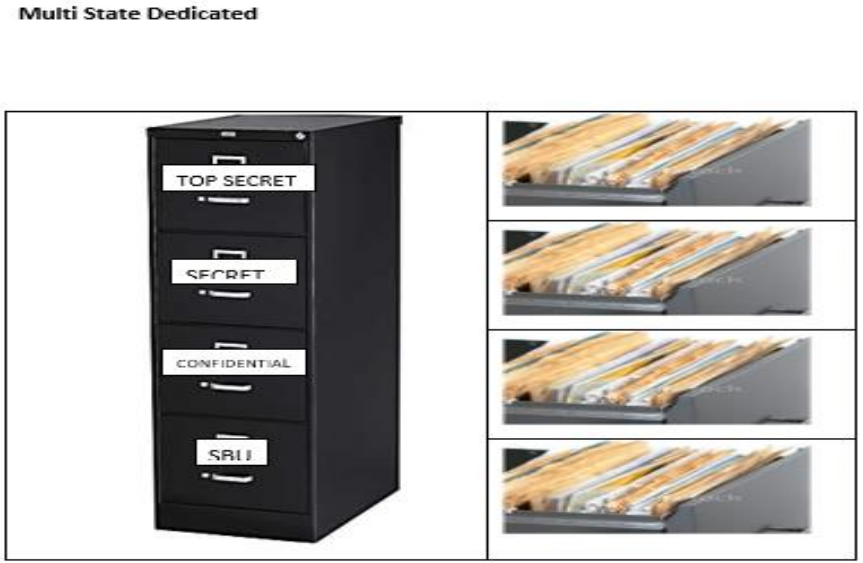
Clearance for everything, need to know for everything

Multi-State, Comparted



Clearance for what will be accessed, need to know for what will be accessed

Multi-State, Dedicated



Clearance for what will be accessed, need to know for what everything at that level

Certification and Accreditation

Evaluation Criteria

- Why Evaluate?
  - To carefully examine the security-related components of a system
  - Trust vs. Assurance
- CMMI
- The Orange Book (TCSEC)
- The Orange Book & the Rainbow Series
- ITSEC (Information Technology Security Evaluation Criteria)
- Common Criteria

Trusted Computer Security Evaluation Criteria (TCSEC)

- Developed by the National Computer Security Center (NCSC)
- Also known as the Orange Book
- Based on the Bell-LaPadulla model (deals with only confidentiality)
- Uses a hierarchically ordered series of evaluation classes
- Defines Trust and Assurance, but does not allow for them to be evaluated independently

TCSEC Evaluation

Trusted Computer Security Evaluation Criteria (TCSEC) aka “The Orange Book”

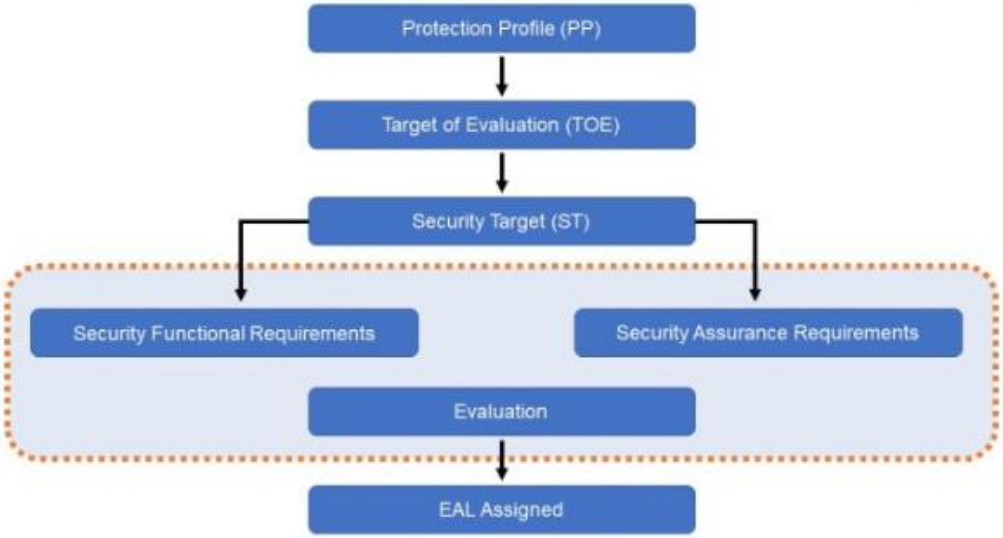
Ratings:

- A1 – Verified Protection
- B1, B2, B3 – Mandatory Protection
- C1, C2 – Discretionary Protection
- D – Minimal Security

IT Security Evaluation Criteria (ITSEC)

- Created by a collection of European nations in 1991 as a standard to evaluate security attributes of computer systems
- The First Criteria to evaluate functionality and assurance separately
- F1 toF10 rates for functionality
- E0 to E6 for assurance

Common Criteria ISO 15408



- Protection Profile: Requirements from Agency or Customer
- Target of evaluation: System Designed by Vendor
- Security target Documentation describing how ToE meets Protection Profile
- Evaluation Assurance Level (EAL 1-7) Describes the level to which ToE meets Protection Profile

Common Criteria EAL Ratings

- EAL 1 – Functionally tested
- EAL 2 – Structurally tested
- EAL 3 – Methodically tested and checked
- EAL 4 – Methodically designed, tested, and reviewed
- EAL 5 – Semi formally designed and tested
- EAL 6 – Semi-formally verified designed and tested
- EAL 7 – Formally verified designed and tested

Certification & Accreditation

- Certification:
  - A process that ensures systems and major applications adhere to formal and established security requirements that are well documented and authorized.
  - It is usually performed by a vendor.
- Accreditation:
  - A formal declaration by a Designated Accrediting Authority (DAA) that information systems are approved to operate at an acceptable level of risk based on the implementation of an approved set of technical, managerial, and procedural safeguards.

Domain 3 Part 2: Security Architecture and Design Review

- Security Models
- System Architecture
- The Trusted Computing Base
- Hardware Architecture
- Software: Operating System Architecture
- Software: Application Architecture
- Secure Modes of Operation
- Certification and Accreditation

Domain 4

Communications and Network Security

"This is Gloria, our Network Administrator, and next to her is Henry, the translator."

CartoonStock.com

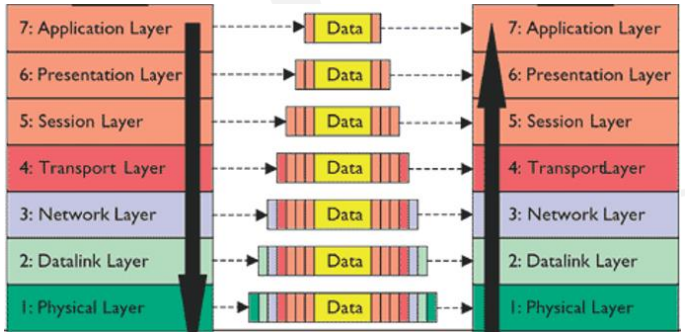
Communications and Network Security Agenda

- OSI Reference Model
  - Physical
  - Data Link
  - Network
  - Transport
  - Session
  - Presentation
  - Application
  - TCP/IP Model and OSI Review
- Security Zones and Firewalls
- Remote Access Protocols
- Tunneling
- Wireless Networking

The OSI Reference Model

What is the OSI Model and Why Do We Need It?

- Promotes interoperability between vendors
- Enables standardization
- Describes the encapsulation (Packaging) of data to enable it to get from point A to point B



Antoinet

Antionette is the CEO of OSI Inc. She works on the 7th floor. She needs to send a letter to Albert, an executive working at the 7th floor of their Manhattan branch office. She writes the letter's content, and then takes it down to Pasqual on the 6th Floor

Pasqual

Pasqual reviews the letter and makes sure that the spelling, grammar and other formatting issues are correct. He then takes the letter down to Sofia on the 5th floor.

Sofia

Sofia Calls the representative of Albert's company to verify that Albert is in the office and accepts incoming letters. Ensure we have the correct information for Albert. She then delivers the letter to Tamir on the 4th floor

Tamir

Tamir enters the subject matter of the letter in the "re:" field, so that Albert will know the general purpose of the letter. Tamir then puts the letter in an envelope and requests a read receipt on the message so he can ensure that the letter was received. On his way out of the office he drops the letter at Naheem's desk on the 3rd floor.

Naheem

Naheem determines the street address for Albert's branch, and uses his GPS to determine the fastest and most efficient path for the message to travel. He jots that info on the envelope and hands the letter to Darrell on the second floor

Darrell

Darrell calls to find out on which floor and suite number Albert works. He adds that information to the envelope. Darrell goes down to the first floor and asks if Pauline would mine delivering the message.

Pauline

Pauline puts the letter in her vehicle and drives to Albert's location. When she arrives, she meets Peter at the Manhattan Office and hands him the envelope.

Albert receives the letter from Antoinette and views the content.

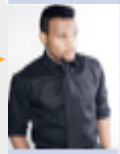
Paul ensures the letter is easy to read and in the format Albert prefers. He delivers the letter to Albert who is able to view the content.

Shalicia calls Sofia from the main office and asks that she stay on the phone line while Albert reads the letter. She transfers the call to Albert letting him know the letter is on his way and to pick up his extension. In walking the letter upstairs she runs in to Paul on the 6th floor.

Tom Completes the read receipt to acknowledge the letter was delivered. He circles the "re: field" so that Albert will know the general type of letter he is receiving. Tom climbs the steps to Shalicia on the 4th floor.

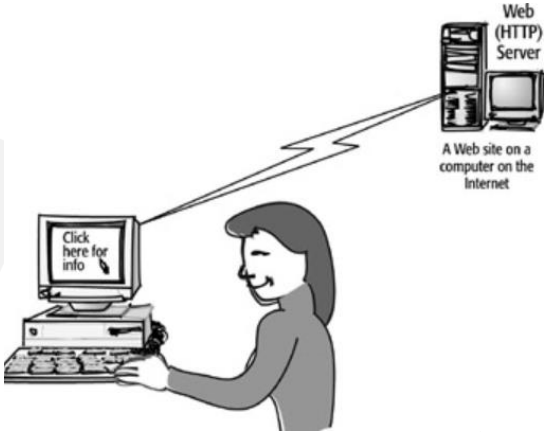
Nadia removes the envelope and passes the letter and read receipt up to Tom on Floor 4.

Dae copies the floor and suite number from the envelope to the actual letter and then delivers it to Nadia on the 3rd floor..

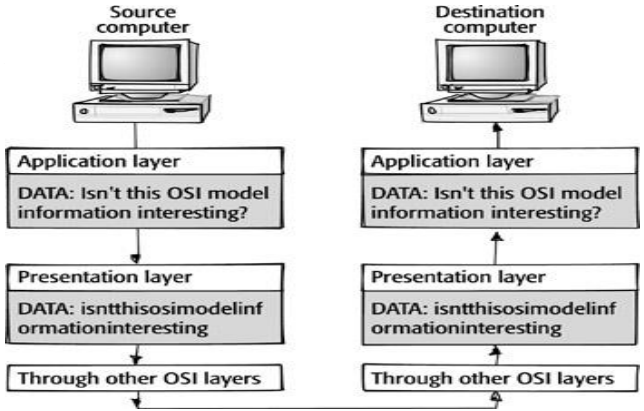


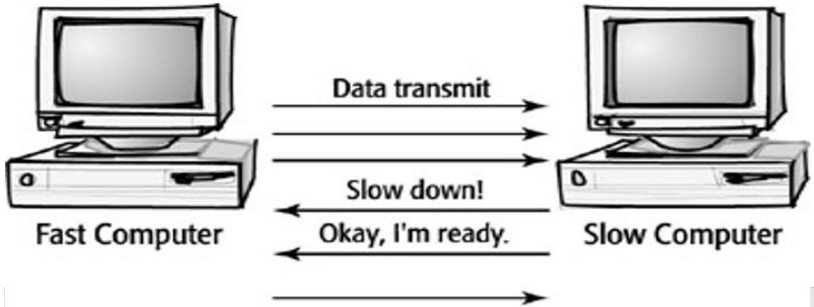
Peter takes the letter from Pauline's car and brings it up to Dae on the 2nd floor.

7. Application Layer



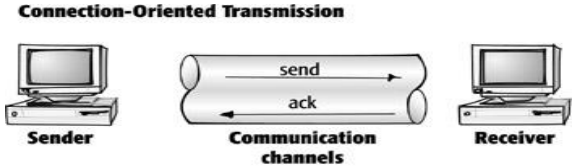
6. Presentation Layer

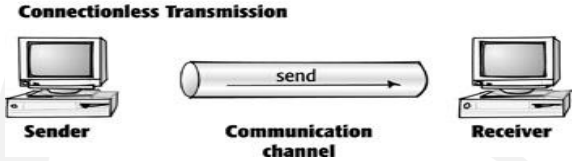




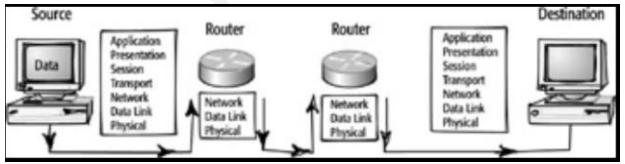
5. Session Layer

4. Transport Layer

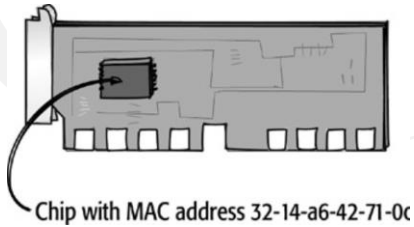




3. Network Layer



2. Data Link Layer



Physical Layer

1. Physical Layer

Data and the OSI

Layer	OSI Layer	Functions/Mechanisms
7	Application	Protocols that support the applications for users. HTTP, HTTPS, SMTP, POP3 Telnet, FTP, TFTP, NTP, NNTP, SNMP, and others
6	Presentation	Formatting of message and multimedia formatting. GIF, JPEG, MP4, etc.
5	Session	Headers are added to data for application-to-application communication (client-server.) RPC, SQL, LDAP Identification of communication streams
4	Transport	Headers are added for acknowledgements and flow control. Port numbers added.. Data has now become a segment. TCP, UDP, SSL, TLS
3	Network	Logical addressing and best path determination information is added to a segment, which now has become a packet. IP, ICMP, IPSec, IGRP Routers
2	Data Link	Packet is delivered to layer 2 where MAC Addressing, Media Access Determination, Framing information are added. The packet is now a frame. ARP, RARP, Ethernet, Token Passing. Switches
1	Physical Layer	Data placed on media. Wiring standards and protocols. Cable types, hubs. Frames are now converted to signal to traverse the physical media.

Layer	OSI Layer	Functions/Mechanisms
7	Application	Reads the application layer protocol commands (such as, http) and display accordingly thru the user application
6	Presentation	Interprets and formats the information correctly
5	Session	Appropriate service is used to access data (based on port numbers) Then session information is used to id the appropriate data stream
4	Transport	Segments assembled, acknowledgements sent. Port number is used to determine which service is needed. The data is passed upwards to layer 5
3	Network	Removes the IP header of the Packet and passes the data on so that Transport layer information can be accessed by Layer 4. Data becomes a Segment after Network layer information is removed
2	Data Link	Data Link headers including MAC addresses, etc are removed and the frame is converted to a packet
1	Physical Layer	Physical signal is received and translated into bits. Bits are translated into frames and sent to Data Link Layer

OSI Model – Layer 1 Physical

Layer 1 Physical – simply put is concerned with physical connectivity and sending electric signals over a medium.

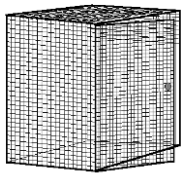
- All hardware devices have a point of connection, therefore at least partially have a layer 1 element

HUB

Layer 1 (Physical) Threats

Threats:

- Theft
- Unauthorized Access
- Vandalism
- Sniffing
- Interference
- Data Emanation



Faraday cage

Data Link Layer

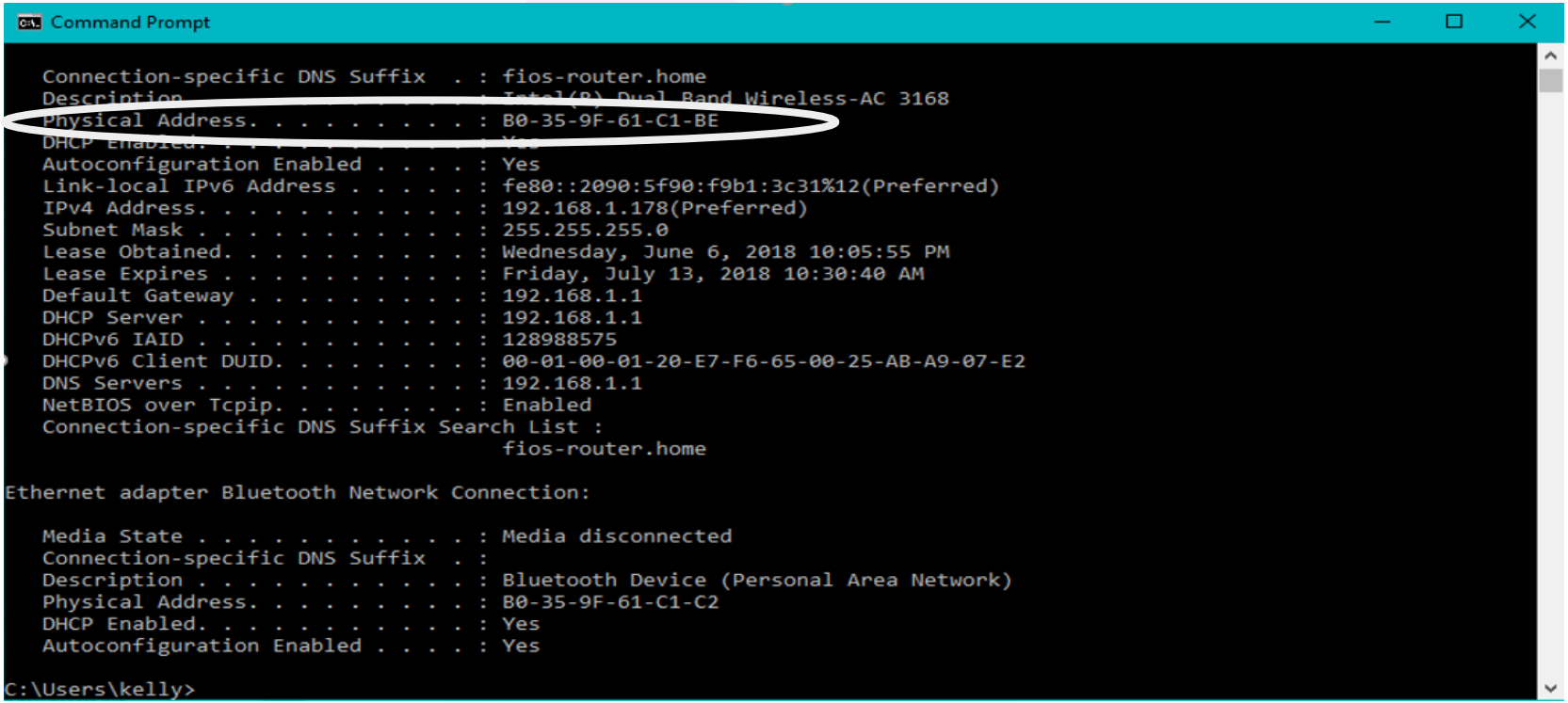
OSI model – Layer 2 Data Link

- Data Link Layer
- Only Layer of the OSI Model with 2 Sub-layers
  - LLC Logical Link Control—error detection
  - MAC Media Access Control—Physical
    - CSMA/CD Carrier Sense Multiple Access with Collision Detection (IEEE standard) 802.3 Ethernet
    - CSMA/CA Carrier Sense Multiple Access with Collision Avoidance(IEEE standard) 802.11 Wireless
    - Token Passing: 24 bit control frame passed around the network environment with the purpose of determining which system can transmit data. There is only one token and since a system can't communicate without the token, there are no collisions.

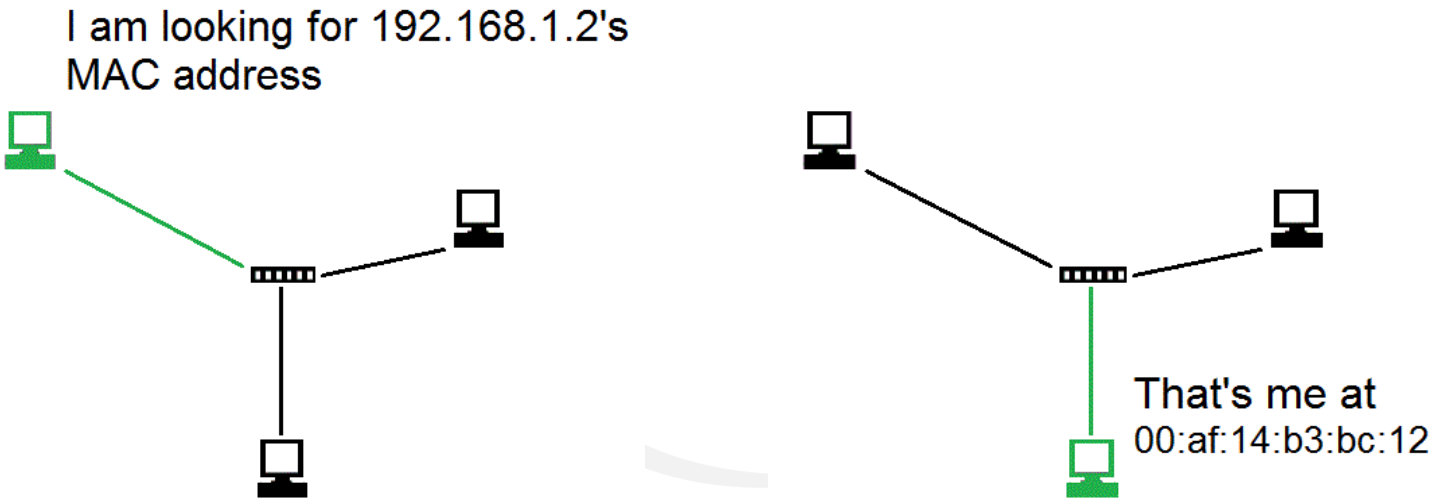
Ethernet

- Carrier Sense Multiple Access with Collision Avoidance
- Used by ethernet
- Contention (or collision based)
- Multiple systems *can* access the network, but data will collide
- Collisions slow things down!
- Ethernet requires the resolution of an IP address to a MAC address

MAC Addresses

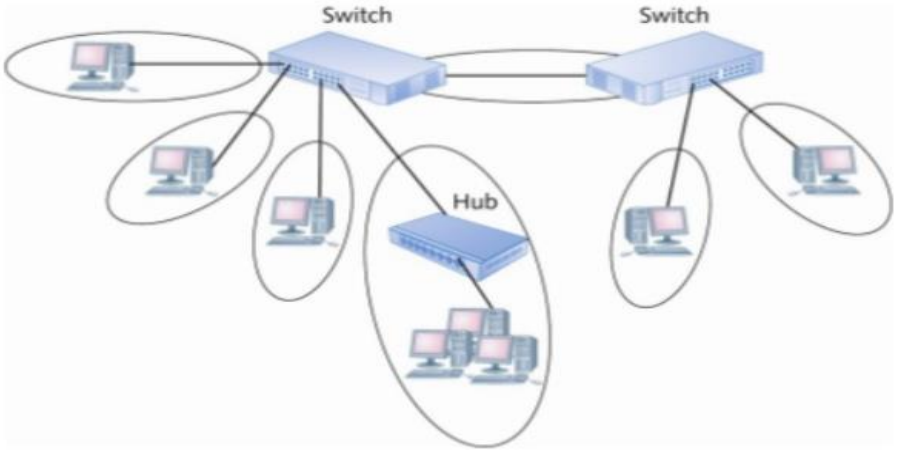


ARP



Switch

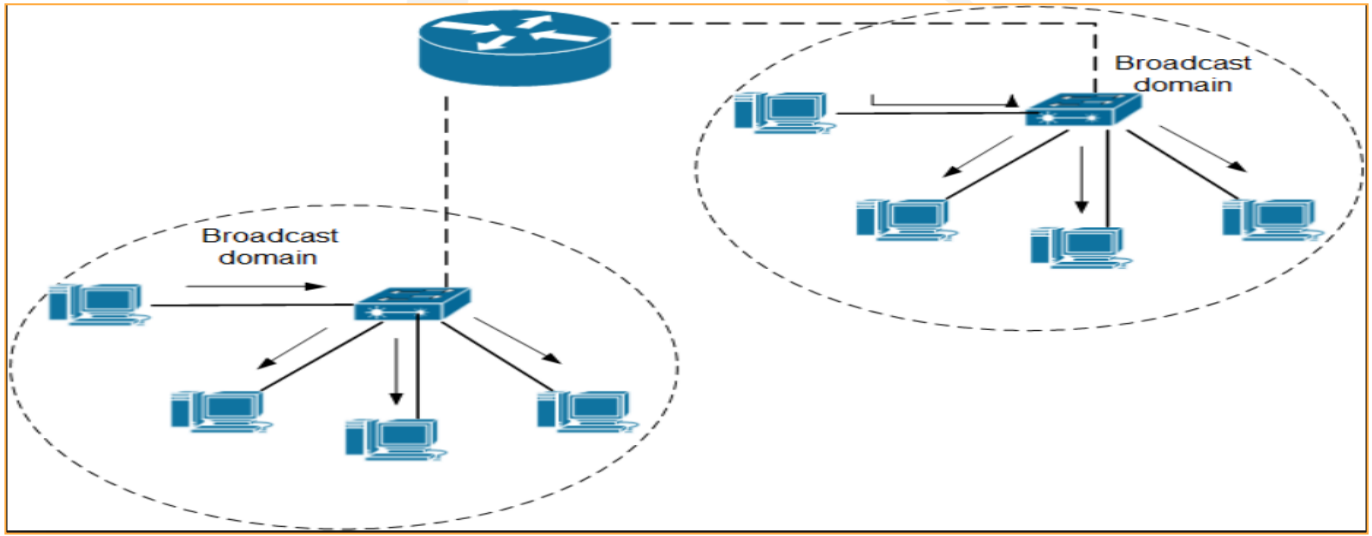
- By default, switches operate at layer 2
- Uses MAC addresses to direct traffic
- Isolates traffic into collision domains
- Does NOT isolate broadcasts natively



Network Layer

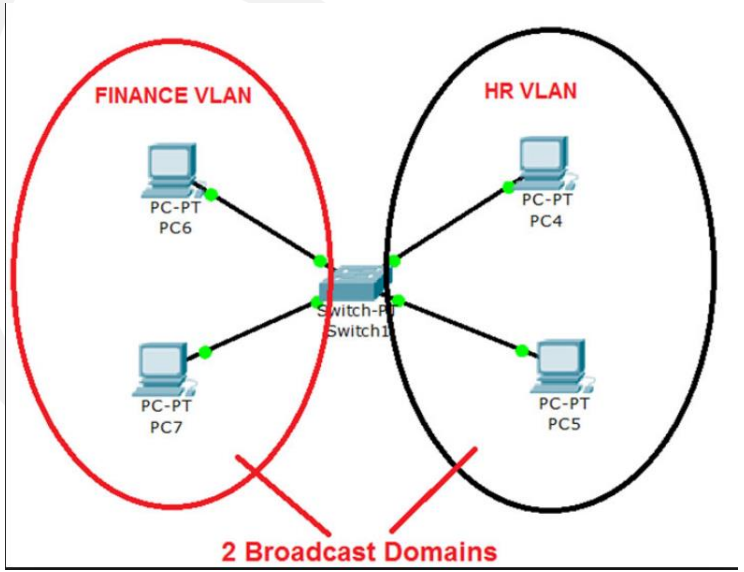
OSI model layer 3 network

- Routers Isolate traffic into broadcast domains and use IP addressing to direct traffic



VLANs

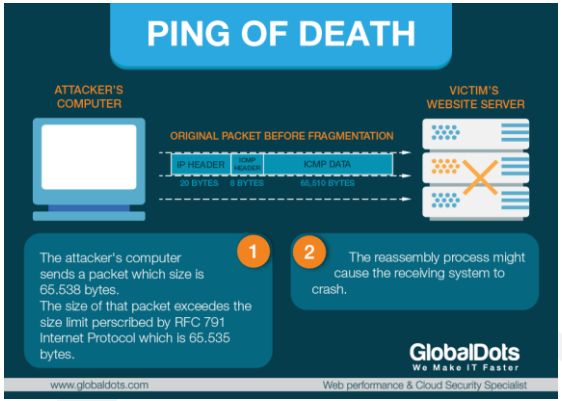
- Routers are expensive
- To get broadcast isolation on a switch, a VLAN is necessary
- Not all switches support VLANs
- A Layer 2 switch (even with a VLAN) doesn't truly understand Layer 3 IP Addressing
- A Layer 3 switch is necessary for inter-Vlan Communication



Layer 3 Protocols

- All Protocols that start with the letter “I” except IMAP (which is a layer 7 mail protocol)
- IP
- ICMP – IP “helpers” (like ping)
- IGMP – Internet Group Message Protocol
- IGRP
- IPSEC
- IKE
- ISAKMP

ICMP



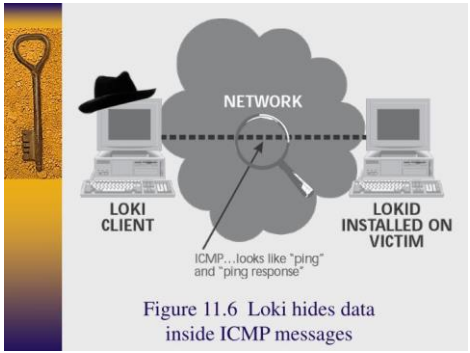
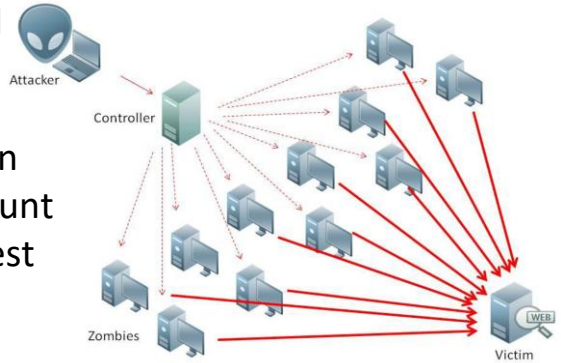
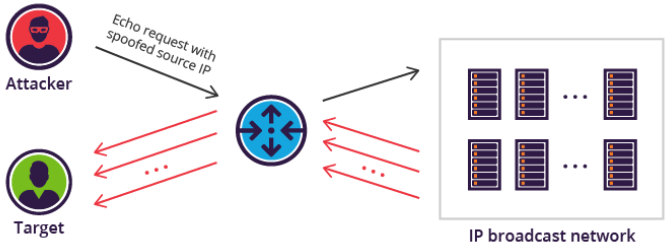


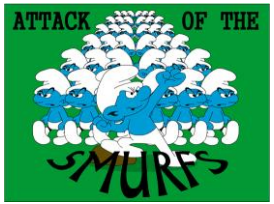
Figure 11.6 Loki hides data inside ICMP messages



Ping Flood: Sends an overwhelming amount of ICMP echo request packets



SMURF: Uses a spoofed source address (Target) and directed broadcasts to launch a DDos



Transport Layer

OSI model Layer 4 Transport

OSI Layer 4 Transport – Provides **end-to-end data transport services** and establishes a logical connection between 2 computers systems"

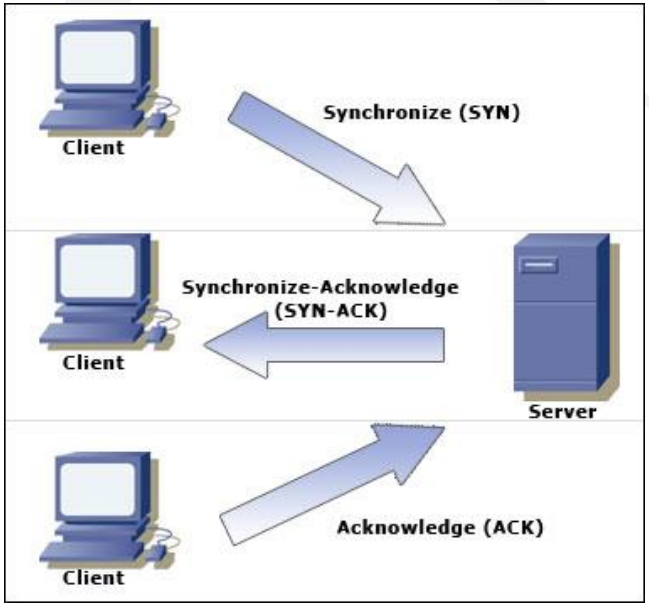
- The "pony express"
- Protocols used at layer 4
  - SSL/TLS (Discussed in Cryptography Domain)
  - TCP
  - UDP

TCP (Transmission Control Protocol)

- Connection oriented “guaranteed” delivery.
- Advantages
  - Easier to program with
  - Truly implements a session
  - Adds security
- Disadvantages
  - More overhead / slower
  - SYN Floods

TCP

A reliable, connection-oriented protocol, which uses the three way handshake as seen below



UDP (User Datagram Protocol)

- Connectionless
- Unreliable
- No handshaking
- Desirable when “real time” transfer is essential
  - Media Streaming, Gaming, live time chat, etc
  - FTP uses TCP
  - TFTP uses UDP

Best Joke Ever…..

What’s the best thing about a UDP Joke???

I don’t care if you get it or not!

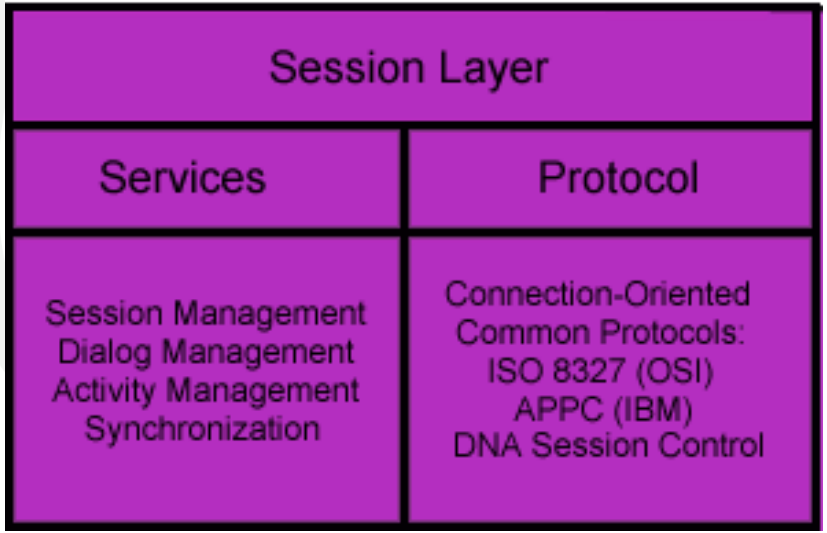
Session Layer

OSI Model Layer 5 Session

OSI Layer 5 (Session) – responsible for establishing a connection between two applications (either on the same computer or two different computers)

Dialogue control

Release connection



Presentation Layer

OSI model Layer 6 Presentation

Present the data in a format that all computers can understand

This is the only layer of OSI that does NOT have any protocols.

- Concerned with encryption, compression and formatting
- Making sure data is presented in a universal format
- File level encryption
- Removing redundancy from files (compression)

Application Layer

OSI model Layer 7 – Application

This defines a protocol (way of sending data) that two different programs or applications understand.

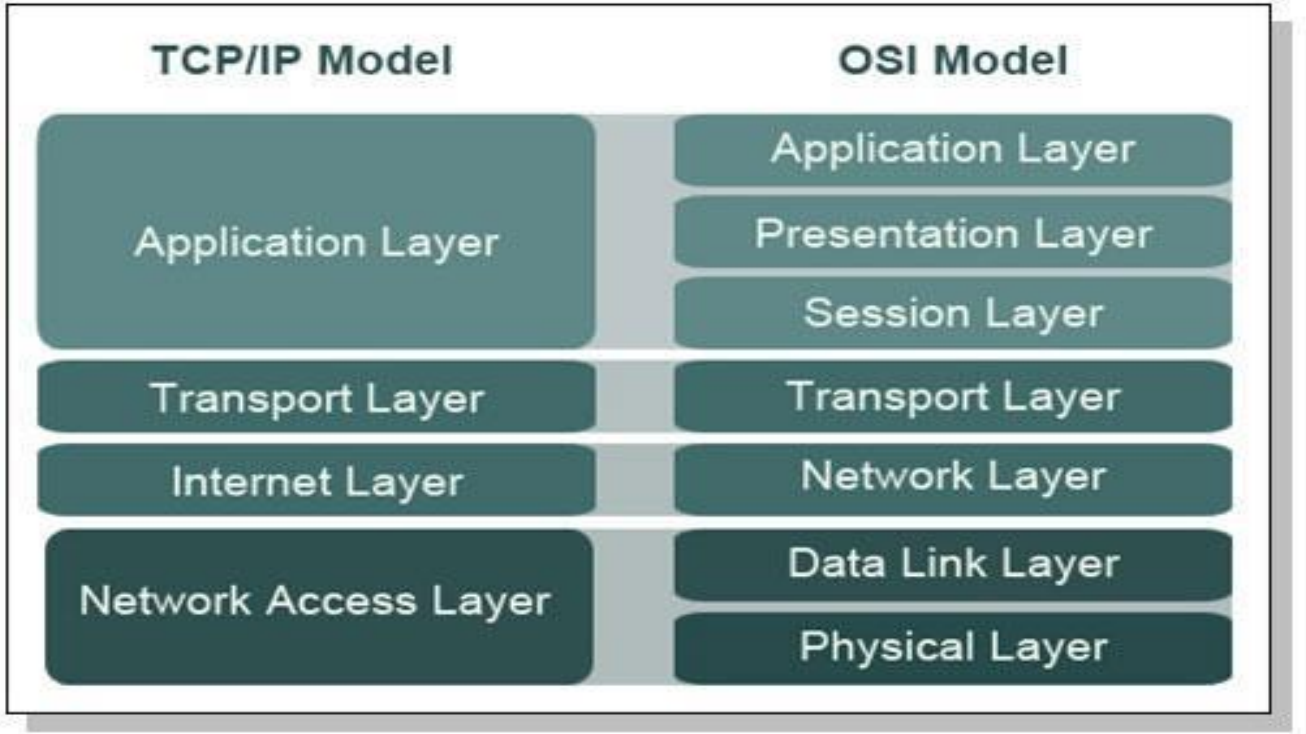
- HTTP, HTTPS, FTP, TFTP, SMTP, SNMP, etc.
- Application Proxies
- Non-Repudiation
- Certificates
- Integration with Directory Services
- Time awareness---NTP Network Time Protocol—Controls synchronization of time on systems---Kerberos, digital forensics, and many other services require time synchronization.

I was going to tell you an NTP joke but…

My timing is always off

TCP Model and OSI Review

OSI vs. TCP/IP model



OSI/TCP…What you need to know

#	OSI Model	Key Responsibilities	Data Type	Info	Firewall	Common Protocols and Technologie	TCP/IP Model
7	**Application**	User Application Services	User Data	**GATEWAYS** (Exam) Smartest Layer / Content Layer / Certs / Non-Repudiation / Mail API - Application Program Interface	Kernel Proxy FW - Very Fast Hardware (GEN 5)	FTP; TFTP; SSH; IMAP; POP; HTTP; HTTPS	**Application**
6	**Presentation**	Data Translation; Compression and Encryption	Data	File Level Formatting; Encryption & Compression		EFS (Encryption File System)	
5	**Session**	Session Establishment, Management and Termination	Data	Application to Application	Stateful FW - Inspects, understands traffic. It allows protocols as long as it behaves like it should (GEN 3)	SQL; RPC (DNS is Layer 5 for the Exam)	
4	**Transport**	End-to-End Connections; Segmentation and Reassembly;	Segment	**(Syn Flood)** **(Fraggle - exploits UDP)**		TCP and UDP SSL / TLS	**Transport** **Host-to-Host**
3	**Network**	Logical Addressing; Routing (Path Determination); Datagram Encapsulation; Error Handling and Diagnostics	Packets / Datagrams	**Router** (Isolates Broadcast Traffic) Logical Addressing (IPSec for Security) **(PING Floods /Ping of Death / Loki)** **(Smurf Attack-spoof source address)**	Static / Stateless FW - Very limited / All or nothing - FW blocks or allows entire Protocol (GEN 1)	IP; IPv6; IP NAT; IPsec; ICMP; RIP; BGP	**Internet**
2	**Data Link**	Logical Link Control; Media Access Control (MAC); Data Framing; Addressing; Error Detection	Frames	**Switch** (Doesn't address Broadcast Traffic), **MAC, Ethernet, NIC** **Tunneling - Encapsulation (L2TP gives you the tunnel / IPSec gives you the Security)**		IEEE 802.2 LLC; Ethernet; Token Ring; FDDI and CDDI; IEEE 802.11 (WLAN, Wi-Fi); PPTP; L2TP	**Network Access**
1	**Physical**	Encoding and Signaling; Physical Data Transmission; Hardware Specifications; Topology and Design	Bits	Cable, Hub, Modem (No Addressing)		(Physical layers of most of the technologies listed for the data link layer)	

OSI - Open System Interconnect - Created by ISO / Job - Promoting Interoperability among vendors (standardization among the layers)

Security Zones and Firewalls

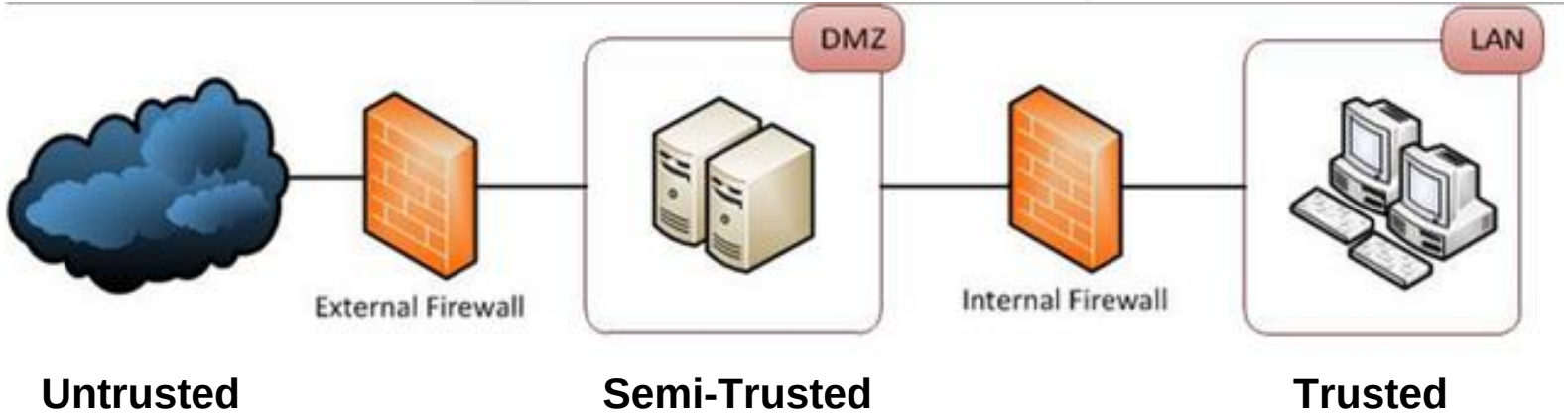
Security Zones

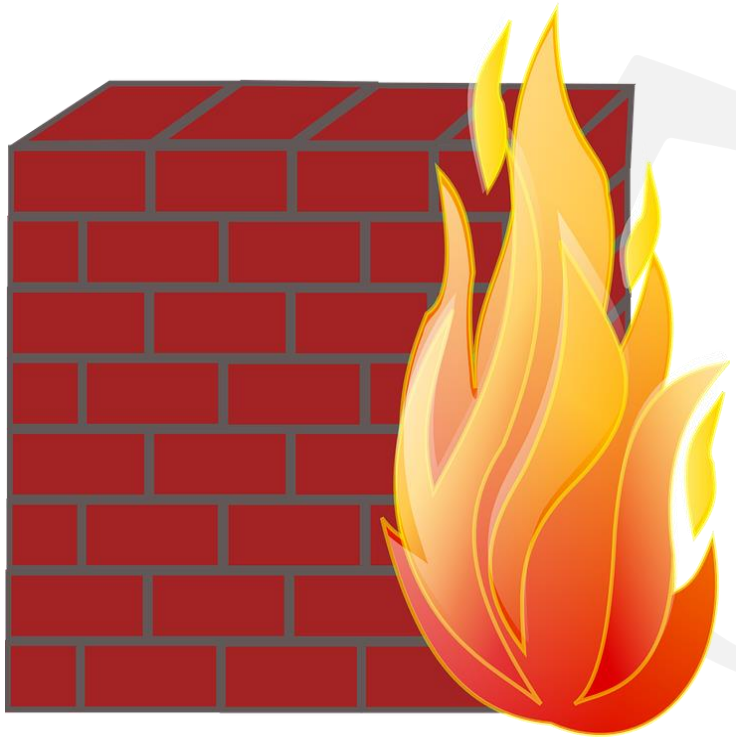
It is common practice in network and physical security to group different security levels into different areas or zones. Each zone is either more or less trusted then the other zones. Interfaces between zones have some type of access control to restrict movement between zones (like biometric and guard stations) or firewalls.) In Network security there is often a median zone between the Internet and internal network called a DMZ.

DMZ

A buffer zone between an unprotected network and a protected network that allows for the monitoring and regulation of traffic between the two.

- Internet accessible servers (*bastion hosts*) are placed in a DMZ between the Internet and Internal network





Firewalls

- Designed to provide filtering between Trust Zones
- Software or Hardware Based
- Provide isolation and separation
- Create zones based on trust
- Used Rule-based access control

Firewalls and the OSI Model

- Layer 3 (Network Layer)
  - Packet Filtering
  - Screening Routers
  - Inspect Layer 3 & Layer 4 Headers
    - Source and Destination IP
    - Source and Destination Port
    - Protocol (TCP or UDP)

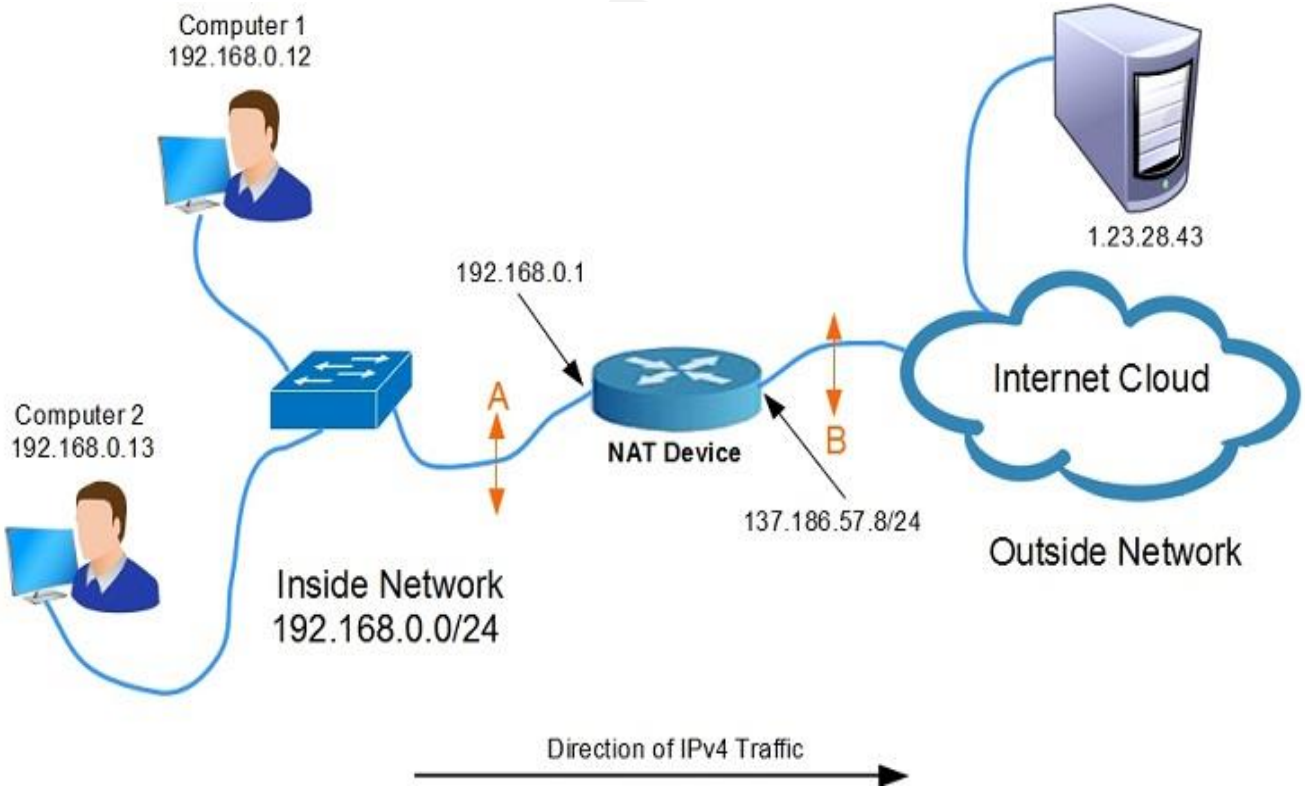
Firewalls and the OSI Model

- Layer 5 (Session Layer)
- Stateful Filtering
  - Awareness of the initiation of the session and the state
  - Can block unsolicited replies
  - Can understand syntax of lower layer protocols and can block “misbehaving” traffic

Firewalls and the OSI Model

- Layer 7 (Application Layer)
  - Called Application Proxies/Firewalls
  - Deep Packet Inspection
  - Forward Proxy inspects traffic from inside going out
  - Reverse Proxy inspects traffic from outside going in
  - Can inspect on content, time, application-awareness, certificates, etc.
  - Specific to the application protocol

NAT/PAT



NAT / PAT

- Advantages
  - Allows you to use private addresses Internally, you don’t need to get real public IP addresses for each computer
  - Allows the use of RFC 1918 IP addresses
    - 10.x.x.x
    - 172.6.x.x-172.31.x.x
    - 192.168.x.x
  - Hides internal network structure
  - Transparent, doesn’t require special software
- Disadvantages
  - Single Point of Failure / Performance Bottleneck
  - Doesn’t protect from bad content

Overall Firewall best practices

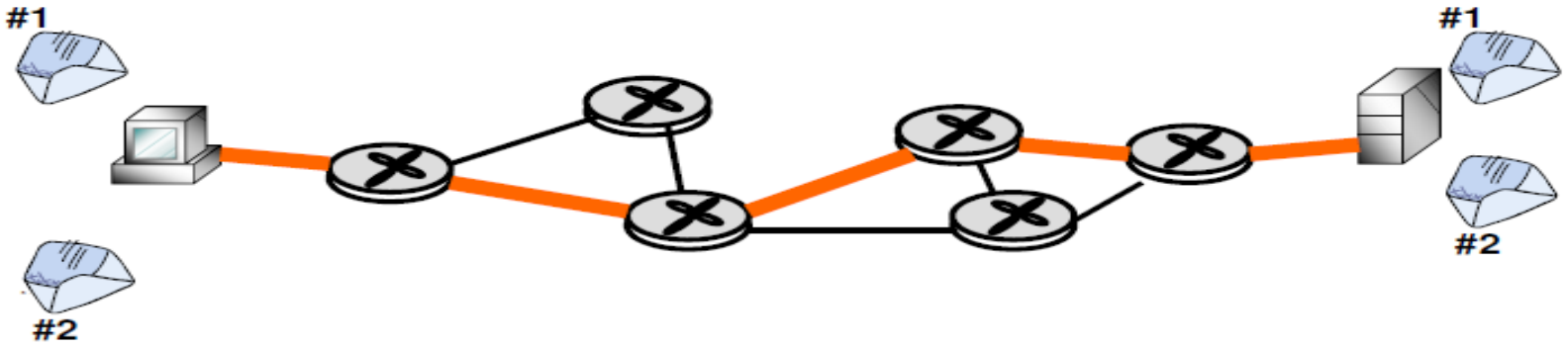
- Block un-necessary ICMP packets types.
  - (Be careful though, know your environment)
- Keep ACLS simple
- Use *Implicit deny**
- Block *directed IP* broadcasts
- Perform *ingress and egress filtering**
  - Block traffic leaving the network from a non-internal address (indicates the network is possibly being used as zombie systems ina possible DDoS attack.
  - Block all traffic entering the network from an internal address (indicates a potential spoofing attack)
- Enable logging
- Drop fragments or re-assemble fragments

WAN Technology

LAN, WAN

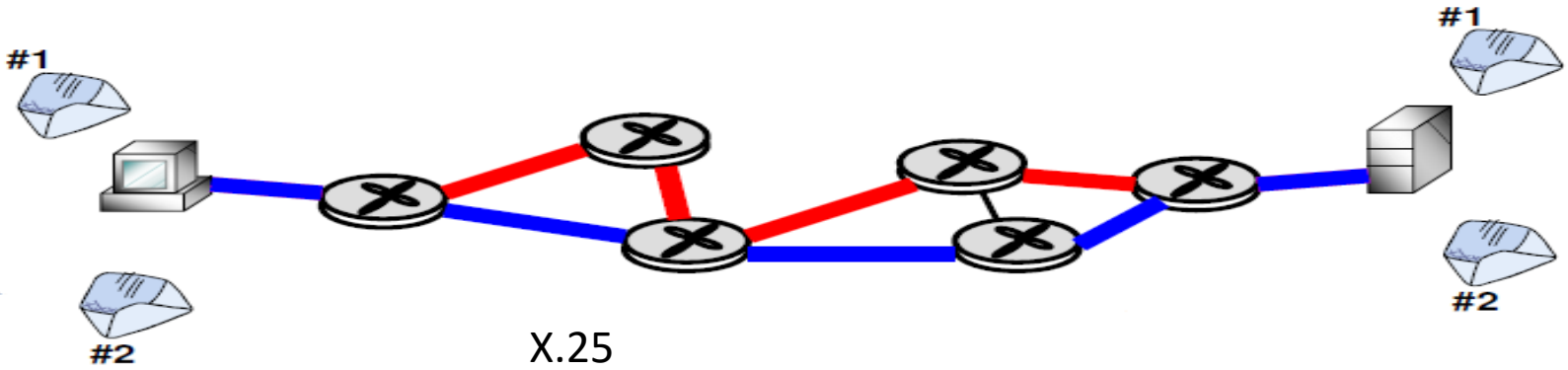
- LAN – local area network
  - High speed
  - Small physical area
- WAN – wide area network
  - Used to connect LANS
  - Generally slow, using serial links

Circuit Switching



- PSTN
- ISDN
- DSL
- T-carriers

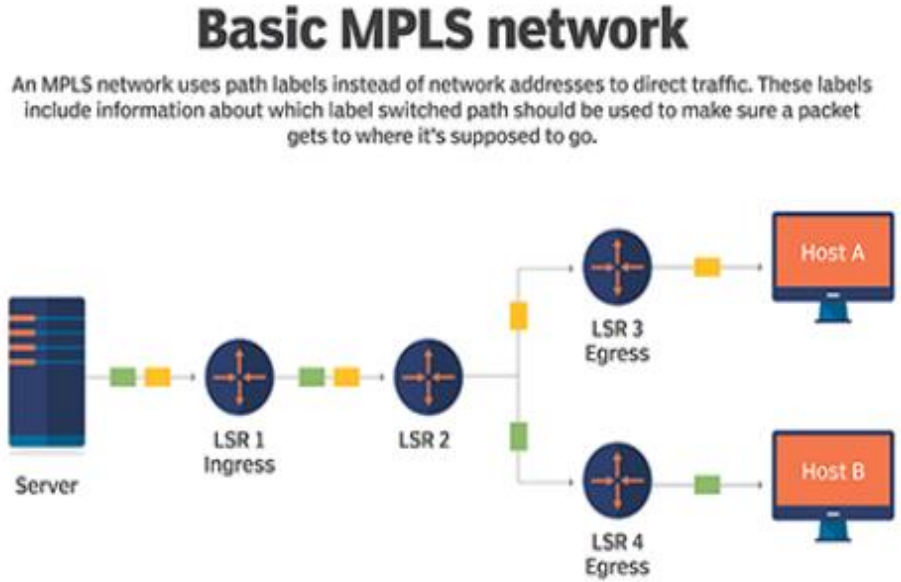
Packet Switching



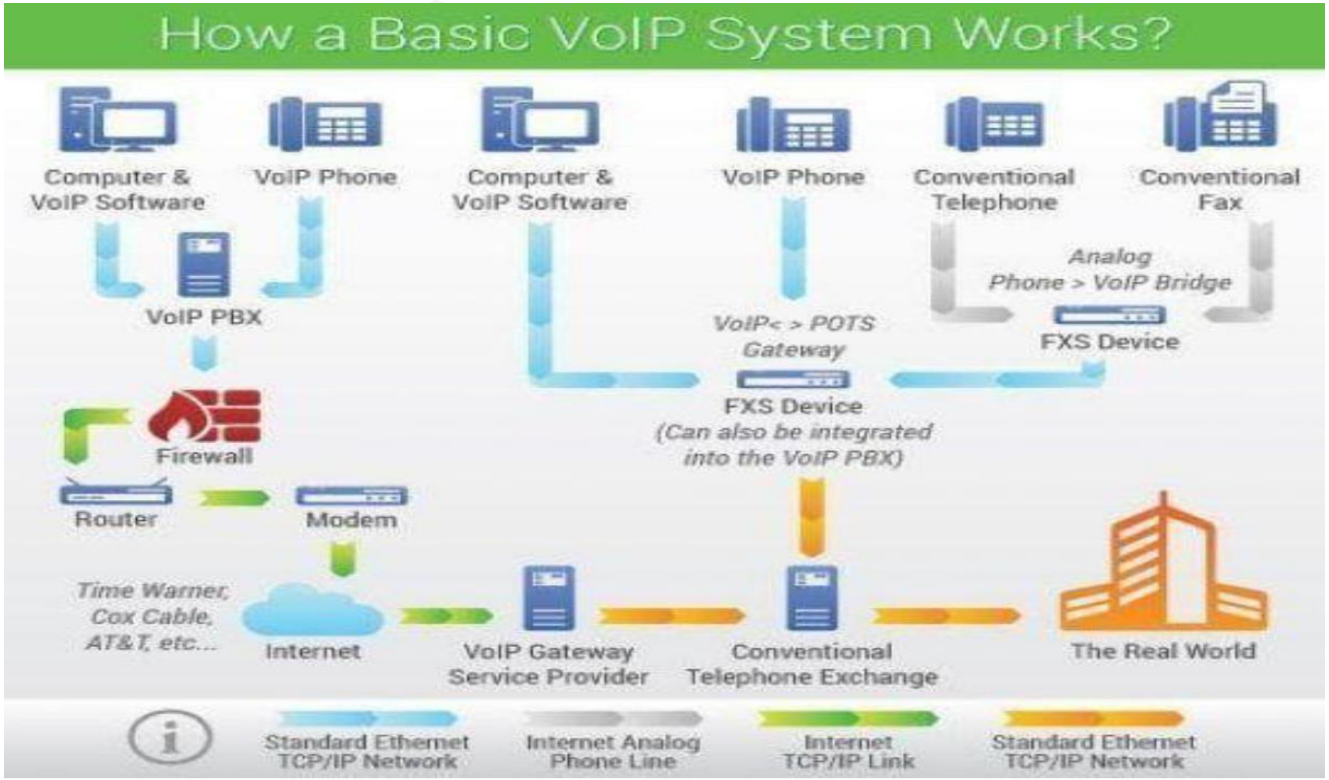
X.25
Frame Relay
ATM
IP Networks
VOIP
MPLS
Cable

MPLS (Multi Protocol Labeled Switching)

In an MPLS network, each packet gets labeled on entry into the service provider's network by the ingress router, also known as the label edge router (LER). This is also the router that decides the LSP the packet will take until it reaches its destination address.
All the subsequent label-switching routers (LSRs) perform packet forwarding based only on those MPLS labels -- they never look as far as the IP header. Finally, the egress router removes the labels and forwards the original IP packet toward its final destination.



VOIP Voice Over IP



VOIP Security Issues

- Eavesdropping (greatest threat)—Enable S/RTP
- Toll Fraud
- Vishing
- SPIT

Performance Issues

- Latency
- Jittering

Remote Access Protocols

Remote Access

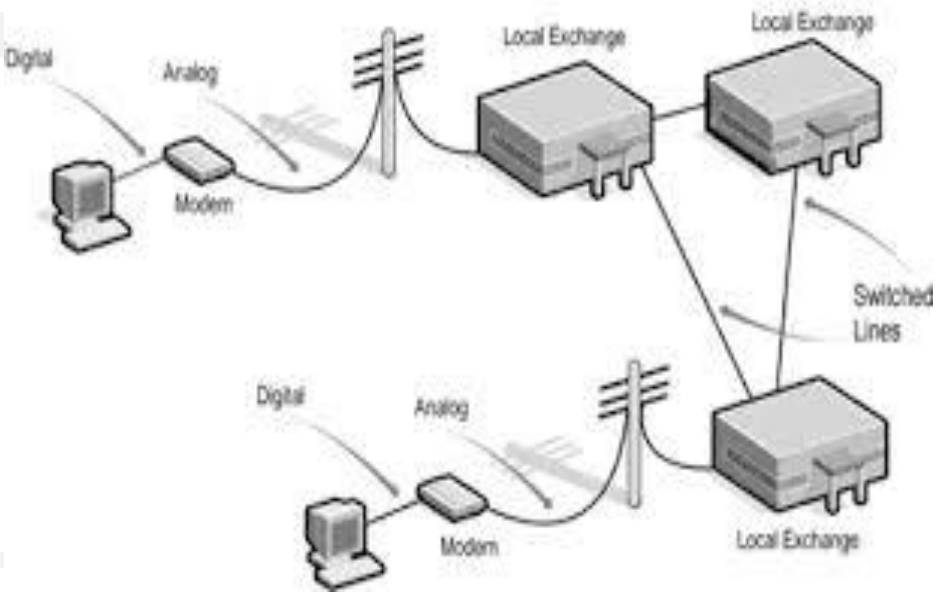
- Dial Up
  - PPP
    - PAP, CHAP EAP
- Tunneling
  - PPTP
    - PAP, CHAP EAP
    - MPPE
  - GRE
  - L2TP
    - IPSEC
  - IPSEC

- Wireless
  - Encryption
    - WEP, WPA, WPA II
- Authentication

  - 802.1x

Dial-up

- PPP Point to Point Protocol: Provides Layer 2 framing for dial-up. Needs other protocols for security
  - Encryption: MPPE
  - Authentication:
    - PAP (Password Authentication Protocol): Clear Text
    - CHAP (Challenge Handshake Authentication Protocol) Client responds to a challenge from the server. The only way the client can answer correctly is if the correct password had been entered.
    - EAP (Extensible Authentication Protocol) Extends capabilities beyond passwords (smart cards, biometrics, token devices, etc)

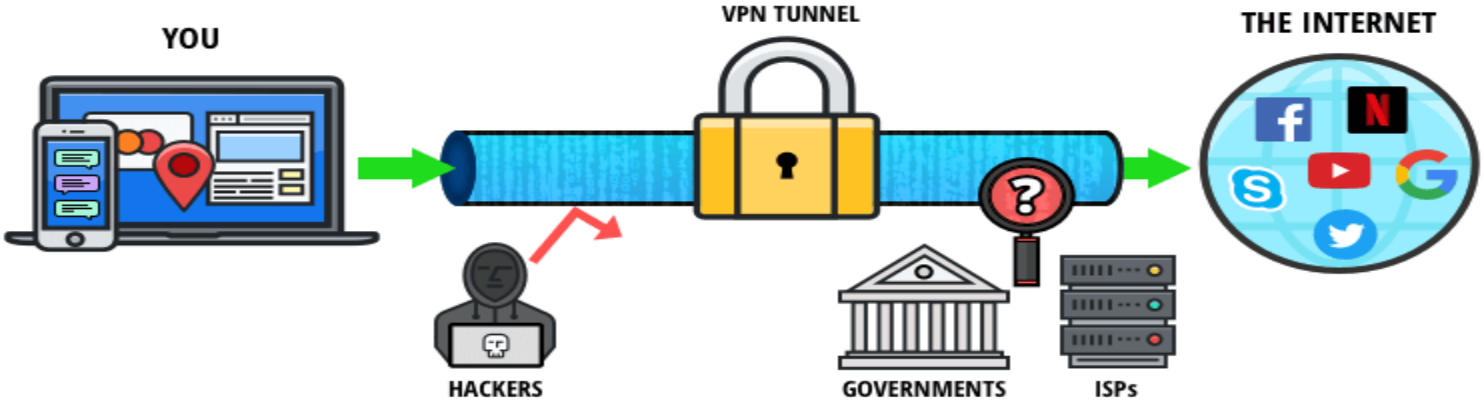


Tunneling

Tunneling

A function of VPNs - Tunnel encapsulates one protocol within another creating a virtual network.

- Can encrypt original IP headers
- Can encrypts data
- Allows for routing non routable protocols and IP addresses
- Can provide remote/internal IP addresses



Tunneling protocols

Different protocols

- PPTP
- L2TP
- IPSEC
- GRE

PPTP

Point to Point Tunneling Protocol

Based on PPP (uses MPPE for encryption and PAP, CHAP or EAP for authentication)

- Lead by Microsoft protocol for a tunneling VPN
- Only works across IP networks
- Remote user connects to ISP, gets an Internet Address
- Establishes VPN connection to work VPN server, get's Internal IP address.
- Sends private IP packets encrypted within other IP packets.

L2TP

Layer 2 Tunneling Protocol

- Cisco designed L2F to break free of dependence on IP networks, but kept it proprietary.
- L2TP was a combination of L2F and PPTP
- Designed to be implemented in software solutions
- THERE IS NO SECURITY with L2TP. It MUST use IPSec to secure

Generic Routing Encapsulation (GRE)

Point to point link between two networks. It adds an extra IP header to the original packet. Much more frequently used in the past to encapsulate AppleTalk, IPX and other older protocols.

- **Data encapsulation** – GRE tunnels encapsulate packets that allow protocols to traverse an incompatible network. For example, to route IPv4 packets across a network that only uses IPv6.
- **Simplicity** – GRE tunnels lack mechanisms related to flow-control and security by default. This lack of features can ease the configuration process. However, you probably don't want to transfer data in an unencrypted form across a public network; therefore, GRE tunnels can be supplemented by the IPSec suite of protocols for security purposes. In addition, GRE tunnels can forward data from non-contiguous networks through a single tunnel, which is something VPNs cannot do.
- **Multicast traffic forwarding** – GRE tunnels can be used to forward multicast traffic, whereas a VPN cannot. Because of this, multicast traffic such as advertisements sent by routing protocols can be easily transferred between remote sites when using a GRE tunnel.

Wireless Networking

Wireless Networking

- **Mobility** – A wireless communications system allows users to conduct business from anywhere without
- **Reachability** – Wireless communication systems enable people to be stay connected and be reachable, regardless of their location.
- **Simplicity** – Wireless communication system are easy and fast to deploy in comparison of cabled network. Caution: Ease of use is often the enemy of security!
- **Maintainability** – In a wireless system, you do not have to spend too much cost and time to maintain the network setup.
- **Roaming Services** – Using a wireless network system, you can provide service any where any time including train, buses, airplanes etc.
- **Additional Services** – Wireless communication systems provide various smart services like SMS and MMS

Wireless security problems

- Unauthorized access
- sniffing
- War driving
- Unauthorized access points (Man in the middle)

Wireless Security

- Encryption
  - WEP
    - Shared authentication passwords
    - Weak IV (24 bits)
    - IV transmitted in clear text
    - RC-4 (stream cipher)
    - Easily crackable
    - Only option for 802.11b
  - WPA
    - Stronger IV
    - Introduced TKIP
    - Still used RC-4
  - WPA2
    - AES
    - CCMP
    - NOT backwards compatible
- Authentication
  - WPA and WPA2 Enterprise Uses 802.1X authentication to have individual passwords for individual users (RADIUS)

Bluetooth

Bluetooth is a Personal Area Network protocol designed to free devices from physical wires.

- Bluetooth Modes
  - Discovery Mode
  - Automatic Pairing

Blue jacking
Sending SPAM to nearby bluetooth devices
Blue Snarfing
Copies information off of remote devices
Blue bugging
More serious
Allows full use of phone
Allows one to make calls
Can eavesdrop on calls

Communications and Network Security Review

- OSI Reference Model
  - Physical
  - Data Link
  - Network
  - Transport
  - Session
  - Presentation
  - Application
  - TCP/IP Model and OSI Review
- Security Zones and Firewalls
- Remote Access Protocols
- Tunneling
- Wireless Networking

I don't care if this security software was a bargain; it shouldn't reply with "close enough" when I enter the wrong password.

CartoonStock.com

Domain 5

Identity and Access Management

Domain 5 Identity and Access Management Review

- Overview
- Identity Management
  - Identity Proofing
  - Account Provisioning/Deprovisioning
- Authentication
  - Type 1, Type 2, Type 3
  - Kerberos and Single Sign on
  - Single Sign on: Federated Services
- Authorization
- Access Control Models
- Enforcing Access Control
- Access Control Management
- Auditing/Accountability
- Data Emanation

Identity and Access Management

- Per ISC2, Identity and Access Management solutions “focus on harmonizing the provisioning of users and managing their access across multiple systems with different native access control systems”.
- Identity Management
  - Controls the life cycle for all accounts in a system
- Access Management
  - Controls the assignment of rights/privileges to those accounts

IAAA of Access Control

The components of Access Control that we are about to discuss are:

- Identification:
  - Make a claim (userid etc)
- Authentication:
  - Provide support (proof) for your claim
- Authorization:
  - What rights and permissions you have
- Auditing:
  - Accountability—matching actions to subjects

Identity Management

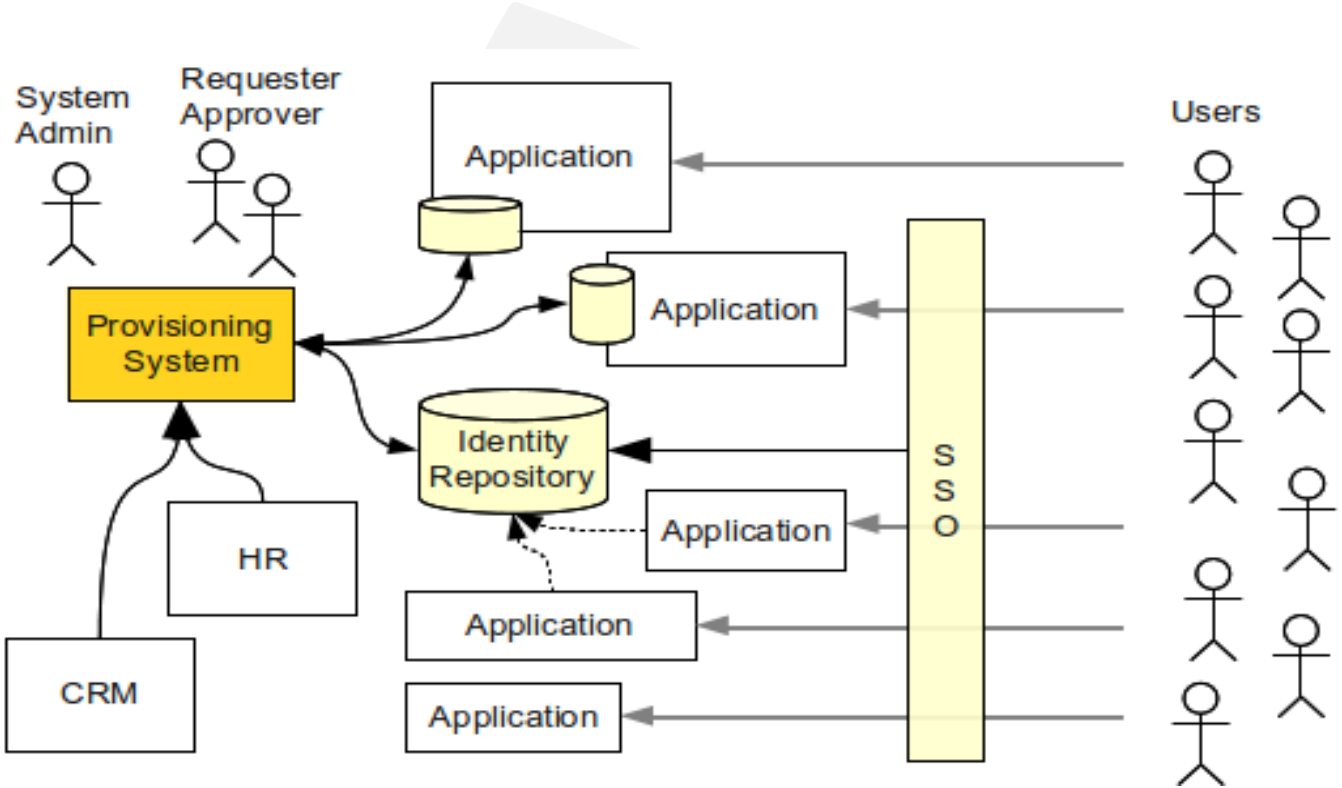
Identity Proofing

- Proceeds the creation of a user account
- Not the same as authentication
- Requires the prospective employee to prove their identity to the employer.
- Long before an employee is given a user account to identify with on the network, they have proven their identity to their employer

Account Provisioning

Account provisioning or identity provisioning technology creates, modifies, disables and deletes user accounts and their profiles across IT infrastructure and business applications.
Discretionary account provisioning: Administrators determine which applications and data a user should have access to
Self-Service account provisioning: users participate in some aspects of the provisioning process, thus reducing administrative overhead. Often, users are allowed to request an account and manage their passwords.
Workflow-based account provisioning - gathers the required approvals from the designated approvers before granting a user access to an application or data. For example, the business rules in a finance application might require that every new account request be approved by the company's Chief Financial Officer (CFO).
Automated account provisioning -- requires every account to be added the same way through an interface in a centralized managment application. This streamlines the process of adding and managing user credentials and provides administrators with the most accurate way to track who has access to specific applications and data sources.

Identity/Account Provisioning



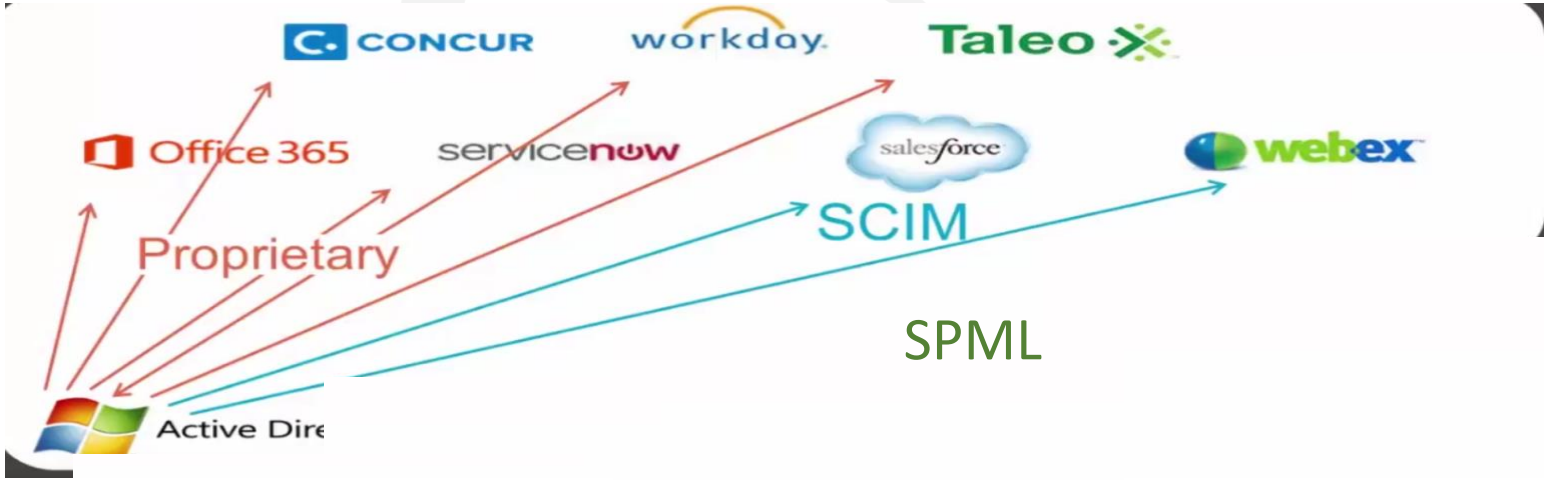
Identity Management: Provisioning/Deprovisioning

- Traditionally, different cloud vendors used non-standard provisioning APIs
- Enterprises to develop and maintain proprietary connectors to integrate with multiple SaaS providers
- Alternatively, Provisioning can be managed easier through
  - Service Provisioning Markup Language (SPML)
    - Older, seldom implemented due to the inflexibility and lack of vendor support
  - System for Cross-domain Identity Management…or…Simple Cloud Identity Management (SCIM)
    - Defines a Schema and an API for managing identities
    - System for Cross-domain Identity Management (SCIM) is an open standard for automating the exchange of user identity information between identity domains, or IT systems.

Traditional Identity Management in the Cloud

- Manual hand-entry
  - Error prone and slow
- Bulk upload
  - High latency – often a one-time operation
- Custom APIs and connectors
  - High cost to develop against
  - Proprietary to each service provider
- SAML Just-in-Time Provisioning
  - No pre-provisioning
  - No deprovisioning

Proprietary APIs, SPML and SCIM



System Identification

- Once an account has been provisioned, the first step a user undertakes to access a system is to provide identification
- Public Information (usually we aren't concerned with protecting identities)
- Identification **must** be unique for accountability
- Standard naming schemes should be used
- Identifier should not indicate extra information about user (like job position)
  - User ID
  - Account Number
  - RFID
  - IP or MAC address

Authentication

Authentication

Proving a claimed identity

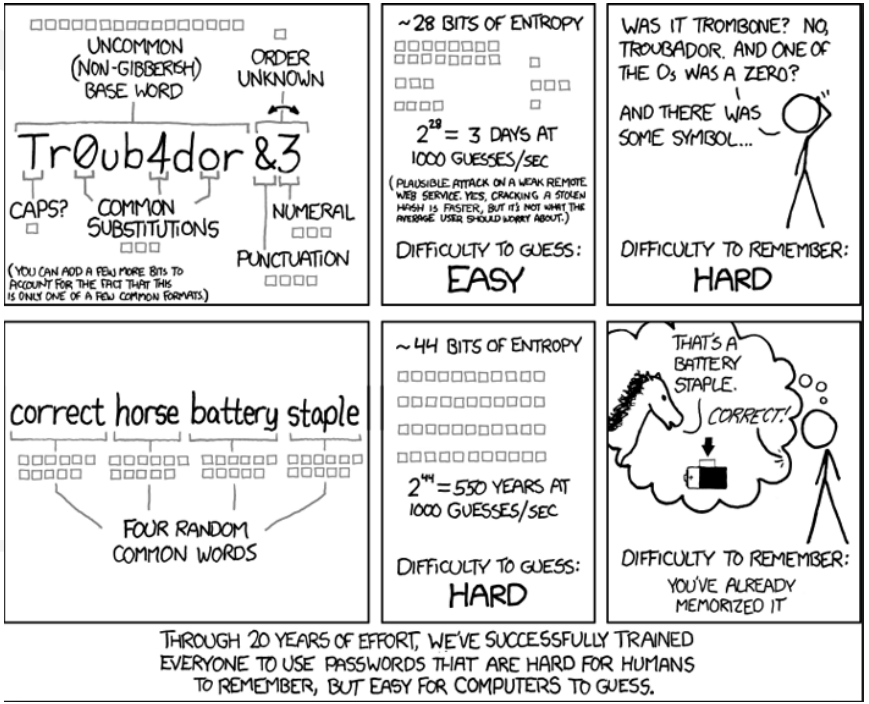
- Type 1: Something you know
- Type 2: Something you have
- Type 3: Something you are

- The Strongest authentication is multi-factor---a combination of the above
- Mutual Authentication is desirable as well

Type 1: Something You Know

Type 1: Something You Know

- Passwords/Passphrases/Cognitive Password
- Best practices
  - No less than 8 characters
  - Change on a regular basis
  - Enforce password history
  - Consider brute force and dictionary attacks
  - Ease of cracking cognitive passwords
  - Graphic Image
  - Enable clipping levels and respond accordingly



Type 2: Something You Have

Type 2: Something you have

- Token Devices
- Smart Card
- Memory Card
- Hardware Key
- Cryptographic Key
- Certificate
- Cookies

Token Devices: One Time Password Generators

Password that is used only once then no longer valid

- One time password reduces vulnerability associated with sniffing passwords.
- Simple device to implement
- Can be costly
- Users can lose or damage
- Two Types: Synchronous/Asynchronous

Token Devices

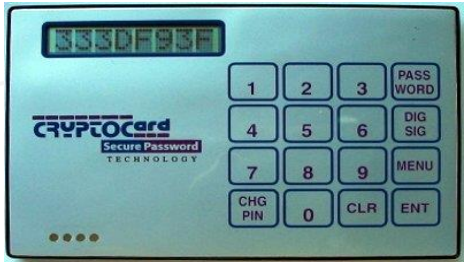
- Synchronous Token Devices
- Rely upon synchronizing with authentication server.

Frequently time based, but could be event based

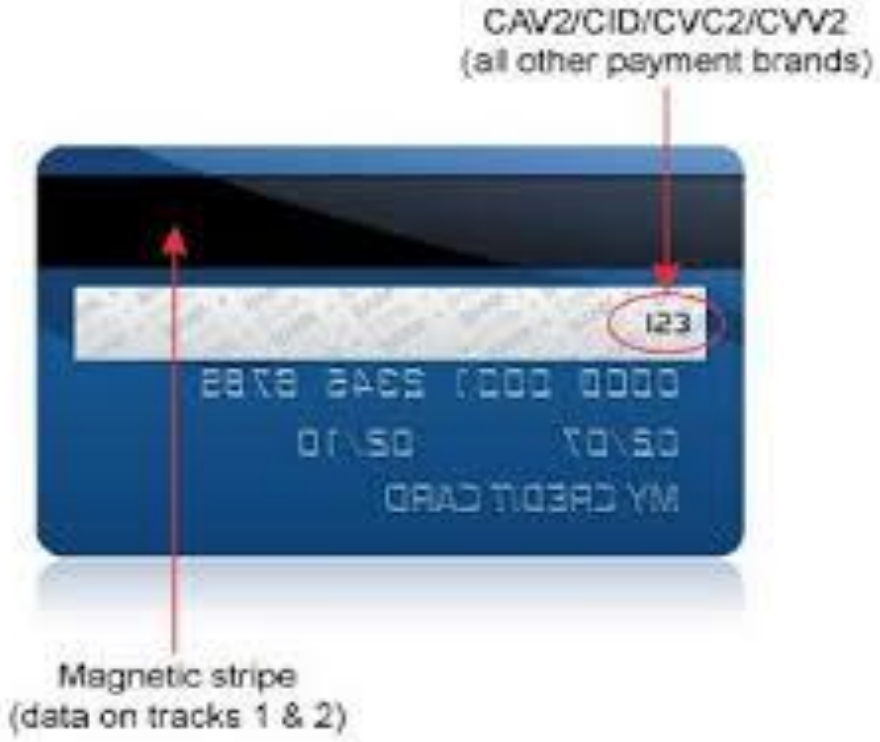
- If damaged, or battery fails, must be re-synchronized
- Authentication server knows what "password" to expect based on time or event.

Asynchronous/ Challenge Response

- User logs in
- Authentication returns a challenge to the user
- User types challenge string into token device and presses enter.
- Token device returns a reply
- Only that specific user's token device could respond with the expected reply.
- More Complex than synchronous
- May provide better protection against sniffing



Memory Cards



Memory Cards

- Holds information, does NOT process
- A memory card holds authentication info, usually you'll want to pair this with a PIN… WHY?
- A credit card or ATM card is a type of memory card, so is a key/swipe card
- Usually insecure, easily copied.*

Smart Card

EMV CHIP

EMV chip technology is becoming the global standard for credit card and debit card payments. Named after its original developers (Europay, MasterCard® and Visa®), this technology features payment instruments (cards, mobile phones, etc.) with embedded microprocessor **chips** that store and protect cardholder data.

Type 3: Something You Are/Do

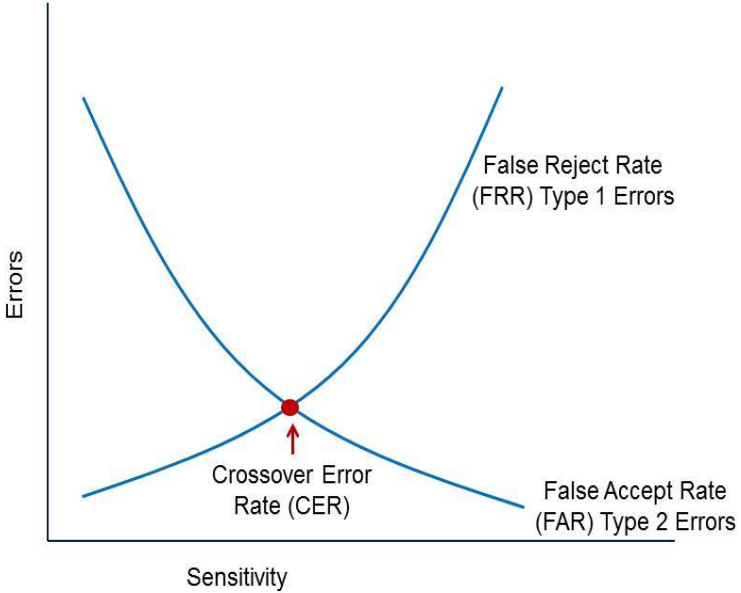
Type 3: Something You Are

- Biometrics
  - Physiological (Static): Should not significantly change over time. Bound to a user's physiological traits
    - Fingerprint, hand geometry, iris, retina, etc
  - Behavior-based (Dynamic): Based on behavioral traits
    - Voice, gait, signature, keyboard cadence, etc
    - Even though these can be modified temporarily, they are very difficult to modify for any significant length of time.

Crossover Error Rate

Accuracy

- Type I Error: False Rejection--A legitimate user is barred from access. Is caused when a system identifies too much information. This causes excessive overhead.
- Type II Error: False Acceptance—An impostor is allowed access. This is a security threat and comes when a system doesn't evaluate enough information
- As FRR goes down, FAR goes up and vice versa
- The level at which the two meet is called CER (Crossover Error Rate). The lower the number, the more accurate the system
- Iris Scans are the most accurate



Biometric Concerns

- User Acceptance
- Many users feel biometrics are intrusive
  - Retina scans can reveal health care information
- Time for enrollment and verification can make user's resistant
- Cost/benefit analysis
- No way to revoke biometrics

Kerberos and Single Sign On (SSO)

Single Sign On

Allows a user to provide credentials to an authentication server and receive accessed to interconnected and disparate systems.

Pros

- Ease of use for end users
- Centralized Control
- Ease of administration

Cons

- Single point of failure
- Standards necessary
- Keys to the kingdom

- Kerberos
- LDAP
- Sesame
- Krypto-Knight

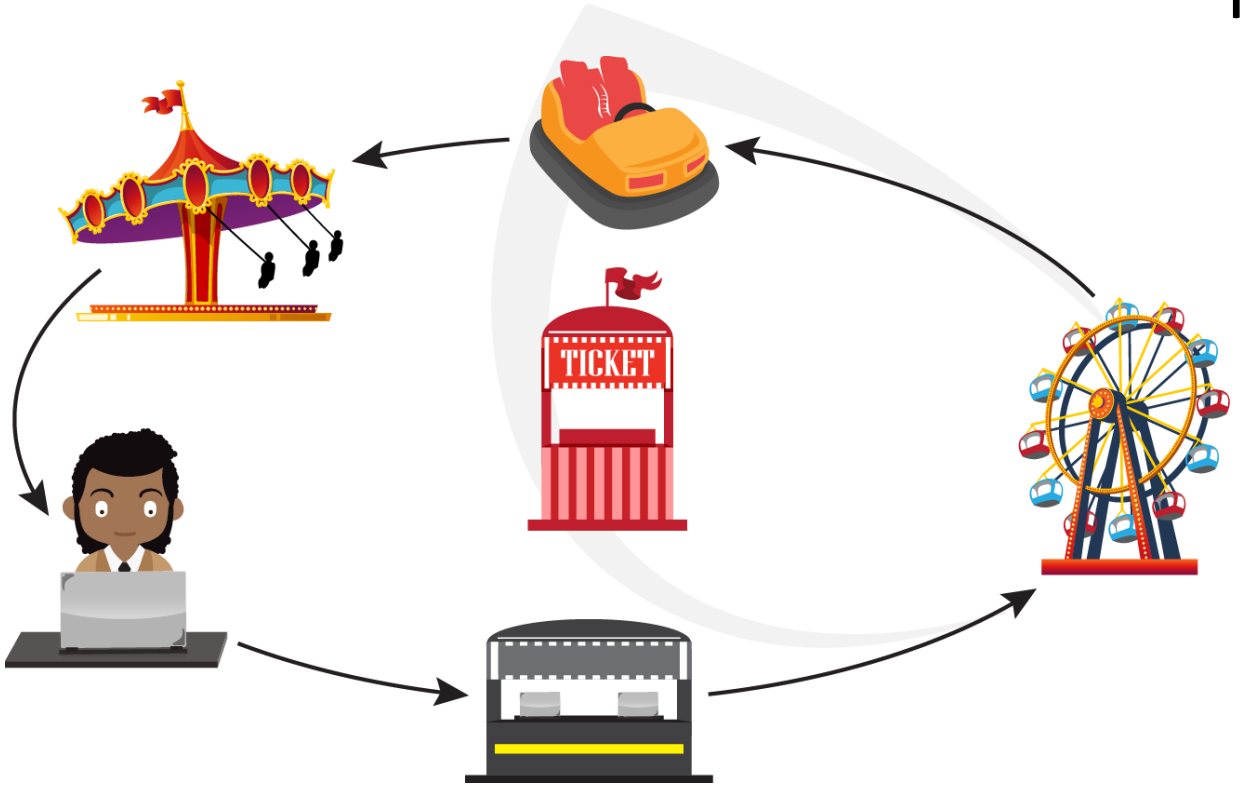
Kerberos

- A network authentication protocol designed from MITs project Athena. Kerberos tries to ensure authentication security in an insecure environment
- Used in Windows2000+ and some Unix
- Allows for single sign on
- Never transfers passwords
- Uses Symmetric encryption to verify Identifications
- Avoids replay attacks

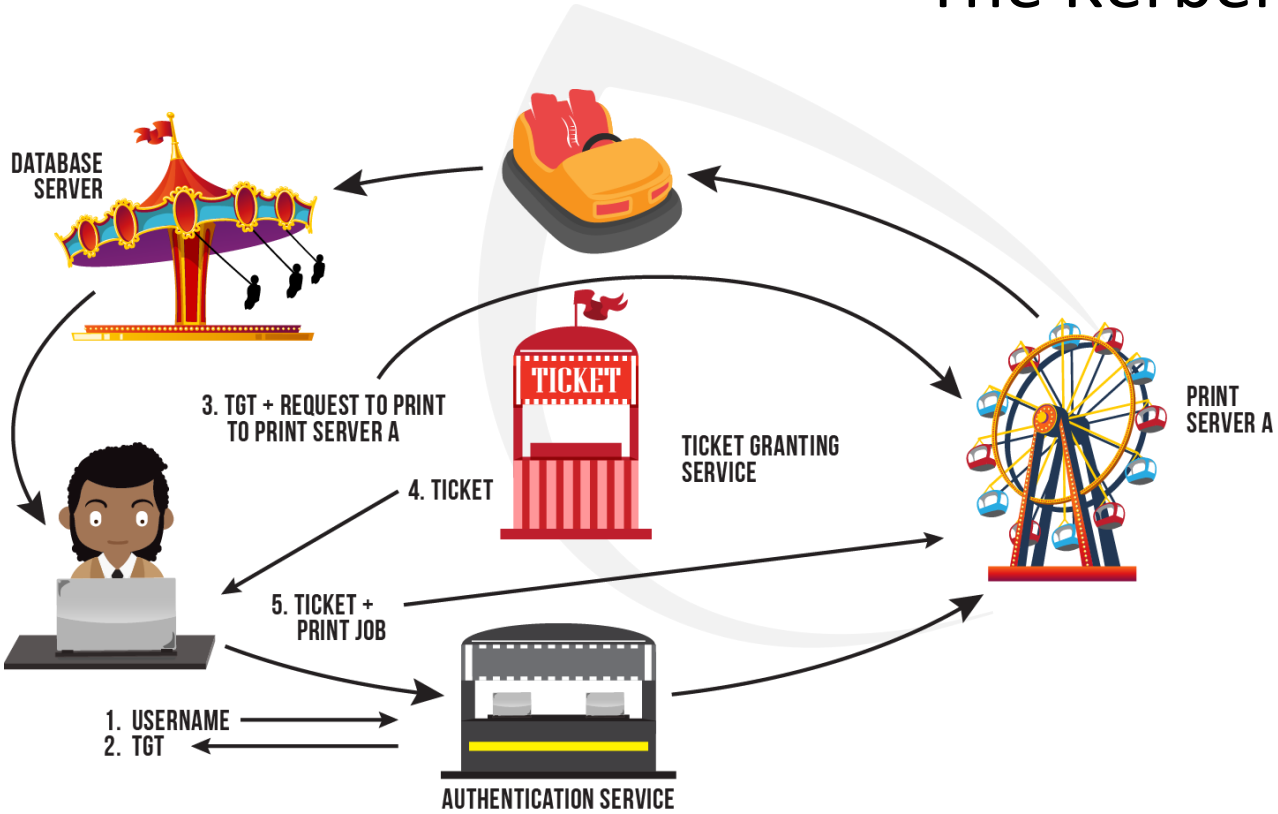
Kerberos Components

- Essential Components:
- AS (Authentication Server): Allows authentication of the user and issues a TGT
- TGS: After receiving the TGT from the user, the TGS issues a ticket for a particular user to access a particular service
  KDC (Key Distribution Center) a system which runs the TGS (Ticket Granting Service) and the AS (Authentication Service)
- Ticket: Means of distributing Session Key
- Principles (users, applications, services)
- Kerberos Software (integrated into most Operating Systems. MS Windows 2000 and up support Kerberos)
- Main Goal: User needs to authenticate himself/herself without sending passwords across the network—needs to prove he/she knows the password without actually sending it across the wire.

The Carnival



The Kerberos Carnival



Kerberos Concerns

- Computers must have clocks synchronized within 5 minutes of each other
- Tickets are stored on the workstation. If the workstation is compromised your identity can be forged.
- If your KDC is hacked, security is lost
- A single KDC is a single point of failure and performance bottleneck
- Still vulnerable to password guessing attacks

Single Sign On Federated Services

Today’s Identity Management in the Cloud

Provisioning Identities

Authentication

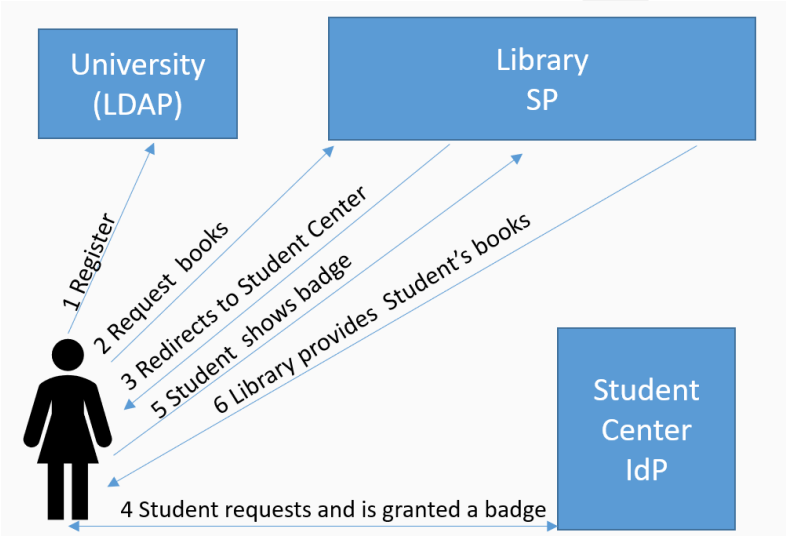
Authorization

As a company on-boards and off-boards employees, they are added and removed from the company's electronic employee directory. As long as the service provider supports the SCIM standard, SCIM Could then be used to automatically add/delete (or, provision/de-provision) accounts for those users in external systems such as Google Apps for Work, Office 365, or Salesforce.com. Then, a new user account would exist in the external systems for each new employee, and the user accounts for former employees would be removed from those systems

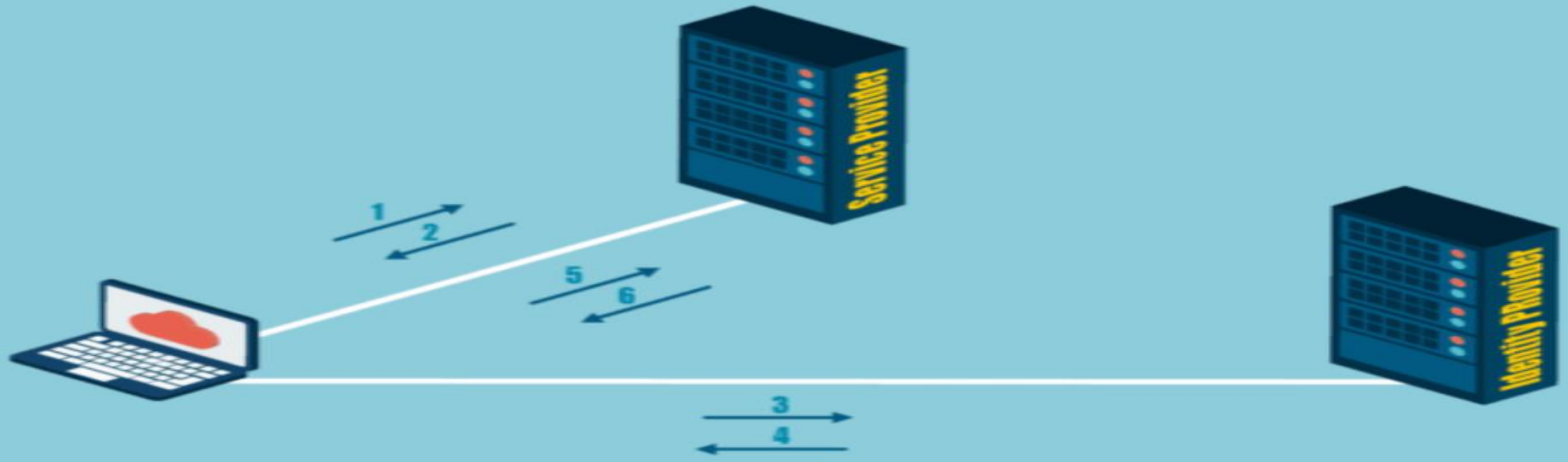
SAML (Security Assertion Markup Language)

- For SSO with web applications, SAML works using set of browser redirects and message exchanges.
    1. User tries to access web application, the application redirects user to identity provider.
    2. User authenticates himself
    3. Identity provider issues a claims token and redirects user back to the application.
    4. Application then validates the token (trust needs to established out of band between application and IdP), authorizes user access by asserting claims, and allows user to access protected resources.
    5. The token is then stored in the session cookie of user browser, ensuring the process doesn’t have be repeated for every access request

SAML Assertions



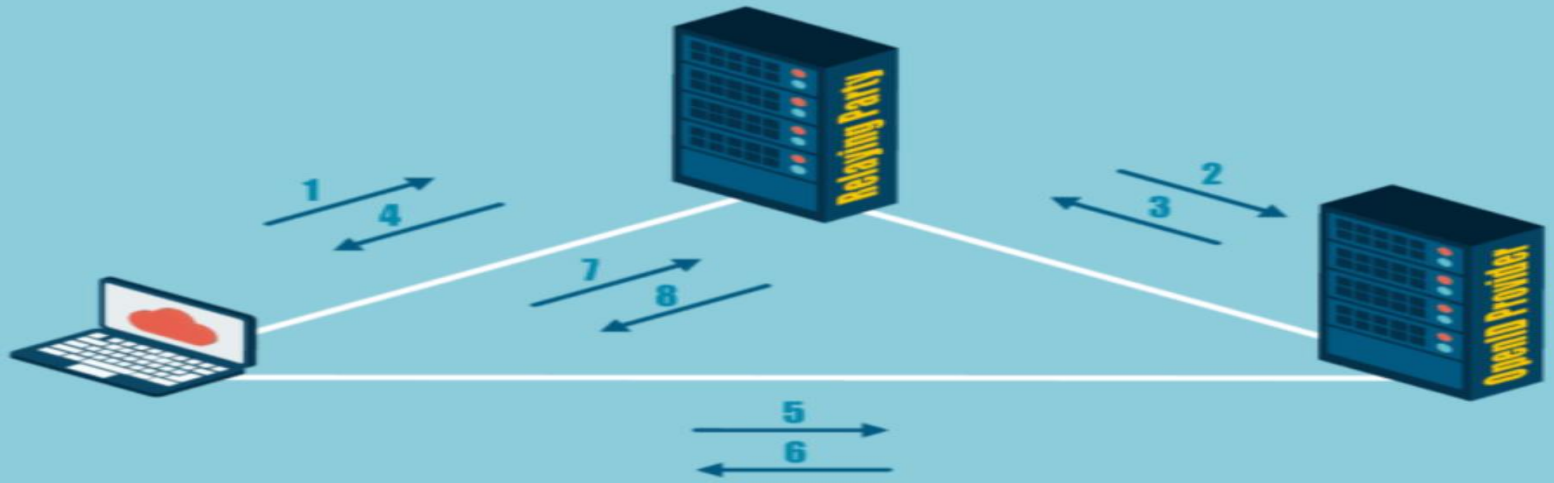
1. Student Registers at School
2. Student goes to library to receive his books
3. Library directs student to the student center to pick up his Student ID badge
4. Student Center has access to the same database as the university, so they verify the identity of the student and give him his student id badge
5. Student Provides the library his Student ID Number and badge and requests his books.
6. Library accepts the school ID as proof of authenticity and provides student his books



SAML v2.0 Process Flow

1. User attempts to access a hosted corporate application
2. *Service provider* generates and sends SAML request to the user
3. User is redirected to the *identity provider* together with the SAML request
4. *Identity provider* authenticates user, parses SAML request and generates encoded SAML response which is sent to the user's browser
5. User's browser sends SAML response to *service provider*
6. *Service provider* verifies the user's SAML response and grants application access

SoftwareSecured



OpenID Connect Process Flow

1. User provides their OpenID URL (https://jane.openidprovider.com)
2. Relaying party discovers via XPDS and initiates association with OpenID provider
3. OpenID provider generates key and association then returns key and association to relaying party
4. Relaying partner forwards key and association to the user
5. User is redirected to OpenID provider with authentication request
6. OpenID validates requests redirecting the user to relaying party with signed assertion
7. User presents signed assertion to relaying party
8. Relaying party valides assertion and creates session

SoftwareSecured

Authorization: OAUTH 2.0

- OAuth (Open Standard for Authorization) has different intent
- Not designed for SSO
- Provides delegation of rights to applications
- In simplest terms, it means giving your access to someone you trust, so that they can perform the job on your behalf. E.g. updating status across Facebook, Twitter, Instagram, etc. with a single click.
- Could go to the sites manually, but easier to delegate access to an app that connect the above platforms
- Authenticate yourself to Facebook, Facebook provides a consent page stating you are about give this app rights to update status on your behalf. If you agree, the app gets an opaque access token from Facebook, app stores that access token, send the status update with access token to Facebook
- Facebook validates the access token (easy in this case as the token was issued by Facebook itself), and updates your status.

Authorization

Authorization

Now that I proved I am who I say I am, what can I do?

- Both Operating Systems and Applications can provide this functionality.
- Authorization can be provided based on user, groups, roles, rules, physical location, time of day (*temporal isolation*)* or transaction type (example a teller may be able to withdrawal small amounts, but require manager for large withdrawals)

Authorization principals

- Default NO access (*implicit deny*)* - **Unless** a subject is **explicitly** given access to an object, then they are **implicitly** denied access.
- Principle of Least Privelege
- Need to know
- Content-based

Access Control Models

Access Control Models

A framework that dictates how subjects access objects.

- Uses access control technologies and security mechanisms to enforce the rules
- Supported by Access Control Technologies
- Business goals and culture of the organization will prescribe which model is used
- Every OS has a security kernel/reference monitor (talk about in another Domain) that enforces the access control model.

Access Control Models

The models we are about to discuss are

- From the TCSEC(Trusted Computer System Evaluation Criteria—Orange Book)
  - DAC (Discretionnary Access Control)
  - MAC (Mandatory Access Control)
- Other Models
  - RBAC (Role Based Access Control)
  - ABAC (Attribute Based Access Control)
  - RuBAC (Rule Based Access Control)

DAC

Discretionary Access Control

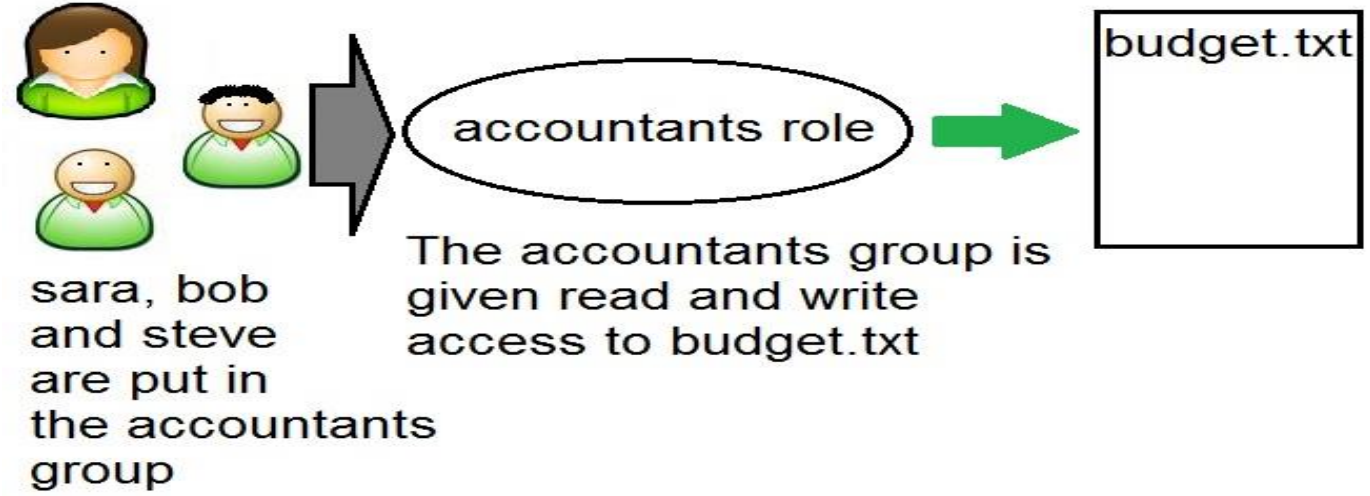
- Security of an object is at the owner's discretion
- Access is granted through anACL (Access Control List)
- Commonly implemented in commercial products and all client based systems
- Identity Based

MAC

MAC is used where classification and confidentiality is of utmost importance… military.

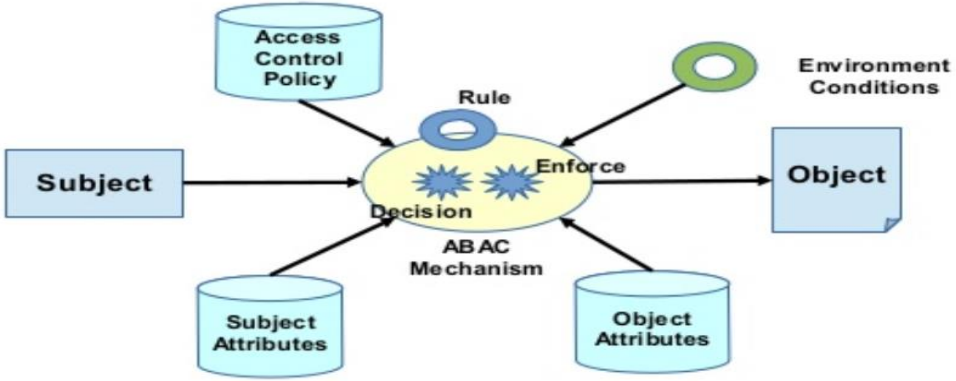
- Generally you have to buy a specific MAC system, DAC systems don't do MAC
  - SELinux
  - Trusted Solaris (now called Solaris with Trusted Extensions)
- All objects in a MAC system have a security label*
- Security labels can be defined the organization.
- They also have categories to support "need to know" at a certain level.
- Categories can be defined by the organization

Role Based Access Control



- RBAC is a good solution to mitigate privilege creep and provides the strongest constraint on user access
- RBAC is well-suited for environments with high turnover rates

Attribute Based Access Control



- Permissions or privilege granted based on attributes of the subject. Attributes can be
  - Location
  - Role
  - Tenure
  - Any other attribute of the subject or object

Enforcing Access Control

Enforcing Access Control

We will talk more in depth of each in the next few slides.

- Constrained User Interfaces
- Access Control Matrix
- Access Control Lists
- Content-Dependant Access Control
- Context-Dependant Access Control

Constrained User Interfaces

Restrict user access by not allowing them see certain data or have certain functionality (see slides)

- Views – only allow access to certain data (canned interfaces)
- Restricted shell – like a real shell but only with certain commands. (like Cisco's non-enable mode)
- Menu – similar but more “GUI”
- Physically constrained interface – show only certain keys on a keypad/touch screen. – like an ATM. (a modern type of menu) Difference is you are physically constrained from accessing them.

Physically Constrained Interface

Content vs. Context Dependant Access Control

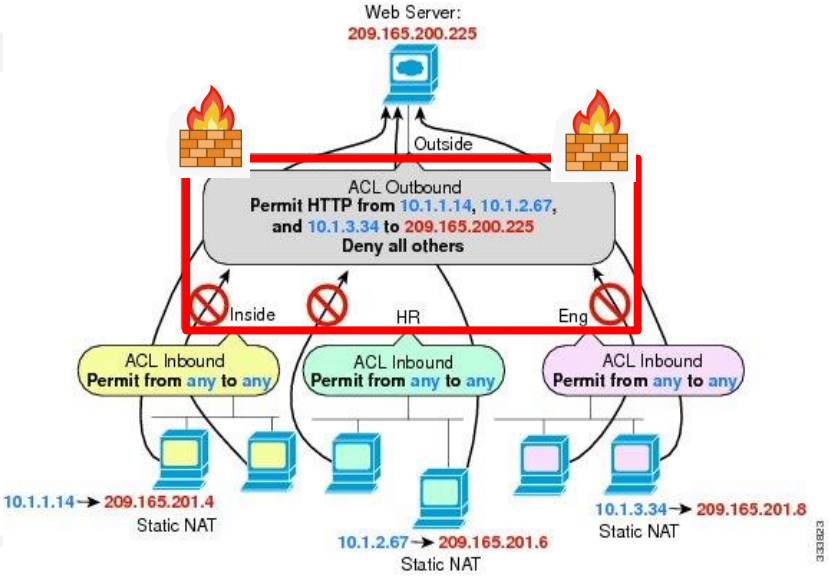
Content: WHAT is accessed? Focus is on the asset

Context: How and Why is it being accessed? The asset isn't the driver for decisions but things like time, location, type of connection, etc

Rule-Based Access Control

- Rule-based access control is based on rules to deny or allow access to resource
- If the rule is matched, access will be denied or allowed, based on the rule
- Routers, Firewalls, Proxies and other filtering devices use rules to enforce access

- Sometimes called “Non-Discretionary” because the rules cannot be arbitrarily bypassed



Access Control Management

Centralization vs. Decentralization

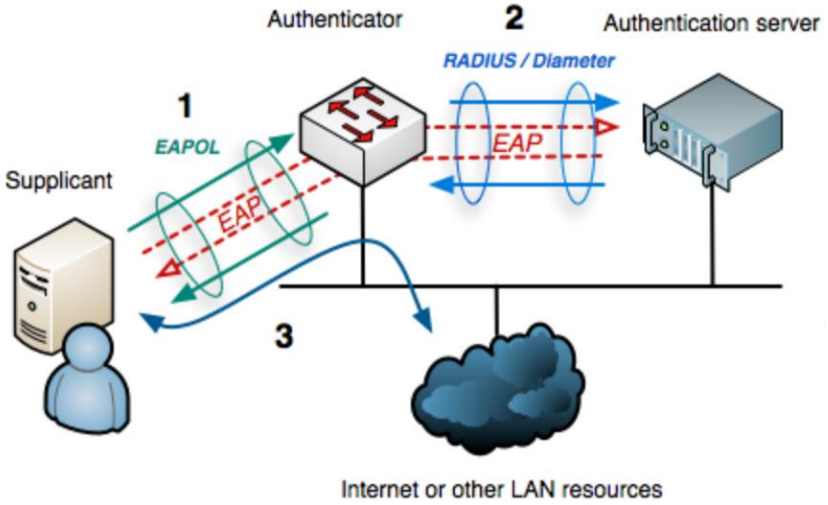
- Centralization:
  - Greater Consistency
  - Ease of Administration
  - Greater Control
  - Usually considered more secure
- Decentralization
  - Granularity
  - Flexibility

Centralized Access Control Administration

- A centralized place for configuring and managing access control
- All the ones we will talk about (next) are “AAA” protocols
  - Authentication
  - Authorization
  - Auditing
- Radius
- TACACS, TACACS+
- Diameter

Centralized Authentication for Remote Clients: 802.1x

802.1X is a security feature that provides a means to authenticate devices before they can access network resources.



RADIUS, DIAMETER, TACACS

RADIUS

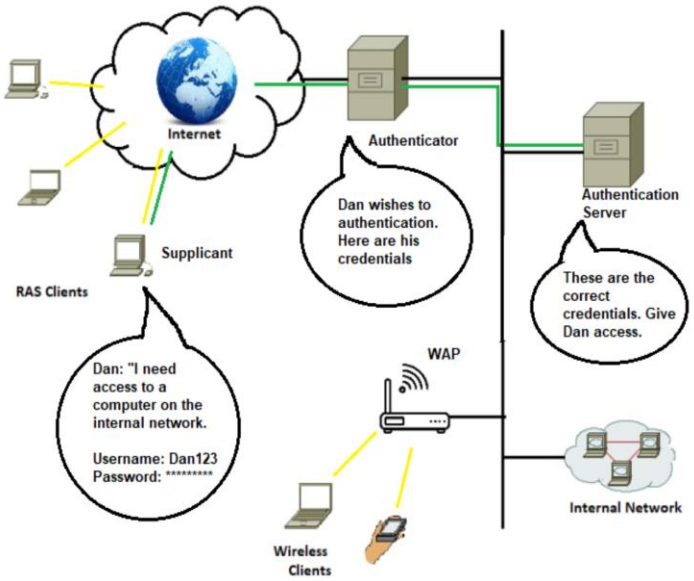
- Designed for dial-up, but extensions are available to allow additional functionality as needed
- RADIUS encrypts only the password in the access-request packet, from the client to the server.
- RADIUS uses UDP

TACACS+

- Provides same services
- Developed by Cisco
- Separates roles of AAA
- USES TCP

DIAMETER

- DIAMETER is a protocol designed as the next generation RADIUS
- RADIUS is limited to authenticating users via SLIP and
- PPP dial-up modem connections



TACACS+

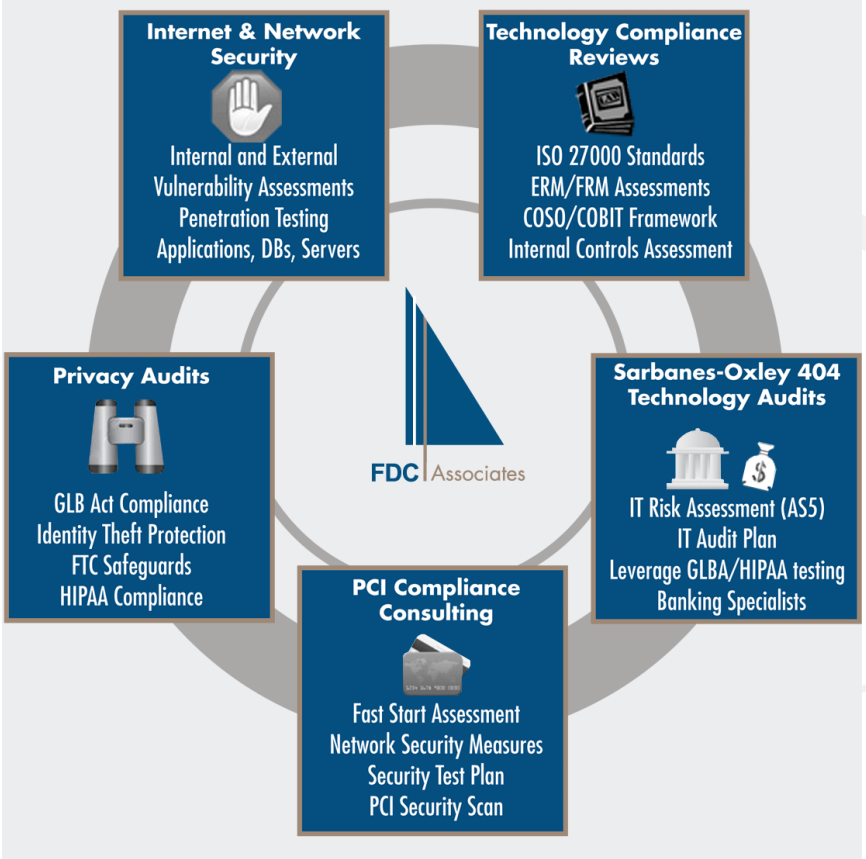
- Provides the same functionality of Radius
- TACACS+ can support one time passwords
- Encrypts ALL traffic data
- TACACS+ separates each AAA function.
  - For example can use an AD for authentication, and an SQL server for accounting.
- Uses TCP

Diameter

- Supposed to be the next generation of RADIUS (Diameter is TWICE the RADIUS)
- Includes better message transport, proxying, session control, and higher security for AAA transactions
- Provides encryption for the communication, not just the password
- Never gained the application support RADIUS did
- USES UDP

Auditing

Audits



Associate Audits with compliance:

- Compliance with policy
- Compliance with Standards

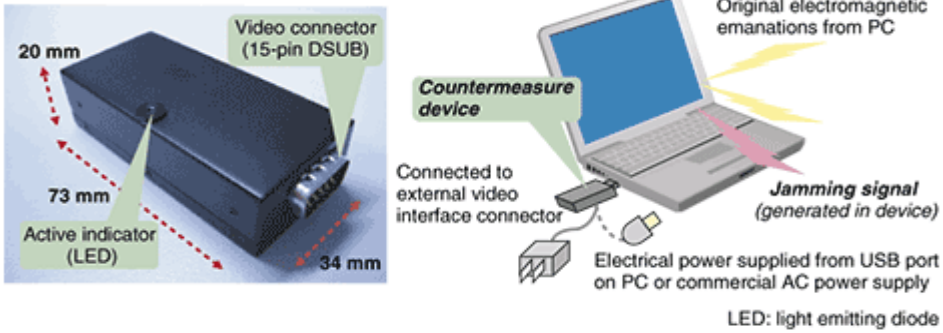
Remember Auditors do not need write protection

Also, auditors do not provide suggestions on remediation

Data Emanation Security

Emanation Security

- All electronic devices emit radiation. TEMPEST was a study t o determine if anything meaningful could be learned. YES!
- Tempest then became a standard to develop countermeasures to protect against this.
  - Faraday cage – a metal mesh cage around an object, it negates a lot of electrical/magnetic fields.
  - White Noise – a device that emits radio frequencies designed to disguise meaningful transmission.
  - Control Zones – protect sensitive devices in special areas with special walls etc.



Domain 5 Identity and Access Management Review

- Overview
- Identity Management
  - Identity Proofing
  - Account Provisioning/Deprovisioning
- Authentication
  - Type 1, Type 2, Type 3
  - Kerberos and Single Sign on
  - Single Sign on: Federated Services
- Authorization
- Access Control Models
- Enforcing Access Control
- Access Control Management
- Auditing/Accountability
- Data Emanation